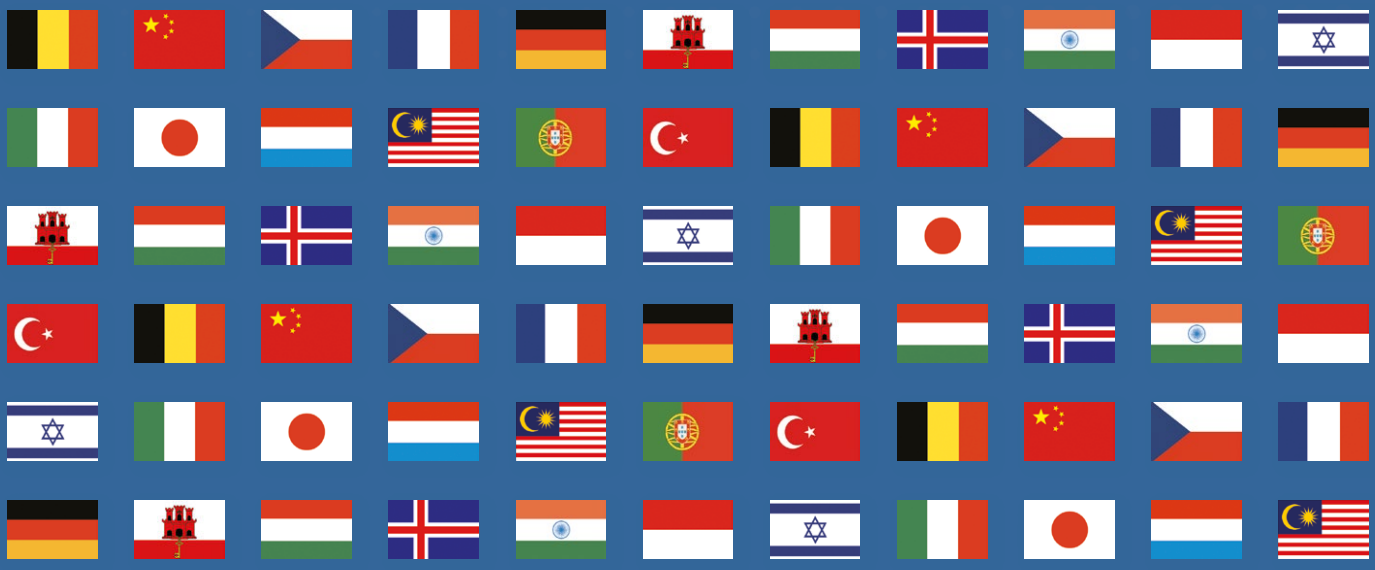
LEXOLOGY
Getting The Deal Through

# DIGITAL BUSINESS 2024

Consulting editor
**Ashley Winton**





LEXOLOGY
Getting The Deal Through

START READING

# Jurisdictions





Published September 2023

# Belgium

Steven De Schrijver*

Agio Legal

RETURN TO CONTENTS

## Summary

**Read this article on Lexology**

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

Belgium is a highly digitalised and modern country with many innovative businesses. It ranks high in the list of most innovative economies in the world and has one of the best digital infrastructures in Europe. The federal and regional governments support further growth of the technology sector with national and regional support strategies and plans on technologies such as artificial intelligence, Internet of Things, robotics and cybersecurity. There is a wide array of tax incentives and subsidies available for research and development and investment in innovation. Universities and other educational institutions also obtain important funding to provide support to digital businesses, train the next generation of technology specialists and conduct important research on technological developments. Digital business is, therefore, seen as a positive factor that strongly contributes to the economy and therefore its growth must be stimulated.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

Given the broad impact of digital businesses and digital transformation in different sectors, it is difficult to pinpoint all the specific legislation that comes into play. The most important laws are the following:

- the Belgian Code of Economic Law;
- the (new and old) Belgian Civil Code;
- the Telecommunications Act of 13 June 2005;
- the Belgian Privacy Act of 30 July 2018 (implementing the General Data Protection Regulation where necessary); and
- the NIS Act of 7 April 2019.

### Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The most important regulatory bodies in the digital sphere are:

- Belgian Institute for Postal Services and Telecommunications (BIPT/IBPT) (telecommunications regulator);
- Federal Public Service Economy (FOD Economie/SPF Economie) (consumer and economic law regulator);
- Belgian Data Protection Authority (DPA) (Gegevensbeschermingsautoriteit/Autoritée de protection des données);

- National Bank (Nationale Bank van België/Banque Nationale de Belgique) (financial services regulator); and
- Financial Markets and Services Authority (FSMA) (financial services regulator).

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Under Regulation (EU) 1215/2012 of 12 December 2012 (Brussels I bis Regulation), a consumer may in principle bring proceedings against the digital business either in the home state of the digital business or in his or her own jurisdiction. On the other hand, a digital business may only bring proceedings against a consumer in the latter's home state. Where the customer is not a consumer, the parties may agree on a forum in their agreement or apply the other rules foreseen in the Brussels I bis Regulation.

Where disputes are held against a party outside the European Union, specific international private law rules will apply to determine the applicable jurisdiction. For example, Belgian courts have jurisdiction if the defendant is domiciled or habitually resident in Belgium when the claim is initiated, or if the parties have so agreed.

A party who finds that a dispute brought before a Belgian court should be brought somewhere else based on the underlying agreement, the Brussels I bis Regulation or other laws, must raise this in court. The Belgian court will in principle have to respect such rules, and in any case has to respect these when it comes to the Brussels I bis Regulation, save for a number of exceptions. The applicable law can be different to that of the applicable forum.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

No particularities apply to digital companies compared to 'normal' companies, and digital businesses can therefore be established in the same way. In principle, there is no authorisation or permit required to provide digital content and services, unless the company is operating in a regulated sector (eg, financial services or gambling).

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

It is possible to form and conclude contracts digitally. The general formation rules of the Belgian Civil Code apply, namely, the parties must have the capacity to enter into an agreement, the valid consent of the parties is required, there must be a clear object and a lawful cause. A contract can be concluded digitally (eg, through a distance sale, email, etc). Additional rules may apply, especially in consumer contracts in distance sales, which among others require certain pre-contractual information obligations to be met and include mandatory post-sale rights such as a revocation of sale right. Belgian contract law also includes rules on unfair terms in both business-to-consumer (B2C) and business-to-business (B2B) relationships, some of them being null and void by law.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Regulation (EU) 1215/2012 of 12 December 2012 (Brussels I bis Regulation) determines the courts before which a person may be called upon to appear in another member state. The law applicable to non-contractual obligations is determined by Regulation 864/2007/EC of 11 July 2007 (Rome II Regulation). The parties are in principle free to determine the forum and applicable law themselves, except in the case of specific agreements (eg, in a B2C relationship, an insurance agreement, etc) where restrictions apply.

While the parties are free to choose the language of the contract, the language used in specific contracts, such as in a B2C relationship, must be understandable and legible. To avoid the nullity of a contract with consumers, it is required that it be drafted in the language of the consumers, especially when it concerns complex services.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

According to the Belgian Civil Code, a signature is valid when it consists of a sign or a succession of signs, affixed by hand, electronically or by any other process, by which a person identifies themself and from which their expression of will appears. The Civil Code acknowledges that such a signature can be electronic.

A qualified electronic signature is recommended, in the sense of Regulation (EU) No 910/2014 on electronic identification and trust services (eIDAS Regulation), when applying a digital signature, rather than a scanned copy. Qualified electronic signatures can only be provided by a registered trust service provider, who is subject to a number of rules when providing an electronic signature service (especially in respect of consumers).

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

No. Ordinary courts or arbitration institutes (eg, CEPANI in Belgium) will deal with such disputes.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The advertising or selling of financial services products to consumers or to business digitally is very strictly regulated. This includes rules in the Belgian Code of Economic Law and specific regulatory financial laws and may, for instance, include certain prohibitions on the type of advertising, the provision of comprehensive pre-contractual information or the provision of a cooling-off period during which the consumer can withdraw from the contract. Rules depend on the type of product, and will list in detail what information must be provided and which other obligations apply. General rules on unfair commercial practices may apply too. The supervisor of these rules is in principle the Financial Markets and Services Authority or the Federal Public Service Economy. When financial instruments are offered via the internet, the issuers thereof must also carefully verify whether or not the detailed rules on public offers, which are substantially based on European law, apply.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

The Belgian Act of 11 March 2018 on the Legal Status and Supervision of Payment Institutions and Electronic Money Institutions, Access to the Business of Payment Service Provider and to the Activity of Issuing Electronic Money, and Access to Payment Systems, regulates the issue of electronic money, which is a licensed activity. Any person wishing to issue electronic money as an e-money institution in Belgium must, save for a number of limited exceptions, obtain a licence from the National Bank of Belgium. Book VII of the Belgian Code of Economic Law contains further rules on the issuing of e-money. A number of European regulations may also apply, as well as anti-money laundering regulations. Substantially the same rules apply throughout the European Union (EU).

There are, in principle, no specific rules applicable to digital assets and digital currencies. However, under the Belgian Anti-Money Laundering Act of 18 September 2017 and the Royal Decree of 8 February 2022, the providers of exchange services between fiat and virtual currency must register in Belgium. Providers of such services from outside the European Economic Area (EEA) are prohibited from providing their services in Belgium.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

The Belgian Anti-Money Laundering Act of 18 September 2017 regulates crypto exchanges and wallet providers. The new rules require providers engaged in exchange services between virtual currencies and fiat currencies, as well as custodian wallet providers, to be registered in Belgium (including if they own ATMs in Belgium). Above all, they prohibit such providers from providing services in Belgium when they are established in a third country without having an establishment in the EEA. The Royal Decree of 8 February 2022 further details the registration conditions (eg, a fully deposited minimum registered capital of €50,000 and a fit and proper management). This is a unique Belgian law that is not found across all jurisdictions of the EU, and is for now separate from the rules under the future Markets in Crypto Assets (MiCA) Regulation.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

The Belgian Act of 11 March 2018 on the Legal Status and Supervision of Payment Institutions and Electronic Money Institutions, and the Code of Economic Law, contain the rules on electronic payment systems, implementing thereby the EU PSD2 framework into Belgian Law. Such payment institutions must be licensed in Belgium with the National Bank. The PSD2 framework regulates rules on third-party access to digital information in bank accounts, which may also be subject to the General Data Protection Regulation. Substantially the same rules apply throughout the EU.

## Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

The Anti-Money Laundering Act of 18 September 2017 regulates AML requirements and is applicable to a long list of institutions, including financial institutions, providers of certain financial services and providers of gaming services. The Act is based on a risk-based approach that, depending on the customer, obliges organisations to apply different identification procedures before entering into a business relationship. Specific KYC rules may also

apply in financial law based on the MiFID framework. Substantially the same rules apply throughout the European Union.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

At international level, the non-profit organisation Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the management of domain names. A domain name must be requested from an authorised agent. At European level, several regulations govern the legal framework surrounding domain names with the .eu extension. EURid, a Belgian non-profit association with its head office in Brussels, takes care of the management. These domain names can only be requested by European Union (EU) citizens or persons or companies who have their residence or establishment within the EU. At national level, the Belgian Association for Internet Domain Name Registration (DNS Belgium) is only responsible for the management of domain names – not for requesting the domain name; that must be done through an authorised agent or 'registrar' who has entered into an agreement with DNS Belgium. The nationality of the party requesting the domain name is irrelevant, nor are there any other special restrictions. Foreign agents can request the registration of a domain name from DNS Belgium. Likewise, Belgian agents can address requests from Belgian and foreign customers to the relevant manager in another country.

It is interesting to note that the Belgian Data Protection Authority and DNS Belgium have concluded an agreement, dated 1 December 2020, pursuant to which certain restrictions can be placed on websites with a Belgian domain name that do not comply with the General Data Protection Regulation (GDPR), even possibly leading to a cancellation of the domain name. This procedure makes it possible to redirect .be domain names to a warning page of the government body that has the legal authority to act against serious breaches of certain rules of law. For instance, if the processing of personal data, via a website linked to the domain name, constitutes a violation of the GDPR, the Data Protection Authority can issue an order to freeze or stop that processing. Also, subsequently DNS Belgium can revoke the website linked to the .be domain name.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Strictly speaking, the applicant only receives a licence or exclusive right to use the domain name, but not the actual ownership. Nevertheless, a domain name holder can take action

under the Code of Economic Law against another domain name holder if the domain names are similar or identical, subject to a number of conditions. Ownership of a trademark can also support a challenge against a similar domain name, as the owner can also invoke trademark law.

## ADVERTISING

### Regulation

**17** | What rules govern online advertising?

Advertising is a commercial practice. Therefore, the provisions of the Code of Economic Law apply (both in business-to-consumer and business-to-business relationships). For example, advertising is misleading if it displays false information or omits crucial information such that this induces the average consumer or business to make a decision about a transaction that the consumer or business would not otherwise have made. The rules on the permissibility of comparative advertising are also applicable. Comparative advertising is only permitted on condition that it:

- is not misleading;
- compares goods or services that meet the same needs or are intended for the same purpose;
- objectively compares one or more essential, relevant, verifiable and representative characteristics of these goods and services, which may include price;
- does not cause, among undertakings, the confusion of the advertiser with a competitor, or the confusion of brands, trade names, other distinguishing marks, goods or services of the advertiser with those of a competitor;
- does not damage the good name of or denigrate the brands, trade names, other distinguishing characteristics, goods, services, activities or circumstances of a competitor;
- for goods with a designation of origin, relates in any event to goods with the same designation;
- does not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing mark of a competitor or of the designations of origin of competing goods; and
- does not present goods or services as an imitation or replica of goods or services bearing a protected trademark or trade name.

These are cumulative requirements. Therefore, advertising that does not comply with all conditions is prohibited. Furthermore, specific legislation may apply, such as in the case of advertising for medicine, financial services or alcohol.

Publicity through electronic communication is also regulated in the Code of Economic Law, and may also be subject to the General Data Protection Regulation (GDPR) if it concerns the processing of personal data.

The Code of Economic Law also contains specific identification and transparency principles for online advertising.

## Targeted advertising and online behavioural advertising

### 18 What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

There are no specific regulations regarding targeted and online behavioural advertising in Belgium. These are subject to general rules on advertising and, if personal data is processed to analyse the user's behaviour, the GDPR. When cookies are used, which have a 'tracking' function that allows them to follow the browsing habits of internet users on other websites, prior consent to such use by the user must also be obtained following the provision of clear and precise information concerning the processing of the user's data. This applies regardless of whether the information is personal or anonymous. Consent is only not required if the cookies are used for the sole purpose of carrying out the transmission of a communication or are strictly necessary to provide an information society service explicitly requested by the user.

## Misleading advertising

### 19 Are there rules against misleading online advertising?

The provisions of the Code of Economic Law regulate misleading advertising across all industries. Misleading advertising entails, among others, that false information is displayed or crucial information is omitted. Evidence must be provided that such information or omission of information induces the average consumer to make a decision about a transaction that he or she would not otherwise have made. In case of a misleading omission, the deception must relate to the essential information (eg, the main characteristics of the product, the price or the method of payment).

## Restrictions

### 20 Are there any digital products or services that may not be advertised online?

There are no specific restrictions for digital products and services, besides those with respect to financial services and gambling (the advertising of non-licensed gambling facilities and games being prohibited).

## Direct email marketing

### 21 What regulations and guidance apply to email, SMS and other direct marketing?

The e-Privacy Directive has been implemented in the Code of Economic Law, which contains the opt-in principle for publicity. This means that the use of electronic communication for advertising is prohibited without the prior, free, specific and informed consent of the addressee. The GDPR may equally apply. Nevertheless, an exemption from consent applies in two situations.

- Firstly, by means of an entry in the customer file. This exception requires three conditions:

- it must concern a real customer (this is a person with whom the service provider already had at least a contractual relationship) from whom the service provider received the electronic data directly, and not through third parties;
- the service provider may only use the customer's electronic data for advertising purposes for similar products or services to those it offers; and
- the service provider, at the time it receives the electronic data, allows the customer to object to such use free of charge and in a simple manner.

- Secondly, if the electronic message is sent to legal entities. It is irrelevant whether the legal entity is even a customer. However, two conditions apply:

  - the advertisement must be sent to a non-personal electronic address (eg, contact@firma.be), not to the address of an employee of a legal person; and
  - the products or services offered in the advertisement must be directed to legal entities – the advertising must not be intended for natural persons, as is the case regarding vacation destinations, for example.

Both the Belgian Data Protection Authority and the Federal Public Service Economy have issued detailed guidelines on direct marketing and publicity through electronic communications.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Under the Code of Economic Law, and pursuant to European law, three different types of exemptions of liability for providers of information society services exist when they act as intermediaries under the *mere conduit* principle. Generally speaking, when such providers do not initiate the transmission or do not have the opportunity to modify the information transmitted, they are exempted from liability. Specific conditions must be assessed for each type of exemption.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

There are no specific rules regarding liability for advertising and information published online. The general liability rules of the Civil Code, including those regarding the exemptions on liability through a disclaimer and its limitations, apply.

The Belgian Code of Economic Law provides for a cascading presumption of liability in the event of an action against publicity:

- the advertiser (if domiciled in Belgium);
- the publisher of the written advertising or the producer of the audio-visual advertising;
- the printer or the director; and
- the distributor.

Liability can be shared. Criminal liability is equally possible.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

How online content providers and ISPs deal with defamatory material is primarily regulated by themselves. There is no Belgian legislation with respect thereto. The upcoming European Digital Services Act will introduce certain rules on transparency of content moderation platforms.

Nevertheless, the Belgian Supreme Court (Hof van Cassatie/Court de Cassation) did accept in 2013 that internet access providers can be required to make a website inaccessible to internet users. The purpose of the data seizure is to stop acts that appear to constitute a crime. The data seizure is possible in two situations. Firstly, if the data constitutes the object of a crime or arose from a crime and is contrary to public order or morality; (criminal) hate speech and crimes always fall into this category, because of the broad wording. Secondly, if the data endangers the integrity of information systems or data stored, processed or transmitted by them.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

It is generally accepted that data are not protected by intellectual property rights. After all, there is no creative process happening with data as there is in relation to copyright. However, this view needs to be nuanced. For example, it is possible that the selection and arrangement of data take place in a certain way for which creative choices have been made. In such a case, one can claim copyright on the structure of the database.

Databases, on the other hand, are protected by intellectual property rights, specifically by the Code of Economic Law. These can be protected by:

- a specific sui generis right, protecting the content of the database, even if it is not original, and certain conditions (eg, sufficient investments were made); and/or
- copyright law protecting the structure of the database, if it is original.

## Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

In principle, it is permitted to link to a third-party website. However, liabilities arise if a link is made to unlawful content. Restrictions may also apply if content is embedded in a webpage by means of hyperlinks and frames wherein third-party content is displayed. Under European Union copyright law, it is permissible to hyperlink to a website of a third party if the linked material is: (1) still publicly available; and (2) was originally communicated on the internet with the content owner. The link may be infringing a third-party copyright if the linked material has been removed or if it circumvents any subscription, pay or other technical barriers imposed by the original content owner.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Yes, unless such content is protected by copyright laws or if it contains personal data, in which case the obligations under the General Data Protection Regulation apply. Scraping could also be prohibited based on a website's terms of use.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Novel technologies often give rise to novel legal issues, as the law is usually behind technological developments. The metaverse is not different in this sense. Examples thereof are the questions regarding the creation and protection of intellectual property rights for downloadable virtual goods and services in the metaverse, and the scope of the rights to use the content held by a non-fungible token owner (eg, with respect to the classification and similarity of goods and services and the doctrine of exhaustion).

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

The first-sale doctrine is recognised under European law and requires a first sale that occurred with the consent of the right holder within the European Economic Area. The Court of Justice of the European Union stated that a sale may involve tangible and intangible property. Consequently, for digital products, one can speak of a 'first-download doctrine'.

### Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

The General Directorate of Economic Inspection has several tasks, listed in the Code of Economic Law. One of its roles is to monitor compliance with economic regulations through informative, preventive, warning and repressive action. This includes detecting and determining violations of the Code of Economic Law and various economic regulations. For example, the Directorate can carry out dawn raids and seize false products that infringe intellectual property rights. In 2020, the Directorate seized 83,729 fake products in 179 of its 377 controls thereon. This number was lower due to the pandemic, as in 2019 182,554 fake products were seized in 278 such controls.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

The IP owner can file a cease-and-desist action in a civil court to order the cessation of an infringement of IP rights. The cessation may be accompanied by a penalty payment. The owner may also seek damages to compensate them for their loss. Furthermore, they can request measures for the description and preservation of any infringing material. This procedure is called 'the seizure of counterfeit'. Finally, certain ancillary claims are possible, such as for the remittance of profits, the recall of the goods from the market or the forfeiture of the infringing goods.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Under the General Data Protection Regulation (GDPR), 'personal data' means any information relating to an identified or identifiable natural person whereby an 'identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This definition applies throughout the European Union (EU).

Additionally, a number of categories of sensitive personal data exist (eg, data about a person's health, ethnicity, sexual orientation or political views). The processing of these data is prohibited, barring exceptions. For example, if the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent, or if the processing relates to personal data that are manifestly made public by the data subject.

## Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

There is no registration requirement to be allowed to process personal data. However, any organisation processing personal data must have a valid legal basis to do so. There are six legal bases listed in the GDPR:

- consent;
- performance of a contract;
- legitimate interest;
- vital interest;
- legal requirement; and
- public interest.

Each legal basis is subject to a number of conditions that have to be carefully assessed. Further obligations apply under the GDPR, including the requirement to document all activities concerning the processing of personal data in the data register.

The GDPR prescribes the appointment of a data protection officer (DPO) in three cases: (1) if there is a large-scale regular and systematic monitoring of users; (2) if the processing is carried out by a public authority; and (3) if the organisation is performing complex operations with user data. If the organisation falls outside one of these cases, the appointment of a DPO is not mandatory, but allowed voluntarily.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The GDPR is applicable in the three following situations:

- the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not;
- the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:
    - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
    - the monitoring of their behaviour as far as their behaviour takes place within the EU.
- the processing of personal data by a controller not established in the EU, but in a place where member state law applies by virtue of public international law.

Nevertheless, data controllers or processors that are not based in the EU but perform processing activities that fall within the scope of the GDPR, must designate a representative in the EU.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

There are six legal bases for processing listed under the GDPR:

- consent;
- performance of a contract;
- legitimate interest of the data controller;
- vital interests;
- legal requirement; and
- public interest.

Each of them is subject to its own rules and conditions. A sufficient legal basis must be established to export personal data to a jurisdiction outside the EU, to which additional obligations apply.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Cross-border data transfers within the European Economic Area or to countries that are considered to provide adequate data protection in comparison to the EU are permitted. An adequate level of protection is provided through a European Commission adequacy decision. A transfer outside the EU is then equated with a transfer within the EU. The countries that benefit from the adequacy decision are, currently, Andorra, Argentina, Canada (for commercial organisation), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay.

In the absence of an adequacy decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals. Examples of safeguards are the use of binding corporate rules, (the 'new') standard contractual clauses (SCCs) (taking into account the European Court of Justice's *Schrems II* judgment) and adherence to other formalities. The *Schrems II* judgment states that the US does not provide an adequate degree of protection due to a lack of proportionality of mass-surveillance programmes and a lack of effective remedies equivalent to those required by the GDPR. Therefore, the EU-US Privacy Shield adequacy decision is invalid, which means that it can no longer be relied on to transfer personal data to the US.

If there is no adequacy decision and no safeguards, a transfer can be made based on a limited number of derogations for specific situations. For example, it may be sufficient

that an individual, who is aware of all the risks of the transfer, explicitly agrees to such data transfer.

### Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

The two most generally accepted legal bases in the GDPR for the sale, license or transfer of personal data are the data subject's consent and the data controller's legitimate interests. If the data is sold or transferred without a legal basis for the processing, it must be deleted by the purchaser. The seller can be held liable for the sale price and any damages in case of an illicit transfer.

### Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Data subjects have multiple rights and remedies under the GDPR. For instance, they have the right to lodge a complaint with a supervisory authority (the Data Protection Authority), the right to an effective judicial remedy against a controller/processor/supervisory authority and the right to compensation and liability. Specifically in Belgian law, they can invoke article 1382 of the (Old) Civil Code to hold another party liable for infringements of the GDPR and the Belgian Privacy Act of 30 July 2018.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

Answer in progress.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

In principle, most documents and archives can be held digitally, provided that the authenticity of the digital copy can be proven to the authorities when required.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Different retention periods apply to different types of documents. These range, for the most important categories, from five years following the completion of the liquidation of a company for corporate documents to 10 years for the accounting documents. Invoices must be kept for seven years. Documents with respect to the employment of personnel must usually be kept for five years.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

Under the General Data Protection Regulation (GDPR), organisations must take appropriate technical and organisational measures to protect their processing of personal data, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity of these risks to potentially infringe the rights and freedoms of natural persons.

The Belgian Network and Information Security Act of 7 April 2019 (the NIS Act) transposed the EU Network and Information Security Directive 2016/1148 (the NIS Directive). In addition to the GDPR, the NIS Act adds a legal requirement for higher cybersecurity standards in respect of certain 'essential' services, such as energy (electricity, oil and gas), financial platforms, digital infrastructures (DNS services and domain name registrations) and transportation (air, rail, water and road). Importantly, certain digital services – such as online marketplaces, online search engines and cloud computer services – fall within the NIS Act's scope.

To ensure an adequate level of network and information security in these sectors and to prevent, handle and respond to incidents affecting networks and information systems, the NIS Act sets out the following obligations for the operators of essential services:

- to take appropriate technical and organisational measures to manage the risks posed to their network and information systems, and to prevent or minimise the impact in the event of a data breach; and
- to notify the competent authority, without undue delay, of all incidents with a 'significant impact' on the security of the core services provided by these operators. To assess the impact of an incident, the following criteria should be taken into account:

    - the number of users affected;

- the duration of the incident;
- the geographical spread with regard to the area affected by the incident; and
- in relation to certain operators of essential services, the disruption of the functioning of the service and the extent of the impact on economic and societal activities.

A new NIS 2 directive is currently under negotiation. One of most important changes will be the extension of its scope. This means that it will not only apply to essential sectors, but also to other important sectors, including additional digital infrastructures such as trust services providers.

## Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

With respect to data breach notifications, the Electronic Communications Act of 13 June 2005 requires companies in the telecommunications sector to notify immediately (within 24 hours) personal data breaches to the Data Protection Authority (DPA), which must transmit a copy of the notification to the Belgian Institute for Postal Services and Telecommunications. If there is a breach of personal data or the privacy of individuals, the company must also notify the data subjects affected by the breach. The NIS Act additionally provides for a detailed procedure regarding breaches for operators of essential services.

The GDPR provides for a duty for the data controller to report personal data breaches to the DPA without undue delay, and where feasible, not later than 72 hours after having become aware of a breach. This notification must describe the nature of the breach, communicate the contact details of the data protection officer or other contacts where more information can be obtained, explain the likely consequences of the breach and describe the measures taken or proposed to be taken by the controller to address the breach. A communication to the data subjects is in some cases necessary if there is a high risk to their rights and freedoms. The DPA stresses that, in the event of public incidents, it must be informed of the causes and damage within 48 hours after the data controller became aware of the breach.

## Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Article 46 bis of the Code of Criminal Procedure provides that the Public Prosecutor, in the detection of crimes and malpractices, may, by a reasoned and written decision, on the basis of any data in his or her possession or by means of access to the customer files of the actors, proceed to:

- the identification of the subscriber or habitual user of a service, or of the electronic means of communication used; and
- the identification of the services subscribed to or habitually used by that person.

To this end, the Public Prosecutor may, if necessary, issue a request through a police department or the Federal Computer Crime Unit. He or she may also request the cooperation of the operator of an electronic communications network.

Article 88 bis states that the investigating judge, when there are serious indications that the offences may result in a correctional punishment of one year or a more severe punishment, and when he or she considers that there are circumstances that make it necessary to have electronic communications traced or to locate the origin or destination of electronic communications in order to uncover the truth, can:

- cause the traffic data of electronic means of communication, from which or to which electronic communications are or were made, to be traced (essentially the IP addresses); and
- have the origin or destination of electronic communications traced.

A number of additional legal grounds on lawful access to data exist, including for the secret services in the Act of 30 November 1998 Governing the Intelligence and Security Services.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Belgium has a 'system of additional licences'. Only existing gaming establishments already licensed to operate games of chance in the real world (offline) can apply for an additional licence for the internet (online). Gambling is strictly regulated.

The Gambling Act requires a minimum age of 21 to play in a casino or slot machine hall, both offline and online. In addition, you are required to register for this purpose. To participate in either offline or online betting, the minimum age is 18. Certain professions are prohibited from accessing casinos and gaming arcades, for example magistrates. Also, certain persons can be placed in a database of excluded persons that must be consulted by gambling businesses before allowing customers to play. Online gambling businesses must impose compulsory game limits and include the possibility of temporary self-exclusion for customers, who must also be informed of the risks of online betting. Credit cards cannot be used to pay for online gambling services, nor can any credit or loan be provided.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Member states of the EU are free to define the level of protection on games of chance, as long as their national legislation complies with European law. They can restrict the cross-border supply of online gambling services on the basis of public interest objectives that they seek

to protect (eg, fighting fraud). Therefore, the exclusion of online gaming providers located in other member states is not a restriction on the free movement of services. The provision and use of the cross-border gambling offer falls within the scope of the fundamental freedoms of the Treaty on the Functioning of the European Union. A Belgian gambling licence will therefore rarely provide the possibility to provide services in another European Union member state.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Since the pandemic, the outsourcing of cloud computing services has boomed in Belgium. One of the most important concerns in this field remains privacy and cybersecurity, which must be extensively addressed in the outsourcing agreement. This is also necessary in other outsourced activities. If services are outsourced outside Belgium, and especially outside the European Union, the strict European rules on personal data transfers are likely to apply and cause issues that need to be addressed in a data processing agreement. Another crucial negotiation subject is an adequate service level agreement, which guarantees that the provider will sufficiently support the customer's outsourced services. If personnel are to be transferred together with the outsourcing, it is essential to obtain advice on the Belgian employment law in this area, as such transfers are strictly regulated, among others pursuant to the European Acquired Rights Directive. The customer must also pay attention to the exclusions and limitations of liability clauses in the outsourcing agreement. The inclusion of common law terminology such as 'indirect damages' does not correspond with Belgian law, which has separate rules on liability that must be carefully transposed in the agreement. The parties must also think of the exit arrangements, as a lack of them can cause major issues for the customer when the agreement is terminated for any reason.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

There are no specific regulations that would prohibit the outsourcing of digital business services. There are, however, specific rules on the outsourcing of activities by financial institutions and insurance companies that must be adhered to. For instance, the Act of 25 April 2014 on the Status and Supervision of Credit Institutions and Listed Companies states that the financial sector must take appropriate measures to limit the risks of outsourcing. Further European and national regulatory guidelines on outsourcing may apply in the financial sector.

## Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

Belgian law does not prescribe any specific terms for an outsourcing agreement, as the main principle is contractual freedom subject to the general rules of the Belgian Civil Code and the Code of Economic Law.

## Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

If a service is outsourced, there may be circumstances in which the EU directive on Transfers of Undertakings with Protection of Employment (TUPE) applies, namely, the Acquired Rights Directive (ARD). In Belgium, the ARD is incorporated by the Act of 5 December 1968 on Collective Bargaining Agreements and by the Collective Bargaining Agreement No. 32 bis (CBA 32 bis), which may apply if an asset and employee transfer takes place at the moment of the initial outsourcing, or if there is a change of supplier or a reverse transfer.

Belgian law will apply to any employee who usually executes their contract in Belgium, even if they are temporarily seconded to another country. If an employee does not execute their contract in one single country, the law of the country in which the employer is situated will apply.

All employees connected to the outsourced (transferred) activity must transfer, and will do so automatically, so that no new employment agreement is required with their new employer. A dismissal due to the transfer of undertaking is only possible for economic or technical reasons. Infringement may lead to additional compensation being due to the employees who were wrongfully dismissed.

The employer (transferor) must inform and consult its works council prior to making any official decision on an outsourcing that results in a transfer of employees. The works council must be informed regarding the reasons for the contemplated outsourcing and the consequences for the employees. There is only a duty to consult the works council, its consent is not required. The new employer (transferee) must also inform and consult its works council beforehand. Failing to inform and consult the works council can be sanctioned by a criminal fine.

If no works council (or trade union delegation) exists within the transferor, the employees concerned must be individually informed beforehand of the envisaged transfer date, the reasons for the transfer, the legal, economic and social consequences, and the intended measures that will affect the employees. In practice, the customer and the service provider will in most cases agree on a joint communication.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

No specific legislation has yet been adopted as regards artificial intelligence (AI), machine learning and big data in Belgium. It seems that the main focus is on researching the ethical questions with respect to the use of such technologies, the impact on society of which is as yet difficult to fully grasp. The upcoming European AI Regulation, which is currently being negotiated, will impact the industry and introduce certification mechanisms and other obligations for a range of high-risk AI systems. This could lead to more national laws on other AI systems that for now remain out of the European Regulation's scope.

Apart from this, article 22 of the General Data Protection Regulation (GDPR) must be kept in mind – this gives data subjects the right not to be subject to a decision based solely on automated processing if such processing will lead to a decision that produces legal effects or has a significant impact on the data subject. Data subjects have the right to request that the decision be reviewed by a human. Additionally, under Belgian law, the Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data prohibits a person from being made subject to the legal consequences of a decision that was taken based on automatic processing of personal data evaluating certain aspects of a person's personality.

Moreover, AI should be transparent to meet the principle of transparency under articles 13 to 15 of the GDPR. The data subject should know that automated decision-making (including profiling) exists in the processing of its data and, in such case, must receive meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing. Evidently, the AI systems themselves should also be designed in a way that secures processing of data and which only allows processing that is necessary for the organisation's legitimate goals.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

It depends on the type of data that are being used to train machine learning-based systems. Personal data will belong to the data subject and cannot thus be owned by, for instance, a developer of AI systems. The GDPR must be respected for any use of such personal data. A database containing personal data, in contrast, could enjoy protection by either or both of the following: (1) a specific sui generis right, protecting the content of the database, even if

it is not original, and subject to a number of strict conditions; (2) copyright law protecting the structure of the database, if it is original. Non-personal data may be owned and licensed contractually.

A work created by AI does not meet the current conditions for copyright protection. After all, no creative choices are made by the system. Also, the European Patent Office has rejected patent applications based on inventions with an AI system as inventor, as the latter should have a family name and thus be a natural person.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Answer in progress.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

A sales tax rate (VAT) of 0 per cent, 6 per cent, 12 per cent and 21 per cent applies in Belgium, depending on the product. The applicable rate for digital products and services is in principle 21 per cent. Income from digital products (such as speculation on tokens and crypto currency) may be taxed at 33 per cent on gains made, depending on the circumstances.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

The relevant criterion to determine whether or not a foreign company is active in Belgium depends on whether the activity concerned (such as placing a server, platform or metaverse) in Belgium can be seen as a 'permanent establishment'. The US concept of 'being engaged in trade or business' does not apply. The term 'permanent establishment' will depend on the circumstances of the activity and on the definition provided in the tax treaty between Belgium and the country of the foreign entity, if available. Generally, this is defined as the fixed place of business through which the business of an enterprise is wholly or partially carried on.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The content of an invoice is regulated by law, which also applies to electronic invoices. E-invoicing is generally allowed, provided that the customer agrees to receive its invoice electronically. It must further be made sure that the electronic invoice is authentic, readable and the integrity of its content is maintained. It is also important to take Belgian language rules into account: the invoice must be provided in the language of the region in which the company's seat is located (Dutch in Flanders, French in Wallonia, Dutch or French in Brussels). This language must also be maintained if an invoice is provided to another region within Belgium or outside the European Economic Area. Within the European Economic Area, a copy of the local invoice in another language will also be declared valid. In practice, multilingual invoices are often used.

Copies of the invoices need not be provided to the tax authority or other agency on a regular basis, but must be kept for at least seven years to remain available during tax inspections.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

No, ordinary courts or arbitration institutes (CEPANI) must be applied to online/digital issues and disputes.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

The Federal Public Service Economy has created the Belmed platform that facilitates alternative dispute resolution through the internet by bringing both parties together in a platform and also providing access to partners to act as mediator. Its scope is not limited to online/digital disputes. The parties can also engage qualified mediators or mediation institutions such as CEPANI. Various sectors, organisations and professional associations have also set up ADR bodies that can be involved in dispute resolution.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The world of digital technologies is growing exponentially and poses new challenges to existing legal frameworks due to the novel issues it creates. The European legislator has boosted efforts in recent months to cope with these rapid evolutions, proposing and introducing laws that will significantly impact digital transformation and online businesses. The AI Regulation, which is being negotiated, will be one of the first comprehensive global laws on artificial intelligence (AI), potentially clearing the way forward for other jurisdictions to regulate this technology as was the case for privacy with the General Data Protection Regulation. Although the AI Regulation will mainly govern 'high-risk' AI systems, it will put forward important principles (eg, the quality of data sets and transparency obligations) that could be applied similarly to other AI products. Certain jurisdictions may become inspired by these rules and also extend them voluntarily to other systems. The challenge will, however, be to establish a legal framework that equally safeguards innovation and does not generate excessive compliance costs, especially for small and medium enterprises such as start-ups. A future revision of the Product Liability Directive may tackle further issues with respect to the liability rooted in AI and Internet of Things systems.

Cybercrime continues to be a challenge for many countries, including Belgium. The revised NIS Directive (NIS 2), with an expanded scope of application, may further boost cybersecurity efforts from a legal standpoint. It remains unclear when another important piece of legislation, the ePrivacy Regulation, which will provide for more clarity regarding specific issues that may arise concerning privacy in connection with online interactions and electronic communications, will be agreed upon. Its purpose is to reinforce trust and security in digital services, while providing flexible regulatory tools to enable innovation. The ongoing negotiations mean that its implementation will again be delayed, until 2023 or later.

While a first agreement has been reached on the Markets in Crypto Assets Regulation, bringing the first crypto regulation in Europe into being, Belgium has introduced its own rules on crypto exchanges and wallets. It is expected to further regulate crypto advertising in the near future, and could even qualify crypto currencies as financial instruments, closing an opaque gap in law and leading to the direct applicability of important financial legislation to the issue and use of these virtual currencies.

Also, final agreements have been reached on the Digital Services Act and Digital Markets Act, which will govern, respectively, online intermediaries and platforms, as well as 'gatekeepers' in digital markets. These rules will significantly impact tech giants in a bid to increase competition in the digital market. It will be very interesting to see how effective the new rules are and whether they can revolutionise the sector.

The introduction of the above legislation in a way that also meets business interests and innovation can potentially make Europe indeed fit for the digital age – the European Commission's goal.

* *The information in this chapter was accurate as at 5 August 2022.*

Steven De Schrijver sds@agio.legal

Bist 47, Ekeren, Antwerpen B-2180, Belgium
Tel: +32 2 831 09 19
https://agio.legal/en

# China

Li Jiao and Jan Holthuis*
BUREN NV

RETURN TO CONTENTS

## Summary

**Read this article on Lexology**

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The Chinese government now pays attention to internet issues at an unprecedented level. Cybersecurity has officially become an important component of China's national security strategy. Internet legislation is at a higher level, with a wider field of application and a deeper degree of adjustment.

The Chinese government attaches weight to both state security and market-based regulatory systems.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

First, China has introduced several basic laws for cyberspace governance in recent years, including the E-Commerce Law, the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law. In the meanwhile, the supporting regulations of relevant departments are also being further improved, such as Cybersecurity Review Measures (2021) and Regulations for the Administration of Network Data Security (Draft for Comments).

Business on the internet is conducted under a licensing system in accordance with the Telecommunications Regulations. The Classification Catalogue of Telecommunications Services further defines and classifies the sub-categories of telecommunications business, according to which different types of telecommunications licences apply. Depending on the types, businesses on the internet may require, among others:

- an internet content provider licence;
- an online data processing licence; or
- a transaction processing services licence.

Related business operators can only conduct business after obtaining the corresponding licences.

In addition, conducting businesses on the internet shall also comply with legislation applicable to each specific industry and transaction model, such as the Electronic Signature Law, the Advertising Law 2021 and the Encryption Law.

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The Department of Electronic Commerce and Information Technology of the Ministry of Commerce is mainly responsible for supervising companies engaged in e-commerce business. As the main implementing department of the E-commerce Law, the State Administration for Market Regulation also plays a crucial role in the supervision of e-commerce operators.

In terms of data security protection, the Ministry of Public Security is mainly responsible for network security protection, while the Cybersecurity Administration of China and the Ministry of Industry and Information Technology (MIIT) are responsible for network security risk assessment. Internet access is also largely regulated by MIIT.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

For foreign-related disputes, including internet-related transactions or disputes, the courts will apply the Civil Procedure Law and Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law (Amendment 2022) (the Interpretation) to make decisions.

As stipulated in the Interpretation of the Civil Procedure Law, the parties involved can reach a consensus on the choice of jurisdiction of a foreign court in the place where the dispute is associated, as long as the choice of forum does not conflict with the provisions on court-level jurisdiction and exclusive jurisdiction.

In the absence of a choice of the parties, the jurisdiction should be determined in accordance with the provisions of the Civil Procedure Law and the Interpretation. For example, with respect to a contract dispute, the competent court shall be the people's court at the place where the defendant is domiciled or where the contract is performed.

The place of performance is further clarified by the Interpretation. If the subject matter is payment of money, the place where the party receiving the money is located shall be the place where the contract is performed; if the subject matter is delivery of immovable property, the place where the immovable property is located shall be the place where the contract is performed; as for any other subject matter, the place where the party fulfilling obligations is located shall be the place where the contract is performed. As for a contract with instant settlement, the place of transaction shall be the place where the contract is performed.

With regard to an online sales contract, when the subject matter is delivered through the internet, the place where the buyer is domiciled shall be the place of performance; if the subject matter is delivered by other means, the place of receipt is the place where the contract is performed.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There is no major difference between establishing a digital business and establishing a brick-and-mortar business in China. Most digital business operators shall complete market entity registration formalities, as stipulated in the E-commerce Law. The regulatory and procedural requirements that govern the establishment of digital businesses are as follows.

### Choosing business vehicles

To establish a business in China, the first question to be considered should be which business vehicles to choose. The main business vehicles in China include a limited liability company, a partnership and a company limited by shares. As for foreign-invested enterprises, establishing a representative office instead of a separate legal entity is also available.

### Pre-examination and approval procedures

The second step is to confirm whether the enterprise needs to go through the pre-examination and approval procedures. The pre-examination and approval procedures include three considerations:

- whether or not the project involves approval or filing according to the Administrative Measures on Approval and Filing for Foreign Investment Projects, and the Catalogue of Investment Projects Subject to Governmental Approval;
- whether or not the project is involved in the Administrative Measures (Negative List) for Foreign Investment Access; and
- whether or not a preliminary licence for entry into a specific industry is involved – this is not a pre-procedure aimed at foreign investment, but an administrative licence requirement for conducting business in specific industries or activities.

### Business registration

If the pre-examination and approval procedures are not required, or the approval documents have been obtained, investors can officially initiate the business registration procedures, including:

- business name registration: the name of a company is subject to pre-approval, and the pre-approved name will be reserved for six months; and

- after the company name is pre-approved, investors can submit documents to apply for registration and obtain a business licence through the local Administration for Market Regulation or the online enterprise registration system.

### Relevant identification certificates

After the registration is completed, the foreign-invested enterprise's information will be automatically synchronised to other departments. Investors should then complete the following procedures:

- carve and record official seals in the public security department;
- collect the invoice from the tax department;
- complete social security registration via the online platform;
- apply for foreign exchange registration with the foreign exchange administration department; and
- open a public account in a bank.

After completing these formalities, the enterprise shall check whether additional administrative licensing is required before starting its business.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

In general, parties can conclude a contract electronically in China. According to article 469 of the Civil Code, the parties may conclude a contract in writing, orally or in some other form. Any electronic data that can show, in material form, the contents that it specifies through electronic data exchange or email and can be accessed for reference and used at any time shall be regarded as a written form. Where the parties conclude a contract in the form of electronic data and subject to the execution of a letter of confirmation, the contract shall be established at the time of execution of the letter of confirmation. Where the information of any commodity or service released by one party via the internet or any other information network meets the conditions of offer, the contract shall be established when the other party selects such commodity or service and submits the order successfully, unless otherwise agreed by the parties.

Only certain types of contracts cannot be concluded electronically, such as documents related to personal relationships (marriage, adoption and succession), conveyance of rights and interests on real estate, and stay of public services.

If the contract is an online sales contract, a click-to-accept process can be adopted. As long as the online contract does not violate the provisions on validity of contract under Chinese law and is deemed a legally valid contract, the contract can be enforced in China.

For example, where a term in a contract unconditionally restricts the rights and interests of the parties to a 'click-wrap' contract, the term might be deemed unenforceable.

## Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

In the contract law section of the Civil Code, specific provisions are provided for the conclusion and performance of electronic contracts.

The E-Commerce Law is the main piece of legislation in China that regulates conduct of online business activities, including electronic contracts. The Electronic Signature Law is also applicable for online contracting. The Electronic Signature Law recognises that, under prescribed circumstances, electronic data messages can have the same legal effect as an original document or a written document.

In addition, the Process Specification for Online Conclusion of Electronic Contracts, a mandatory national standard approved and issued by the Ministry of Commerce in 2013, stipulates general process guidelines for e-commerce parties to follow when concluding electronic contracts via the internet in China.

## Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

In China, the Electronic Signature Law mainly regulates the conduct of electronic signature and confirms the legal validity of electronic signature. Parties involved in civil activities may agree to use, or not to use, electronic signature and data telex for contracts or other documents and instruments.

Electronic signature usually refers to data incorporated into or associated with any electronic form, which may be used to identify the signatory and indicate the signatory's approval of the information contained in the data telex. 'Data telex' means information generated, sent, received or stored by electronic, optical, magnetic or similar items.

Electronic signatures have the same legal validity as wet-inked signatures or affixation of seal, provided that the electronic signature has satisfied the conditions provided by law. Documents for which the parties involved agree to the use of electronic signature or data telex shall not be denied of legal validity on the ground of electronic signature or data telex being used. However, e-signatures cannot be used in documents or instruments related to personal relationships, conveyance of real estate and stay of public services.

At present, Chinese laws only regulate the form, function and effect of electronic signatures without specifying the specific technical means. Therefore, there is no unique format for electronic signature.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

Common remedies for breach of both electronic and offline contracts are the same, including specific performance, damages compensation, and other remedies.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

On 28 July 2015, 10 Chinese central regulatory agencies and industry regulators, including the People's Bank of China, the China Banking Regulatory Commission, the China Insurance Regulatory Commission and the China Internet Information Technology Office jointly released the Guiding Opinions on Promoting the Healthy Development of Internet Finance (the Guiding Opinions), which is the first comprehensive regulation issued by the Chinese government in relation to internet finance.

In the Guiding Opinions, the government set out general rules, basic rules and specific preferential measures relating to internet finance, covering internet payments, online lending, equity crowdfunding, internet fund sales, online insurance services and internet consumer finance.

In late 2021, Chinese financial regulators demanded fintech firms to rectify prominent issues, including:

- putting all financial activities under supervision;
- requiring that all financial businesses have a certificate; and
- cutting off the improper linkage between payment tools and other financial products.

Also, internet firms are required to strictly control the expansion of non-banking payment accounts to the public domain. They are also required to strengthen the management of key procedures, including the certification of shareholders, ownership structure and capital, risk isolation and related transactions.

Internet firms should also strengthen the protection mechanism of consumers, including regulating how personal information is collected and marketed, and the text of standard contracts.

## Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

### Electronic banking

The Electronic Payment Guidelines (No. 1), promulgated by the People's Bank of China (PBOC), is the first document that sets out banks' liability regarding online payment. The Measures for Management of Electronic Banking and the Guidance on Evaluation of Electronic Banking Security issued by the China Banking and Insurance Regulatory Commission generally govern the electronic banking business.

### Third-party payment

Third-party payment operators are defined as non-bank institutions that handle internet payments, mobile phone payments, fixed-line payments, digital television payments and other network payment services.

The regulator of third-party payment is the PBOC and its branches. The core of the policy is the Measures for the Administration of Payment Services by Non-Financial Institutions, supplemented by industry self-regulation and supervision by commercial banks. Due to the rapid development of third-party payments, the PBOC has introduced more policies to regulate third-party payments since 2014.

The promulgation of the E-Commerce Law in 2019 brought new requirements to electronic payment service providers, including requirements to:

- notify users of the functions of electronic payment services, use methods, points to note, the relevant risks and fee rates, etc;
- not impose unreasonable transaction conditions;
- ensure the integrity, consistency, trackability and resistance against tampering of electronic payment instructions;
- provide account reconciliation service and transaction records of the past three years to users free of charge;
- promptly investigate and identify the reason for errors in payment instructions, and adopt the relevant measures to correct the error; and
- bear compensation liability where an error causes the user to suffer losses, except where it can be proven that the error in the payment instruction was not caused by the electronic payment service provider.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

There are no particular rules to restrict developing or supplying crypto wallets or other methods of digitally storing value. However, for the time being, China has a strictly prohibitive

attitude towards the issuance and trading of crypto currencies. Financial institutes are forbidden from engaging in financing services and exchange of crypto currencies.

## Electronic payment systems

### 13 How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

There are mainly two types of electronic payments in China: online banking payment and third-party payment (Alipay, WeChat). Online banking payment is regulated by the Electronic Payment Guidelines (No. 1) issued by the People's Bank of China in 2005. The guidance clarifies the obligations of banks when using electronic payment (which include the application of electronic payment, the initiation and receipt of electronic payment instructions and the measures of safety control and error handling).

Third-party payment like Alipay and WeChat is in widespread use from metropolis to remote countryside in China. Third-party payment institutions are now under the regulation of the People's Bank of China and its subordinate units. In 2017, the People's Bank of China issued a total of 106 administrative penalty decisions against third-party payment institutions, many of whom were blamed for not being adherent to the administrative measures issued by the People's Bank of China. Besides, with respect to the conditions for third-party payment institutions carrying out business and their business practices, new normative documents in draft version have set up more strict and comprehensive requirements, including but not limited to anti-monopoly regulatory measures, higher paid-up capital and account classification management.

Third-party access to digital information in bank accounts is subject to regulation under the Civil Code, the Personal Information Protection Law, the Commercial Banking Law and the Consumer Rights and Interests Protection Law, as well as departmental regulations such as the Implementation Measures of the People's Bank of China on the Protection of the Rights and Interests of Financial Consumers. Third-party access to personal bank account information requires the individual's consent, with the exception of requirements by law-enforcement departments.

In addition to the laws, the Technical Specification for the Protection of Personal Financial Information provides a technical standard for financial institutions entrusting the processing of personal financial information to third parties. It stipulates that the entrustment should not exceed the scope of the consent of the subject of the personal financial information. And it places more detailed demands on the entrusted third-party institution.

## Online identity

### 14 Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Pursuant to the China Anti-Money Laundering Law, where a financial institution determines the identity of a customer through a third party, it shall ensure that the third party has

adopted measures for determining customer identity complying with the requirements of this Law. And where the third party has not adopted measures for determining customer identity that comply with the requirements of this Law, the financial institution shall bear the liability of not fulfilling the obligation of determining customer identity. Generally, Chinese law permits the use of third parties to satisfy KYC requirements. In 2022, the People's Bank of China released a regulation requiring financial institutions to assess third parties' risk status and ability to perform the obligations of AML and counter-terrorist financing.

Nevertheless, when it comes to customer identity for credit card applications, the Notice on Further Promoting the Standardised and Healthy Development of Credit Card Business promulgated by the China Banking and Insurance Regulatory Commission and the People's Bank of China stipulates that banking financial institutions shall accept credit card applications, collect customer information and verify customers' identities via their own channels, instead of relying on an internet platform, webpage or any other electronic channel operated or controlled by any cooperative agent. In cases of inquiries regarding bills or payables via the aforesaid electronic channels, prior consent should be obtained from customers and necessary measures must be taken to ensure the security of customers' personal information.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

To take ownership of a domain name, applicants for registration shall register (purchase) the possible domain name from the China Internet Network Information Centre (CNNIC) or the qualified registrars accredited by the CNNIC that then shall provide an electronic certification.

There are no filing formalities for domain names in China. However, applicants who use the registered domain name for a website shall fulfil the website filing formalities with the competent department, according to the Administrative Measures on Internet-based Information Services.

It is possible for a resident to register a country-specific domain name in China without that resident being in China. In China, a country-specific domain name refers to a .cn or a .中国 domain name. The Implementing Rules for the Registration of National Top-level Domain Names 2019 provide that no restriction is imposed against non-residents to register a .cn or a .中国 domain name. Additionally, the Ministry of Industry and Information Technology also specifies the permitted registrants, either individuals or entities.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

The Anti-Unfair Competition Law defines the unauthorised use of the main part of another party's domain name, website name, web page, etc, that is influential as misleading acts, which may cause the public to misidentify the goods concerned as another party's goods or to associate the goods concerned with those of another party. Only domain names or URLs that are influential are protected by the Anti-Unfair Competition Law.

In accordance with the Interpretations of Several Issues Concerning the Application of Law to the Trial of Civil Dispute Cases Involving Computer Network Domain Names from the PRC Supreme People's Court (SPC), the registration or use of domain names – which includes but is not limited to copying, imitating or translating well-known trademarks or being identical with or similar to registered trademarks or domain names – may also constitute infringement and thus be regulated by the Trademark Law.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

The governing rules are the following.

Legislation: the Advertising Law 2021, as amended.

Administrative regulations:

- the Administrative Measures for Internet Advertising 2023; and
- the Provisions on the Governance of Network Information Contents Ecosystem 2019.
- Self-regulatory codes: the China Advertising Association is the industrial self-discipline association for advertising, which formulated and promulgated self-regulatory codes for the advertising industry (eg, the Self-Regulation of the China Advertising Association and the Self-Discipline Pact).

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Online advertising is defined as commercial advertisements that directly or indirectly promote goods or services through websites, web pages, internet applications and other internet media in the forms of texts, pictures, audios, videos, etc.

Online editorial content can be regarded as online advertising provided that there is a paid promotion of goods or services, directly or indirectly, for profit. According to the Advertising Law 2021, commercial advertising shall involve the activities carried out by sellers of goods or service providers to promote their goods or services, directly or indirectly, through a certain medium and form. Therefore, editorial content shall be caught by the rules governing advertising only if it can meet this condition.

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

The rules against misleading online advertising are mainly set forth in Anti-Unfair Competition Law 2019, the Advertising Law 2021 and the Administrative Measures for Internet Advertising 2023.

Under the Advertising Law 2021, a wider variety of advertisements are now vulnerable to scrutiny for false advertising. Advertisers are now required to substantiate all claims and statements regarding their truthfulness to avoid non-compliance. The use of technical or digital methods to create or enhance the true effect of a product or service in advertisements, in particular, is penalised as false advertising.

In accordance with article 13 of the Administrative Measures for Internet Advertising 2023, the advertiser shall be liable for the truthfulness of the contents of an internet advertisement.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

General rules in the Advertising Law 2021 include that the following shall not be advertised:

- narcotic drugs;
- psychotropic substances;
- toxic drugs for medical use;
- radioactive pharmaceuticals and other special drugs;
- drug precursor chemicals; and
- pharmaceuticals, medical machinery and treatment methods for drug abuse rehabilitation.

Prescription drugs other than those stipulated in the above list may only be advertised in medical or pharmaceutical professional journals that are jointly designated by the health department of the State Council and the drug regulatory department of the State Council.

Special rules in the Administrative Measures for Internet Advertising 2023 state that it is prohibited to design, produce, act as agents for or publish on the internet any advertisements for goods or services the production, sales or provision of which are prohibited by laws and administrative regulations, or any advertisements for goods and services that are prohibited from being published. It is also prohibited to publish advertisements for prescription drugs and tobacco via the internet.

Read this article on Lexology

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

Email, SMS and other distance marketing are supervised by the Administrative Measures for Internet Advertising and the Advertising Law.

Unsolicited marketing is not allowed in China. The Administrative Measures for Internet Advertising and the Advertising Law explicitly prohibit advertisers from attaching advertisements to, or including advertising links in, replies to emails sent by users without their permission.

Also, the Advertising Law regulates the sending of advertisements by means of electronic messages, requiring any entity or individual to obtain the consent or request of the person concerned before sending the advertisement, and to provide the recipient with a means to refuse to continue receiving the advertisement after it has been sent. Otherwise, the advertiser shall be subject to administrative liability, which includes orders for corrections and fines.

The Administrative Measures for Internet Advertising 2023 further specify that no advertisements or links to advertisements shall be attached to emails or internet instant messaging, and no internet advertisements shall be sent to users' vehicles, navigation devices, smart home appliances, etc, without the consent or request of the person concerned. Otherwise, advertisers, operators and publishers of advertisements shall bear administrative liabilities, which include orders for corrections, confiscation of illegal income and imposition of fines.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Article 45 of the Advertising Law 2021 stipulates that internet information service providers shall curb the posting and publishing of illegal advertisements through their information transmission and distribution platform of which they are aware or should be aware.

For any violation of these provisions, the State Administration for Market Regulation shall confiscate the illegal income. Where the amount of the illegal income is 50,000 yuan or above, a fine ranging from one to three times the amount of the illegal income shall be imposed simultaneously. Where the amount of the illegal income is less than 50,000 yuan, a fine ranging from 10,000 to 50,000 yuan shall be imposed simultaneously. In serious cases, the relevant authorities shall order the offender to stop the relevant businesses.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

The internet service provider (ISP) shall not bear liability for infringement when the relevant copyright owner fails to issue a warning or provide any other information that is sufficient to make the ISP aware of such an infringement. The necessary measures taken by the ISP include the technical approaches that may directly prevent the occurrence of infringement consequences, such as deleting infringing content, breaking links and filtering keywords.

After receiving the notice, if the ISP still does not remove the infringing link within a reasonable period resulting in the further expansion of the damage, it will bear the legal responsibility for such additional damages.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Shutting down a web page containing defamatory material could be one of the requisite measures according to article 1,195 of the Civil Code. It is an ISP's obligation to take requisite measures if the injured party sends a notice of infringement to the ISP, providing the preliminary evidence of infringement and its true identity information. With respect to which specific requisite measure or measures shall be taken, the ISP shall, based on the preliminary evidence for infringement and the type of services, make the decision accordingly.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

There is no express law that stipulates that all data and databases are protected by IP law. In general, only the data and databases formulated or perceived in an original manner can be granted copyright and thus protected. In accordance with article 127 of the Civil Code, data and internet virtual property are protected based on other regulations, if any. Generally, data and databases are not the objects of civil rights in Chinese law, and have limited protection as objects of IP rights. The Anti-Unfair Competition Law offers protection as data and databases can be defined as trade secrets, trademarks, etc.

## Third-party links and content

### 26 Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Legal practice in China deems that the link itself does not contain any content and therefore is not subject to the control of the right to network dissemination of information. The Supreme People's Court published the Provisions on Several Issues Concerning the Application of Law to Trial of Civil Dispute Cases of Infringement of the Right to Network Dissemination of Information, stipulating that the internet service provider (ISP) whose conduct constitutes joint infringement with other parties shall bear joint and several liabilities, but also providing an exemption for the ISP if it only provides a link.

However, for built-in deep linking behaviour, it is a different case. Deep linking is a technical means that allows users to directly see the content of the linked website on the linking website without a webpage transition.

### 27 Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Where a network user or an ISP provides works, performances, and audio and video products via an information network without the permission of the right holder for network dissemination of information, such provisions shall be deemed an infringement of the rights to network dissemination of information. Meanwhile, making available works, performances, and audio and video products in the information network by means of uploading to a network server, setting up shared files or using file-sharing software, etc, that enables the general public to download, browse or by other means obtain them at any desired time and location shall be deemed constitutions of the aforesaid provisions.

## Metaverse and online platforms

### 28 Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

The legislation for the metaverse and virtual property is still under development. At the current stage, intellectual property protection in the metaverse faces a few difficulties.

First, the rules for evidence collection and burden of proof concerning infringement of intellectual property rights (IPR) in the metaverse are unclear. For instance in commercial practice, virtual reality (VR) service providers usually only conduct formal review and ignore substantive review, leading to the problem of copyright infringement where many VR applications are copied illegally.

Second, the general laws applied for IPR infringement may become inapplicable for IPR infringement in the metaverse. For example, 'without the consent of the trademark registrant, replaces his registered trademark and puts the goods with the replaced trademark back on the market' is stipulated as an act of trademark infringement according to the

Trademark Law. However, it becomes difficult to identify such acts since only virtual products, not physical objects, exist in the metaverse.

Third, according to the current IPR protection law system, a trademark is only protected within the territory where the trademark is registered. However, in the metaverse, the territoriality of IPR protection may be challenged.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

The principle of exhaustion of rights has been recognised by PRC law in some areas.

For example, in new plant variety rights protection, the Supreme People's Court proposed that, after the variety right-holder authorises or licenses the plant variety material to be sold, it shall not claim that the production, propagation or sale of such plant material by others constitutes infringement (exceptions apply). Similarly, the PRC patent law stipulates that once the patented products are sold by the patentee or its licensee, the use, offer for sale, sale and importation of such products no longer constitute infringement of the patent right.

Regarding digital products, the Copyright Law and Regulations on Computer Software both indicate that for legally distributed copies of software, the right-owner's distribution right has been exhausted.

In April 2022, the PRC's first non-fungible token (NFT) infringement case was decided by Hangzhou Internet Court. The judgment denied application of the principle of exhaustion of rights for NFT digital products. It reasoned that the principle is based on the inseparability of the work itself and its tangible carrier. Since the distribution of NFT digital works does not lead to the distribution of their tangible carriers, NFT digital works do not meet the prerequisite to apply the exhaustion of rights principle.

In addition, the original purpose of the exhaustion of rights principle is to balance the conflict of interests between the copyright owner and the legitimate buyer, but NFT digital works can be copied without cost and in unlimited quantities, so unauthorised duplicates and distribution would seriously harm the interests of the copyright owner.

This case is a preliminary exploration of Chinese justice in the field of the metaverse. As discussion over the topic grows, more authoritative legislation is expected in the near future.

## Administrative enforcement

### 30 Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

The term 'dawn raid' is not directly incorporated into Chinese law, but the most similar existing concepts are administrative or criminal investigations (inspections), which allow law enforcement to conduct on-site inspections as well as search corporate records and files to gather information and evidence on suspected violations of law.

In administrative procedures, which are usually initiated by a complaint filed by the IP right holder, the competent administrative authorities – such as the Copyright Bureau in a case of copyright infringement – do not have the power to issue a freezing injunction. However, in terms of dawn raids, the administrative authorities may, when investigating the suspected infringement;

- question the relevant parties;
- investigate the matters relating to the alleged illegal acts;
- conduct on-site inspections of premises and articles of the parties concerned that involve alleged illegal acts;
- inspect and make copies of contracts, invoices, account books and other relevant materials relating to the alleged illegal acts; and
- seal up or seize the premises and articles involving the alleged illegal acts.

## Civil remedies

### 31 What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Civil remedies rendered in a civil judgment may include ordering the infringers to stop infringement, eliminate impact, apologise or compensate losses to IP owners.

Search orders and freezing injunctions are available under different circumstances. Freezing injunctions are available as a preservation measure before and during the litigation.

After the civil judgment comes into effect, the IP owner may file an application for enforcement with the enforcement division of the court.

If the infringer does not perform the obligations ordered in the civil judgment, the court shall have the right to enquire about the infringer's properties and issue freezing injunctions. If the infringer does not perform the obligations ordered in the civil judgment and conceals its properties, the court shall have the right to issue a search order signed by the president of the court. The court shall also have the right to conduct a search on the infringer and its residence or the place where the property is concealed.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

The Personal Information Protection Law (PIPL), effective as of 1 November 2021, defines personal information and personal data as:

> *all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously. The processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure and deletion, etc. of personal information.*

Sensitive personal information refers to the personal information that is likely to result in damage to the personal dignity of any natural person, or damage to his or her personal or property safety once disclosed or illegally used, including information such as biometric identification, religious belief, specific identity, medical health, financial account, whereabouts and previous location history, as well as the personal information of minors under the age of 14.

Additional rules apply to the processing of sensitive personal data including, subject to the individual's separate consent (written consent is required in some cases), the need to inform the individual of the necessity of processing his or her sensitive personal information and the impact on his or her personal rights and interests. The consent of a minor's parents or other guardians in the case of processing the personal information of a minor under the age of 14 must be obtained.

Information processed anonymously is currently not regulated.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

The Cyberspace Administration of China (CAC) is the competent authority for leading and coordinating the supervision of personal information processors. Meanwhile, other government departments including the Ministry of Industry and Information Technology, the Ministry of Public Security and the State Administration for Market Regulation (SAMR) are responsible for protecting, supervising and administering the protection of personal data within the scope of their respective duties. Currently, there is no regulatory registration system designed for personal information processors. However, this does not mean personal information processors in China can avoid supervision.

The Personal Information Security Standards 2020 regulate the personal information protection officer system. Where a personal information processor meets any of the below thresholds, it shall designate a personal information protection officer:

- if it processes personal information as its main business and has more than 200 employees;
- if it processes the personal information of more than one million people or expects to process the personal information of more than one million people within the next 12 months; or
- if it handles the sensitive personal information of more than 100,000 people.

## Extraterritorial issues

### 34 Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The PIPL shall apply to all processing activities of personal information that occur in China. The PIPL also applies to the processing activities of personal information that occur outside China if:

- the purpose of such processing activity is to provide products or services to a natural person within China; or
- the activities of the natural person within China are analysed and evaluated.

Where a personal information processor needs to transfer personal data outside China, it shall:

- get the certificate issued by a specialised agency appointed by the CAC;
- pass the security evaluation organised by the CAC; and
- enter into a contract with the overseas recipient under the standard contract formulated by the CAC.

In addition, the personal information processor shall take necessary measures to ensure that the overseas recipient also satisfies Chinese standards.

Foreign national residents within China will also be protected by the PIPL.

## Bases for processing

### 35 What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

With globalisation and the booming of the internet economy, there are many scenarios in which enterprises transfer domestic personal information across borders to foreign countries. The following are the most commonly seen:

- global enterprises require their subsidiaries, branches or representative offices in the PRC to transfer management information, such as personal information of employees, to the headquarters abroad;
- companies collect personal information during business operations in the PRC, and then share it with their foreign parent companies;
- cross-border e-commerce operators store personal information on servers outside the PRC, or outsource their personal information processing to companies abroad;
- cross-border service providers, such as of insurance, medical care, tourism and study consultancy, collect personal information in the PRC and store it on a server abroad or provide it to foreign companies; and
- enterprises provide investigation and evidentiary materials involving personal information to offshore government departments and parent companies, for the purpose of anti-fraud investigations, offshore litigation and arbitration bodies.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

The Security Assessment Measures for Outbound Data Transfers came into effect on 1 September 2022. Meanwhile, the Personal Information Protection Law, Data Security Law and Cybersecurity Law supervise the export or transfer of personal data to another jurisdiction.

Under the Security Assessment Measures for Outbound Data Transfers, to provide data abroad under any of the following circumstances, a data processor must declare a security assessment for its outbound data transfer to the Cyberspace Administration of China (CAC) through the local cyberspace administration at the provincial level:

- where a data processor provides critical data abroad;
- where a key information infrastructure operator or a data processor processing the personal information of more than one million individuals provides personal information abroad;
- where a data processor has provided personal information of 100,000 individuals or sensitive personal information of 10,000 individuals in total abroad since 1 January of the previous year; and
- in other circumstances prescribed by the CAC for which declaration for security assessment for outbound data transfers is required.

According to the security assessment result, the CAC may rule the data provider to terminate the data export.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

In accordance with article 10 of the PIPL, no organisation or individual may illegally buy or sell the personal information of others. Shanghai Data Regulation expressly indicates that natural persons, legal persons and other organisations may conduct data trading in compliance with the laws and regulations. Pudong New District has set up a data exchange for the convenience of data trading, and transactions are encouraged to be secured there.

Accordingly, the transaction of data products that contain personal information shall face strict review. The consent of individuals must be obtained in advance, and such individuals must be informed of the name of the receiver, the aim of the transfer, and how the receiver will handle the information, among others.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

The right to personal information mainly includes the following subsidiary rights:

- The privacy disposition right: the right of a person to directly control and dominate his or her personal data. The person also has the right to decide whether, and in what manner, purpose and scope, his or her personal data will be collected, processed and used.
- The privacy secrecy right: the right of a person to request that information be kept confidential by the information processing subject.
- The inquire right: the right of a person to enquire about his or her personal information and the processing thereof, and to request a response. The control of information must begin with knowing what personal information is collected, processed and used, and whether the information is kept complete, correct and up to date in the process.
- The correct or supplement right: the right to request the subject of information processing to correct and add to personal information that is incorrect, incomplete or, from time to time, new.
- The deletion right: the right to request the information processing subject to delete personal information for legal or agreed reasons.

The protection of personal information is applicable to the activities of processing the personal information of natural persons in China and applies to the principle of territoriality, without distinguishing by nationality.

## Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

In China, there is no specific law that regulates the use of non-personal data. The flow of data from China to other jurisdictions should be approved by the relevant authorities if the

data reach the threshold specified by article 4 of the Security Assessment Measures for Outbound Data Transfers, which doesn't distinguish between personal data and non-personal data.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

China encourages and supports the digitisation of archives. The general law governing document retention, the Archival Law, does not require any particular document or record types to be kept in original paper form and not converted solely to a digital representation. Instead, it emphasises that electronic archives and archives carried in traditional forms have the same legal effect, and in the case of digitalised archives, the original archives shall be properly kept.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

The National Archives Administration of China formulates regulations for different authority systems, stipulating minimum retention periods or permanent retention for different types of documents.

For example, the National Archives Administration of China and the Supreme People's Court collaboratively promulgated the Measures for the Administration of Litigation Archives of the People's Courts in 2013, which stipulate three retention periods: at least 20 years, at least 60 years and permanent retention. Those litigation archives with long-term value for investigation and utilisation shall be classified as permanent retention, such as those pertaining to cases with a death sentence. Those litigation archives with relatively long-term value for investigation and utilisation shall be classified to be kept for at least 60 years, such as those pertaining to cases with fixed-term imprisonment sentences of five to 15 years. Those litigation archives with short-term value for investigation and utilisation shall be classified to be kept for at least 20 years, such as those pertaining to cases with fixed-term imprisonment sentences of less than five years.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

#### E-commerce business operators

The E-Commerce Law sets out the following requirements which should be met by E-commerce business operators:

- collect and use the personal information of their users compliant with the provisions of laws and administrative regulations on the protection of personal information;
- adopt technical measures and other requisite measures to ensure the secure and stable operation of their network, prevent cybercrime activities, deal with cyber security incidents effectively, and ensure the security of e-commerce transactions; and
- formulate cyber security incident emergency plans, and forthwith trigger the emergency plans upon the occurrence of a cyber security incident, adopt the corresponding remedial measures, and report to the relevant competent authorities.

#### Internet service providers

The Cybersecurity Law provides more requirements for internet service providers (ISPs) to ensure the security of internet transactions. ISPs must:

- provide network products and services satisfying the mandatory requirements in the applicable national standards;
- not install malware;
- immediately take remedial action against any risk such as security defects or bugs that are found, inform users of the risk and report the case to the competent authority;
- provide consistent security maintenance for the ISP's products or services;
- expressly notify and obtain the consent of users if the products or services provided by the ISP collect user information; and
- comply with provisions of the Cybersecurity Law as well as the relevant laws and administrative regulations governing the protection of personal information if the personal information of users is involved.

Network operators must develop an emergency plan for cybersecurity events to promptly respond to security risks such as system bugs, computer viruses, network attacks and network intrusions. For an event that threatens cybersecurity, the operator concerned must initiate the emergency plan, take corresponding remedial actions and report the event as required to the competent authority.

Network operators shall take technical and other necessary measures to ensure the security of the personal information that it collects, and to protect such information from disclosure,

damage or loss. In cases of disclosure, damage or loss (or possible disclosure, damage or loss) of such information, the network operator shall take immediate remedial action, notify users in accordance with the relevant provisions and report to the competent authority.

Network operators shall strengthen the management of the information released by their users. If the operator finds any information that is prohibited by laws and administrative regulations from release or transmission, it shall immediately cease transmission of such information and take measures such as deletion to prevent the dissemination of such information. The operator shall also keep a relevant record and report the case to the competent authority.

Encryption is not a mandatory security measure.

## Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Both the Cybersecurity Law and the PIPL regulate that, in the case of a data breach, the network operator (ie, the information processor) shall be obliged to take immediate remedial actions, notify the users and report to a competent authority.

Currently, there is no detailed data breach notification system specific to e-commerce that is regulated by laws and regulations.

## Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

There is no specific rule on whether authorities can require private keys to be made available. However, according to article 31 of the Cryptography Law, cryptography administrations, related authorities and the staff thereof shall not require commercial cryptography-related agencies and commercial cryptography testing or certification agencies to disclose their source codes or other proprietary cryptography-related information.

Certification authorities are permitted and operate under a licensing system. Certification authorities can only provide service after going through the approval of the Ministry of Industry and Information Technology (MIIT) and the Ministry of Commerce. For the provision of an electronic authentication service without a licence, MIIT will order the providers to stop the illegal act and illegal income (if any) shall be confiscated.

Encrypted communications are mainly regulated under the Electronic Signatures Law, the Cryptography Law and the Administrative Measures on Electronic Certification Services.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

The Chinese mainland is staunchly opposed to gambling. Both online and offline gambling are illegal, with both being punishable by criminal penalties and detention.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Online betting is illegal in China. Advertising and providing access to online betting with earnings of not less than 20,000 yuan constitute a joint offence with the crime of running a casino.

As for operation of a gaming business in another jurisdiction, PRC laws require the operator to obtain authorisation from the copyright owner, and approval from competent copyright administrative departments and provincial publication bureaus. Unapproved advertisement or access services will be curbed, the operator's internet service will be stopped and its website shut down. Operation without legal authorisation from the game's copyright owner will be investigated by the National Copyright Administration. Serious infringement of copyright may constitute a criminal offence.

Regarding gaming businesses on the metaverse, clarifying legislation is yet to come. However, since the metaverse is closely intertwined with virtual currency, whose legitimacy has been denied by existing regulation, metaverse gaming in China faces considerable difficulties. Operations relevant to virtual currency could constitute the criminal offences of, for example, fund-raising fraud or illegally engaging in fund payment and settlement business.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

#### Agreement

When choosing the provision of services on an outsourced basis, an enterprise shall try to avoid direct personnel management, including signing any written agreement with outsourced employees or paying salaries and social insurance premiums. Instead, the enterprise should sign standardised outsourcing agreements with its outsourced services provider.

### Qualification

The outsourced services provider shall possess corresponding qualifications if the outsourcing business involves qualification requirements.

### Business secrets

Enterprises shall not assign outsourced employees to core positions that may have access to the business secrets of the enterprise.

### Tax

If an outsourced service provider is qualified for the recognition of advanced technology-based service enterprises in terms of employee qualifications, sources and percentages of revenue, it will be entitled to tax incentives.

## Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

In general, outsourcing of digital business services is allowed and encouraged. A few particular digital financial services are prohibited from outsourcing, such as the following:

- Risk management of commercial banks accepting loaning applications online. According to the rule, commercial banks must strengthen their responsibilities regarding risk control. Banks shall independently carry out risk management of loans operated through internet platforms, and complete the whole risk management process, which has important impacts on loaning risk assessment and risk control. It is strictly prohibited to outsource the key links of loaning management at any time, including pre-loan, in-loan and post-loan.
- Information technology of banks, asset management companies and insurance institutions, which is related to the financial institution's core competitiveness, shall not be outsourced.

## Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

It is provided in the Measures for the Risk Supervision of Information Technology Outsourcing of Banking and Insurance Institutions that the following contents in information technology outsourcing contracts or agreements shall be specified (including but not limited to):

- Service scope, service content, service requirements, working time limit and arrangement, responsibility allocation, delivery requirements, relevant restrictions in follow-up cooperation, and agreement on service quality assessment and evaluation.

- Requirements for compliance, internal control and risk management, compliance with laws and regulations and internal management systems of banking and insurance institutions, and notification and implementation mechanism for regulatory policies.
- Service continuity requirements – the service continuity management objectives of service providers shall meet the business continuity objectives requirements of banking and insurance institutions.
- The right of banking and insurance institutions to conduct risk assessment, monitoring, inspection and auditing of service providers, and service providers undertake to accept the supervision and inspection of the outsourcing services of banking and insurance institutions undertaken by the China Banking and Insurance Regulatory Commission.
- Triggering conditions for contract modification or termination, and transitional arrangements for contract modification or termination.
- The ownership of relevant information and intellectual property rights in outsourcing activities, as well as the content and scope that service providers are allowed to use, and the requirements for service providers to use legal software and hardware products.
- Resource guarantee clauses.
- Security confidentiality and consumer rights protection agreements, including but not limited to:

    - prohibiting service providers from using or disclosing the information of banking and insurance institutions beyond the scope permitted by the contract; and
    - service providers shall not transfer or misappropriate the data of banking and insurance institutions in any form, or seek benefits other than those agreed in the outsourcing contract.

- Dispute resolution mechanism, breach of contract and compensation clauses. Cross-border outsourcing should specify the applicable law and jurisdiction for dispute resolution. In principle, Chinese arbitration institutions and Chinese courts should be selected for jurisdiction, and Chinese laws should be applied to resolve disputes.
- Reporting terms, including at least the content and frequency of regular reports, reporting routes, reporting methods and time-limit requirements in case of emergencies.

What is more, the banking and insurance institutions shall expressly require in the contract or agreement that service providers shall not subcontract outsourced services or subcontract them in disguised form. When it comes to subcontracting outsourced services, the contract or agreement shall include the following terms:

- not to subcontract the main business of outsourcing services;
- the main service provider is generally responsible for the service level and ensures that the subcontracted service providers can strictly abide by the outsourcing contract or agreement; and
- the main service provider monitors the subcontracting service providers and fulfils the obligation of notification or report approval for changes of subcontracting service providers.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

Generally speaking, in the company, the benefits related to salary, annual leave and promotion of outsourced employees might be inferior to regular employees. In terms of the rights of employees (such as severance or consultation) under Chinese employment law, there is no legal distinction between outsourced and regular employees.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

In 2017, the State Council of China issued the New Generation Artificial Intelligence Development Plan (the Plan), providing administrative guidance for artificial intelligence (AI) from the perspective of industrial policy promotion, support and development. Following the Plan, the National New Generation Artificial Intelligence Governance Professional Committee was established, which has issued the Governance Principles for New Generation Artificial Intelligence – Developing Responsible Artificial Intelligence (2019) and the Ethics Norms for New Generation Artificial Intelligence (2021).

On the basis of the above rules, the following requirements are imposed for use of AI:

- The AI developers shall:
    - strengthen self-discipline in all aspects of technology research and development;
    - improve data integrity, timeliness, consistency, standardisation and accuracy;
    - improve transparency and reliability in algorithm design, implementation and application; and
    - avoid possible data and algorithm biases in data collection.
- The AI suppliers shall:
    - abide by rules on market access and competition, and avoid infringement of intellectual property (IP) rights;
    - strengthen the quality monitoring and use evaluation;
    - inform users of the functions and limitations of AI products and services, and protect users' right to know and consent; and
    - respond to and process user feedback in a timely manner, and formulate emergency mechanisms and loss compensation plans or measures.

- The AI users shall:

  - use in good faith;
  - avoid improper use and abuse of AI products and services, and avoid unintentional damage to the legitimate rights and interests of others;
  - not use AI products and services that do not comply with laws, regulations, ethics and standards, and prohibit the use of AI products and services to engage in illegal activities;
  - provide timely and proactive feedback on issues such as technical security loopholes, policy and regulation vacuums, and regulatory lag found in use; and
  - improve usability to ensure safety and efficient use of AI products and services.

In accordance with the Ethics Norms, suppliers are recommended to conduct quality monitoring and use evaluation of AI products and services to avoid undue harm. As for the supervision mechanisms of AI, in July 2023, the Cyberspace Administration of China issued Provisional Measures for the Administration of Generative Artificial Intelligence Services, which is the first supervisory regulation in China regarding artificial intelligence.

## IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Currently, there are no specific rules concerning IP and AI or machine learning. Therefore, such issues are still under general regulation of IP laws, such as the Copyright Law, Trademark Law and Patent Law.

In practice, the protection by IP rights for AI or machine learning remains controversial.

### Under the Patent Law

Article 25 of the Patent Law stipulates that 'scientific discoveries, rules and methods of intellectual activities, etc shall not be granted patent rights'. In the field of AI, the innovation of algorithms is the core of every invention and creation at the technical level. Whether pure algorithms belong to 'the rules and methods of intellectual activities', and whether they can be patented, is controversial. The Announcement stipulates that if a claim contains technical features in addition to algorithmic features or features of business rules and methods, then the claim, as a whole, is not rules and methods for mental activities, and shall not be excluded from patentability. Whether the provision will further help AI be protected under the Patent Law is unclear.

### Under the Copyright Law

Products generated by AI without human participation, based on current laws, cannot be regarded as works protected by the Copyright Law.

**Read this article on Lexology**

### Under the Anti-Unfair Competition Law

Commercial secrets refer to technical information, business information and other commercial information that is not known to the public, has commercial value and has been kept secret by the obligee. Therefore, as the core of AI enterprises, algorithms also have great commercial value, and enterprises usually take strict confidentiality measures to keep the algorithms secret. The Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases of Infringement of Trade Secrets also clarifies that the people's courts can protect algorithms as trade secrets. Therefore, AI might be protected in this way.

China has no special laws or regulations on the ownership of IP created by AI or machine learning systems. However, in a judgment rendered in 2020, Nanshan Primary People's Court, Shenzhen, Guangdong recognised that the works generated by Dreamwriter, an AI robot developed by Tencent, constituted works protected by the Copyright Law, and Tencent, as a legal entity, owned such copyrights. This precedent became one of the 'Top 10 Cases in 2020' certified by the Supreme People's Court, which indicates its value as guidance concerning such ownership.

## Ethics

### 53 Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

The Provisional Measures for the Administration of Generative Artificial Intelligence Services came into effect on 15 August 2023.

The Measures stipulate that when providing and utilising generative AI (GAI) services, the laws and regulations shall be complied with, as well as social moral principles and ethics, which include:

- Conforming to socialistic core values, and not generating content that incites subversion of the state power or the overthrow of the socialistic system, endangers national security and interests, damages the national image, incites separatism, undermines national unity and social stability, propagates terrorism, extremism, ethnic hatred and discrimination, violence, pornography, and false and harmful information.
- Taking effective measures to prevent discrimination in terms of nationality, religion, country, region, gender, occupation, health, etc, in the process of algorithm design, training data selection, model generation and optimisation, service provision, etc.
- Respecting intellectual property rights and commercial ethics, protecting trade secrets, and not committing acts of monopoly and unfair competition with the advantages of algorithms, data, and platforms.
- Respecting the legitimate rights and interests of others, not endangering others' physical and mental health, and not infringing upon others' rights of portrait, reputation, honour, privacy or personal information.
- Taking effective measures in light of the characteristics of different types of services to boost the transparency of GAI services and the accuracy and reliability of content generated.

It is worth noting that both the service providers and the users are obligated to comply with the ethics. In fact, the requirements mainly concentrate on the role of GAI service providers as content producers who thus undertake duties of compliance under the Cyber Security Law and other administrative regulations.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

In general, tax is imposed whenever a transaction takes place, whether online or offline. However, in Chinese tax law practice, virtual product transactions between individuals or between individuals and companies are exempt from value-added tax (VAT) if they do not reach the tax threshold. For individuals who cannot provide evidence of the original value of their property, the competent tax authorities shall approve the original value of their property.

For transactions between companies in China, the seller company shall pay tax in accordance with Chinese tax law. As for cross-border virtual products between companies, China's current practice is that foreign companies that provide virtual product services must set up a standing body in China or cooperate with a domestic entity in China. The authorities will impose VAT on the standing body or cooperative entity. There will also be a tax imposed on for-profit businesses from China.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

If the servers installed overseas by a domestic company are used solely for offshore websites, such servers will not be subject to taxes in China. Nevertheless, if such servers are installed abroad and still engaged in network business related to China or the offshore companies send professionals to provide technical services in China the domestic company receiving services shall withhold the taxes and surcharges.

If an offshore company placed servers in China and receives revenue from China through such servers, that portion of the revenue related to China is subject to taxes.

Where there are special agreements on tax collection of cross-border income in tax treaties or agreements signed between China and an overseas country or region, the domestic company may opt to apply the preferential tax rate in the tax treaties or agreements.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

E-invoicing has been generally implemented in China. In 2015, China started to implement e-invoicing for VAT regular invoices, and in 2020 started to implement e-invoicing for VAT special invoices.

China implements a uniform format for e-invoicing. As of 2019, the national standard Electronic Invoice Based Information Specification came into effect, stipulating the uniform format and required information for e-invoices.

The State Administration of Taxation has built a nationwide unified e-invoice service platform. Issuance of e-invoices are synced on the platform, and thus there is no need to submit copies of e-invoices to the State Administration of Taxation.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

China has established three internet courts in Beijing, Hangzhou and Guangzhou. These courts specialise in internet-related cases online, all of which are located in the most booming and prosperous areas of China's internet industry. These internet courts are skilled in hearing disputes arising from contractual disputes over online shopping or services and underrate financial loans, as well as online copyright disputes and internet-related public interest litigation, among others. Most of the evidence in the cases heard by internet courts is in the form of electronic data and is stored on the internet.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

For online or digital disputes, ADR is a very common practice in China. E-commerce platforms such as Alibaba and JD.com have set up their own ADR platforms and most consumers are accustomed to solving online shopping contractual disputes through such platforms.

For example, on Alibaba, when a consumer is dissatisfied with goods or services online, the consumer usually submits evidence and negotiates with the supplier first. After the consumer submits the dispute, the two parties have three to 30 days to negotiate without the involvement of the e-commerce platform itself. If the supplier provides a different proposal,

the consumer could request Alibaba's assistance by clicking the 'escalate dispute' button or may continue to negotiate with the seller.

In general, the ADR platforms of businesses are more inclined to protect the interests of consumers.

However, some consumers will directly seek the help of the official ADR platform, which is the 12315 platform. The 12315 platform is a hotline that is directly affiliated with the State Administration for Market Regulation (SAMR). In addition, at a local level, many SAMR offices have also established their own separate complaint channels in the form of hotlines or social media accounts.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The most manifest progress in data law is the release of the Provisional Measures for the Administration of Generative Artificial Intelligence Services (the Measures) issued by the Cyberspace Administration of China and seven other national institutions on 10 July 2023. It is the first legal document that regulates artificial intelligence (AI) in China.

The Measures settle the basic principles for generative AI (GAI), which include the principle of tolerance and prudence and the principle of regulation based on classifications. It supports the development of AI from the aspect of compliance and lays the foundation for the coming Artificial Intelligence Law.

The Measures consist of five chapters. Chapter 2, article 7 of the Measures stipulates mandatorily that when service providers conduct data training activities, they must comply with certain requirements, such as using data and basic models from lawful resources, not infringing on intellectual property rights, and obtaining consent of the individual when personal information is involved.

Besides regulation of the use of data, the Measures also clarify the role of service providers as producers of internet information, which means they are obligated to fulfil the duties of cyber security as stipulated in the Cyber Security Law and the Provisions on the Ecological Governance of Network Information Content. Generally, the Measures intentionally leave space for deeper and wider development of GAI and the regulatory policy is still in the phase of exploration.

* *The authors would like to thank Yijie Jiang and Kaixuan Shang, Deken Shanghai Law Firm and Zining Zhou, Buren N.V., for their assistance with this chapter.*

BUREN
LEGAL | TAX | NOTARY

Li Jiao l.jiao@burenlegal.com
Jan Holthuis j.holthuis@burenlegal.com

Zhong Yu Plaza Room 1602, North Gongti Road 6, Beijing 100027, China
Tel: +86 10 852 357 80
www.burenlegal.com

# Cyprus

Anastasios A Antoniou, Ifigenia Iacovou and Orestis Anastasiades
Antoniou McCollum & Co LLC

RETURN TO CONTENTS

## Summary

**Read this article on Lexology**

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

Recent years have seen substantive policy initiatives aimed at digital transformation. At the core of recent policy initiatives is the creation of the Deputy Ministry of Innovation, Research and Digital Policy. The Deputy Ministry developed the digital strategy for Cyprus up to 2025, which is currently being implemented. Updated regulatory frameworks are now in place to govern online business and transactions.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

A wide range of statutes and regulations governs the following domains:

- the provision of digital content and digital services into Cyprus;
- electronic commerce and aspects of electronic commercial contracts;
- the conclusion of online consumer contracts;
- the protection of consumers when purchasing products and services online;
- the conclusion of contracts of the sale of products online;
- the provision of electronic communications services into Cyprus;
- the security of network and information systems (cybersecurity); and
- personal data protection.

### Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The Ministry of Energy, Commerce and Industry is competent for the supervision and effective enforcement of the regulatory framework concerning electronic commerce.

The competent authority for the enforcement of the personal data protection framework in Cyprus is the Commissioner for the Protection of Personal Data (the DPC). The DPC assesses potential infringements of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)) and Cypriot data protection laws, whether on its own initiative or following a complaint, and can impose sanctions on finding an infringement.

The Communications Commissioner (the CC) is the competent authority in Cyprus for the regulation of Internet access in Cyprus. The CC is competent to safeguard an open Internet and ensure consumers of electronic communication services in Cyprus are protected.

The CC also has the power to determine applicable charges and tariffs, including the minimum and maximum tariff thresholds to ensure fair competition, transparency and cost-effectiveness between electronic communications. On finding an infringement of the applicable framework, the CC can impose administrative fines or other sanctions.

The Department of Electronic Communications is a department in the Deputy Ministry of Research, Innovation and Digital Policy, and oversees the national broadband plan of Cyprus.

The Digital Security Authority (the DSA) is competent for the implementation and enforcement of the applicable framework concerning network and information systems security. The DSA is tasked with receiving reports of any cybersecurity incidents by service providers and operators to which the relevant framework applies and to ensure that service providers and operators take appropriate measures to prevent and minimise the impact of incidents affecting the security of networks and information systems. The DSA also supervises the national CSIRT (CSIRT-CY) and ensures that it has access to appropriate, secure and robust communications and information infrastructure at national level, and ensures cross-border cooperation with competent authorities in other jurisdictions.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

EU rules apply to disputes involving defendants selling goods or services from an EU member state to Cyprus. Subject to exceptions, the default position is that defendants domiciled in an EU member state shall, regardless of their nationality, be sued in the courts of that member state. Cypriot courts have consistently applied the EU rules on jurisdiction, including with respect to online transactions.

The rules of jurisdiction may, under certain circumstances, apply to parties domiciled outside the EU, such as the parties to a contract agree that the courts of an EU member state should have jurisdiction. Online traders often use standard terms and conditions and a jurisdiction clause in such standard terms and conditions may satisfy the requirement to confer jurisdiction of the courts of a particular EU member state.

Restrictions apply with respect to sales of goods or services or the provision of digital content to a consumer in Cyprus. A consumer is able to bring proceedings in the courts of Cyprus, rather than those where the digital business is domiciled.

The above rules have not yet been tested in respect of transactions in the metaverse by Cyprus courts.

### Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

Establishing a business in Cyprus to provide services online may require authorisation from competent authorities in certain industries. Such industries include payment services, financial services, banking services, insurance services and electronic communications.

With respect to digital content, establishing a media service provider or a video-sharing platform provider is subject to relevant regulatory authorisations.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Yes, contracts can be concluded digitally, between businesses (B2B), between businesses and consumers (B2C) and in a non-commercial context. Cyprus law recognises the digital conclusion of contracts.

The consumer protection framework applies to consumer contracts, in which cases mandatory information, language and other formalities must be adhered to by the trader, both at a pre-contractual stage and in the trader's terms of sale.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

The seller of goods or services online must provide the purchaser, whether a business or a consumer, with some key information. Such information includes the governing law of the contract and the languages offered for the conclusion of the contract.

With respect to consumers in particular, online traders must provide certain information in Greek (or in the language of choice of the consumer where the trader agrees to such choice of language). Such information includes, where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it.

While the terms of a contract can specify laws other than the laws of Cyprus to govern an online contract, a consumer cannot be deprived of the protection afforded under Cyprus consumer protection legislation where the foreign governing law offers a lower level of protection.

## Electronic signatures

### 8 How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Electronic signatures in Cyprus are regulated by the applicable EU framework and national implementing legislation. The Department of Electronic Communications of the Ministry of Transport, Communications and Works of the Republic of Cyprus (the DEC) is the competent authority for the implementation and enforcement of the applicable framework on electronic signatures in Cyprus.

The types of electronic signatures recognised under Cyprus law are the following:

- An electronic signature, which is defined as data in electronic form that is attached to or logically associated with other data in electronic form and that is used by the signatory to sign.
- An advanced electronic signature, which is defined as an electronic signature that meets the following requirements: it is uniquely linked to the signatory; it is capable of identifying the signatory; it is created electronic signature creation data that the signatory can, with a high level of confidence, use under his or her sole control; and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
- A qualified electronic signature, which is defined as an advanced electronic signature that is created by a qualified electronic signature creation device and that is based on a qualified certificate for electronic signatures.

A qualified certificate for electronic signatures for the purposes of the qualified electronic signature, is issued by a qualified trust service provider. A qualified electronic signature will have the equivalent legal effect of a handwritten signature.

## Breach

### 9 Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

There are no special forums for a case of breach of a digital contract. Subject to jurisdictional rules, Cypriot courts can hear claims alleging breaches of digital contracts.

In relation to consumer contracts, consumers can use the Online Dispute Resolution platform provided by the European Commission for the online resolution of disputes between consumers and businesses. Submission of complaints is usually carried out though the national contact points.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

In the absence of passporting of an investment firm's licence from another EU member state into Cyprus, advertising or selling financial services products in Cyprus may be subject to authorisation by the Cyprus Securities and Exchange Commission (CySEC). CySEC may impose administrative sanctions for breach of licensing or passporting requirements and criminal liability may also become relevant in cases of unauthorised financial services activities in Cyprus.

Where banking or payment services are provided in breach of the respective licensing or passporting requirements in Cyprus, the providers involved may be subject to administrative sanctions that can be imposed by the Central Bank of Cyprus.

Marketing communications addressed by an investment firm to clients or potential clients must be clearly identifiable as such and be fair, clear and not misleading. Certain key requirements applicable to direct marketing of financial services are the following:

- an opt-in requirement applies to unsolicited communications;
- using electronic contact details already provided by the client to directly market a provider's similar products or services should take place only where the client is clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and with every future instance of marketing communication; and
- direct marketing emails are prohibited if they disguise or conceal the identity of the sender and do not include a valid address to which the recipient may send a request for ceasing such communications, or that encourages recipients to visit websites.

Under Cypriot consumer protection legislation, misleading and aggressive commercial practices carried out by any consumer-facing business would constitute unfair commercial practices, which are prohibited under the Consumer Protection Law. These rules will also apply to the advertising of financial services via the internet.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

The Central Bank of Cyprus is the competent authority for the authorisation and supervision of electronic money services providers in Cyprus. Issuing electronic money is an activity that can only be carried out in Cyprus inter alia by authorised credit institutions and electronic money institutions. Electronic money services may also be offered from within Cyprus by electronic money institutions authorised under the laws of another EU member state, under the right of establishment and the freedom to provide services.

**Read this article on Lexology**

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Providers of crypto wallets may be subject to authorisation by CySEC, depending on their precise activities. Activities that require CySEC's authorisation include the following:

- reception and transmission of client orders in crypto-assets;
- execution of orders on behalf of clients in crypto-assets;
- exchange between crypto-assets and fiat currency or between crypto-assets;
- participation in or provision of financial services related to the distribution, offering or sale of crypto-assets, including the initial offering;
- placement of crypto-assets without firm commitment;
- crypto-asset portfolio management;
- administration, transfer of ownership, transfer of site, holding, or safekeeping, including custody, of crypto-assets or cryptographic keys or means enabling control over crypto-assets;
- underwriting or placement of crypto-assets with firm commitment; and
- operation of a multilateral system, which brings together multiple third-party buying and selling interests in crypto-assets in a way that results in a transaction.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Payment institutions can engage in carrying out the operation of payment systems. The Central Bank of Cyprus (the CBC) is the competent authority for the authorisation and supervision of payment services providers in Cyprus, including payment systems.

Under the provisions of the law, payment systems cannot impose on, inter alia, payment service users (ie, payers of payees) any of the following requirements on access:

- restrictive rules for effective participation in other payment systems;
- any rules discriminating between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants; or
- any restrictions on the basis of institutional status.

Payment systems are only permitted to process personal data when it is necessary to safeguard the prevention, investigation, detection and prosecution of payment fraud. Any processing must be carried out in accordance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)). Any access, processing and retention of users' personal data necessary for the provision of the payment services, can only take place with the consent of end customers (ie, payment service users).

### Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

The Central Bank of Cyprus (CBC) is the competent authority for AML and KYC requirements in respect of providers of banking services, payment services and electronic money institutions. The Cyprus Securities and Exchange Commission (CySEC) is respectively tasked with supervising providers' investment services with respect to the AML and KYC requirements that they apply to their business relationships and transactions.

The CBC and CySEC issue subsidiary legislation to regulate AML and KYC requirements pursuant to the provisions of national AML legislation. Cyprus law has transposed the EU AML directives (including Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing).

Reliance on third parties for the implementation of procedures for customer identification and due diligence measures must be done where the third parties are themselves regulated and supervised in accordance with the requirements of applicable law. Nevertheless, the service provider remains liable for compliance with the applicable law at all times, and such liability is not subject to delegation to any third party.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

The country code top-level domain (TLD) name for Cyprus is '.cy'. The competent regulatory authority is the Communications Commissioner (CC). The University of Cyprus (UCY) was appointed by the CC to regulate to handle the .cy TLD, including licensing.

The .cy TLD is divided into several secondary level (Level-B) domain names, each of which describes a specific service. Depending on the type of activities, a company or organisation may opt to be registered with a secondary domain name.

Applicants from any country can apply for a .cy domain name.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

The right to use a .cy domain under a licence granted by the UCY does not confer copyright or trademark-related rights. In considering an application for the registration of a domain name, the UCY does not investigate whether the applicant is the right holder of any rights on the name included in the domain name or is otherwise authorised to use such name. The domain name applicant is responsible to ensure that the name applied for does not infringe the intellectual property of any other party.

The registration of a domain name may be subject to challenge by a third party claiming rights over the domain name due to ownership of a trademark. A third party may apply to the UCY for the revocation of any decision of the UCY to assign a right to use or register a domain name, proving ownership of the trademark.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

An online advertisement to Cypriot users must:

- be clearly identifiable as a commercial communication; and
- clearly identify the person on whose behalf the commercial communication is sent.

If the communication is unsolicited, it must be clearly and unambiguously identifiable as such, as soon it is received.

Rules concerning misleading and aggressive advertising also apply to online advertising to consumers in Cyprus.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

The framework on targeted advertising and online behavioural advertising in Cyprus applies to cookies, bots and any technology that collects, has access to, shares, processes or monitors one or more identifiers or technical equipment of a subscriber or user.

Automated individual decision-making, including profiling is governed by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)).

Under the GDPR, a data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them unless such decision is necessary for entering into, or performance of, a contract between the data subject and a data controller or unless such decision is based on the data subject's explicit consent. However, the controller must implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. In any event, the data subject must have the right to object at any time, to the processing of personal data for profiling purposes.

Information on cookies must be 'clear and comprehensive'. The user must clearly provide their consent to the use of cookies by a website. Mere information that a website uses cookies and that users automatically accept cookies by browsing the website, does not meet the statutory requirements. Consent must be given in the form of an affirmative action. In particular, the Commissioner for the Protection of Personal Data (the DPC) highlights in the DPC Guidance that consent cannot be implied from use of the website and indicates that it must be clear that a user has actively engaged with a cookie banner to unambiguously consent to use of cookies.

Where cookie banners are used, they must not indirectly force a user to accept all cookie; both accept and reject options should be clearly provided on the banner. Also, due to the voluntary nature of consent, where the user is not able to access the service or website in the absence of express consent to cookies, this would mean that the website does not present the user with a genuine choice, therefore it cannot be deemed valid consent as it is not freely given.

Nevertheless, the requirement of the user's consent for the use of cookies is not required:

- for technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network ('communications exemption'); or
- as strictly necessary to provide an information society service explicitly requested by the subscriber or user ('strictly necessary exemption').

The validity period of consent would depend on various factors, including whether the purposes of processing have changed and the period for which the personal data will be stored that the controller shall be determined and communicated to the user.

While the framework does not provide for a specific retention period for cookies, if the collected data constitutes personal data, the provisions of the GDPR must be complied with and such data must not be kept for longer than necessary for the purposes for which the personal data are processed.

'Dark patterns' are also relevant to targeted advertising and online behavioural advertising. Dark patterns, defined by the European Data Protection Board as interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. Dark patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices. The data protection principles applicable to dark patterns are those set out in article 5 the GDPR.

**Read this article on Lexology**

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

Misleading and aggressive commercial practices carried out online by any consumer-facing business would constitute unfair commercial practices, which are prohibited.

Advertisers should make sure that any advertisement as well as its overall presentation and any statements used for commercial reasons do not include any false information and all statements used in the commercial communication are true and verified. The advertisement should also not omit any essential information that the consumer would need, to make an informed decision on the transaction.

Advertisers should keep a record where possible of proof of any market surveys carried out to determine the average consumers views and expectations as to the specific product advertised. Furthermore, any reference to the product's price should be supported by records of price calculations leading to the advertised price. Generally, any competitive claim must be substantiated with relevant evidence. These rules apply to all advertising directed towards consumers. At the same time, specific rules apply to certain industries – for example, electronic communications.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

Audiovisual commercial communications displayed online by media service providers and video-sharing platform providers that fall under the jurisdiction of Cyprus are subject to a wide range of restrictions, whether they concern digital or other products. Several restrictions apply for the protection of minors, such as the prohibition of advertising that may harm minors. Additional restrictions are applicable to prevent any advertising that includes or promotes discrimination based on sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation, encourages behaviour prejudicial to health or safety, encourages behaviour grossly prejudicial to the protection of the environment.

Regarding specific products, it is prohibited to advertise cigarettes and other tobacco products, electronic cigarettes and medicinal products and medical treatments available in Cyprus on prescription. Alcoholic beverages advertisements must not be aimed specifically at minors and shall not encourage immoderate consumption of such beverages.

## Direct email marketing

### 21 | What regulations and guidance apply to email, SMS and other direct marketing?

The following apply with respect to unsolicited marketing communications, including emails:

- prior consent of the recipient for direct marketing communications is required (including via email, SMS and automated calling); and

- using electronic contact details already on file to directly market a provider's similar products or services may take place only where the recipient is clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their details at the time of their collection and with every future instance of marketing communication.

Marketing communications addressed to consumers must have the consumer's prior consent as to the means of communication. Direct marketing emails that disguise or conceal the identity of the sender, and which do not include a valid address to which the recipient may send a request for ceasing such communications, are not allowed.

Where personal data is processed for direct marketing purposes, the data subject will have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Under article 21 of the GDPR, where the data subject objects to processing for direct marketing purposes, any further processing of the data subject's personal data for such purposes would constitute a breach of the provisions of the GDPR.

In the context of banking, credit, insurance, investment or payment services, the consumer's prior consent is required before a service provider performs distance communication techniques using automated calling systems without human intervention.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Where a content provider or a party that is merely hosting content has no actual knowledge of illegal content and is not aware of facts or circumstances from which such activity is apparent, the safe harbour defence is available and the content provider or hosting party may be exempt from liability. Under Cyprus law internet service providers (ISPs) are exempt from liability for content that is hosted on their sites. Liability may occur in the event the host has actual knowledge or awareness of facts or circumstances in which illegal content is apparent. Once such knowledge or awareness is obtained; the host provider must meet takedown or shutdown obligations.

The safe harbour defence may not be strong when invoked in respect of content over which the ISP has editorial control. A case-by-case assessment of the precise facts and circumstances is necessary to determine whether the safe harbour defence can successfully be invoked by any party.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

A digital platform or online content provider may be liable under Cyprus law for mistakes in information that it publishes online where this information would cause a consumer to make a purchasing decision that they would not have taken otherwise. Such mistakes in information may also lead to liability where they are found to amount to misleading advertising – that is, where these are found to affect the economic behaviour of consumers or to be detrimental to a competitor. Liability for such mistakes in information may occur by virtue of the failure to meet information requirements that are imposed by the relevant legislative framework on consumer protection and electronic commerce.

Liability may be mitigated through the use of notices to delimit the reasonable expectations of the recipient of the information. However, liability cannot be excluded where information is clearly and unambiguously misleading.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Online content providers or ISPs may shut down web pages containing defamatory material without court authorisation.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

Data and databases enjoy general copyright protection under the law. Databases, in particular, enjoy such general copyright protection where the selection or arrangement of their contents constitutes the creator's own intellectual creation. Moreover, the database is subject to a specific, sui generis type of intellectual property right allowing the creator of such database to prohibit the unauthorised extraction or reuse of its contents.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Linking to third-party websites or platforms without permission may, under certain circumstances, constitute an infringement of intellectual property rights. The established legal precedent on this matter suggests a case-by-case, individualised approach in

determining whether linking constitutes an infringement. Relevant considerations that are assessed include:

- whether the communication is for profit;
- whether the right holder of the intellectual property has initially provided consent for the linked content and the level of care undertaken to confirm this;
- whether the link to the content allows users to circumvent restrictions that make the content accessible to subscribers only; and
- whether the illegal nature of the content has been notified by the right holder.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Under current Cyprus law, using third-party content that is obtained via automated scraping or otherwise, without permission from the third-party content provider, may constitute an infringement of copyright or other intellectual property rights.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Copyright and database protection would arise for both the computer programs through which a metaverse is operated and for works created in such metaverse. When the metaverse allows users to create works (ie, it is an 'open' metaverse), such works would be protected by copyright. Difficulties are expected when pursuing infringement proceedings with respect to copyright or database rights on a metaverse, as the identity of the infringer may be difficult to ascertain.

As trademarks present a strong territoriality element with respect to their protection, enforcement actions may face difficulties in establishing a potential infringement of a trademark on a metaverse, to the extent it cannot be ascertained which jurisdiction's trademark protection rules would apply.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Exhaustion of rights is recognised in Cyprus. The distribution right in the EU is only exhausted if the first sale or other transfer of ownership in the EU is made by the copyright owner or with their consent. The exhaustion of rights does not generally apply to downloadable digital content for permanent use and right holders may be able to restrict resales of such digital content.

### Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Police authorities may carry out searches in private premises under a search warrant when investigating IP infringements that may involve a criminal offence. Freezing injunctions are generally available by Cypriot courts with respect to IP infringement, when the relevant conditions are met.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

IP owners can pursue remedies for infringement of their IP rights, including damages. When applicable requirements are met, IP owners may be able to apply to court for search orders or freezing injunctions, as well as orders for the destruction or delivery of the copies that infringe copyright, the tools used and an order for account of profits achieved as a result of the infringement.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

The personal data protection framework in Cyprus comprises:

- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)); and
- the Protection of Natural Persons against Processing of Personal Data and the Free Movement of such Data Law of 2018 (L.125(I)/2018) as amended (the Law).

The competent authority responsible for the enforcement of the GDPR and the Law in Cyprus is the Commissioner for the Protection of Personal Data (the DPC).

The definition of 'personal data' under the Law reflects the definition of personal data under article 4 the GDPR.

Special categories of personal data are protected in Cyprus under the provisions of article 9 of the GDPR. Such categories include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Under the GDPR there is an express prohibition on the processing of special categories of personal data, save for specific exceptions, including where the data subject has given their explicit consent to such processing for specific purposes. The Law prohibits the processing of genetic and biometric data for the purposes of health and life insurance. Also, where processing of such personal data is based on explicit consent, any further processing requires a separate consent.

Personal data provided on an anonymised basis would generally not constitute personal data for GDPR purposes. Pseudonymisation would, under specific circumstances, be deemed an alternative to anonymisation where it has the effect of removing 'personal data'. Where pseudonymised data still lead to an identifiable individual under the circumstances, pseudonymisation would not have the effect of anonymisation.

## Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

No registration is required prior to the processing of personal data under Cyprus law.

Article 37 of the GDPR specifically requires the designation of a data protection officer where:

- processing of personal data is carried out by a public authority or body (irrespective of what data is being processed);
- the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The GDPR applies to:

- controllers and processors that process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place within the EU; and
- non-EU controllers and processors with no EU establishment that offer goods or services to individuals in the EU or monitor the behaviour of individuals in the EU.

Business that are not established in the EU but to which the GDPR applies must designate, in writing, a representative in one of the EU member states in which data subjects are affected by the processing concerned. This requirement will not apply if the controller is a public authority or body. This requirement will also not apply if:

- the processing is occasional or it constitutes large-scale processing of special categories of personal data or criminal convictions and offences; and
- is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope, and purposes of the processing.

## Bases for processing

### 35 What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

Processing personal data is lawful when carried out on one of the grounds provided for under article 6 of the GDPR.

Commonly invoked bases for processing personal data include:

- consent given by the data subject to the processing of their personal data for specific purposes;
- where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; and
- where processing is necessary for the legitimate interests pursued by the controller.

Any processing of personal data must be in line with the Protection of Natural Persons against Processing of Personal Data and the Free Movement of such Data Law of 2018 (L.125(I)/2018) as amended (the Law) and the GDPR. The competent authority responsible for the enforcement of the GDPR and the Law in Cyprus is the Commissioner for the Protection of Personal Data (the DPC).

Under the GDPR there is an express prohibition on the processing of special categories of personal data, save for specific exceptions, including where the data subject has given their explicit consent to such processing for specific purposes. The Law prohibits the processing of genetic and biometric data for the purposes of health and life insurance. Also, where processing of such personal data is based on explicit consent, any further processing requires a separate consent.

No additional restrictions apply with respect to transfers of personal data within the EU. However, as the carrying out of the personal data transfer will in all cases constitute processing of personal data, the GDPR principles relating to lawful processing will still apply.

The transfer of personal data to a country for which an adequacy decision has been issued by the European Commission may be performed without restrictions. If there is no adequacy decision for a third country, for a third-country personal data transfer to be lawful, personal data must be sufficiently protected by way of standard contractual clauses, binding corporate rules, European Commission-approved codes of conduct, or by way of certification of the data processing procedure.

In the absence of an adequacy decision or appropriate safeguards, article 49 of the GDPR may be invoked to permit a data transfer to a third country on the basis of a derogation. Such derogations would include:

- explicit consent by the data subject after being informed of the data transfer risks due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- the transfer is necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- the transfer is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent;
- the transfer is necessary for important reasons of public interest or to establish, exercise or defend legal claims;
- the transfer is made from a public register that is intended to provide information to the public and specific conditions are fulfilled; and
- the transfer is in the controller's legitimate interests.

A transfer of personal data to a third country based on a derogation requires carrying out an impact assessment and prior consultation with the DPC.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Personal data may be transferred to a third-country jurisdiction only in compliance with the applicable provisions of the GDPR.

The transfer of personal data to a country for which an adequacy decision has been issued by the European Commission may be performed without restrictions. If there is no adequacy decision for a third country, for a third-country personal data transfer to be lawful, personal data must be sufficiently protected by way of standard contractual clauses, binding corporate rules, European Commission-approved codes of conduct, or by way of certification of the data processing procedure.

The transfer of special categories of personal data – that is, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation – to a third country may, under certain circumstances, require prior consultation with the Data Protection Commissioner of Cyprus, which is legally empowered to impose restrictions on such transfer. In this respect, an impact assessment may also be required.

There are no data sovereignty or national security rules that require data, data servers or databases to remain in Cyprus.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

Sales of personal data to third parties would involve a transfer of personal data. Transfers of personal data are regulated by the GDPR. Any transfer of personal data by either a controller or a processor to any third party will under any circumstances constitute processing of personal data. No additional restrictions apply to the sale of personal data, provided that the requirements of the GDPR for such processing are complied with.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Cypriots and non-Cypriots are afforded the same protection under the GDPR and the Protection of Natural Persons against Processing of Personal Data and the Free Movement of such Data Law of 2018 (L.125(I)/2018), as amended (the Law), when their personal data is processed in Cyprus.

Key rights under the GDPR are the following:

- Right of access – right to obtain information from the controller as to whether or not his or her personal data are processed, the envisaged period for which the personal data will be stored, the purpose for which they are processed, any recipients and as to his or her rights under the GDPR. The Commissioner for the Protection of Personal Data (the DPC) has clarified that the right of access is provided to individuals free of charge. The DPC also advises the controller to respond to such request for access at least within one month from receipt of such request.
- Right to rectification – right to obtain without undue delay the rectification of inaccurate personal data concerning him or her.
- Right to erasure ('right to be forgotten') – right to obtain the erasure of personal data concerning him or her without undue delay. When an individual exercises this right and the personal data are no longer necessary in relation to the purposes for which they were collected or processed, or there is no longer a legal ground for processing after the data subject withdraws his or her consent, or they have been unlawfully processed or they have to be erased for compliance with a legal obligation of the controller, or they have been collected in relation an information society services offering, then the controller must erase the data without undue delay.
- Right to restriction of processing where the accuracy of the personal data is contested by the data subject.
- Right to data portability – right to receive the personal data concerning him or her in a machine-readable format and to transmit such data to another controller without hindrance from the controller or to transmit such data directly from one controller to another, where processing is based on consent or on the performance of a contract and the processing is carried out by automated means.

- Right to object, at any time, to processing, on grounds (e) or (f) of article 6(1) of the GDPR, of personal data concerning him or her, including profiling based on those provisions. Following the exercise of this right, the controller can only process the personal data if it demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- Right to lodge a complaint with the competent authority responsible for the enforcement of the GDPR and the Law in Cyprus – ie, the Commissioner for the Protection of Personal Data.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

Non-personal data in Cyprus is regulated at EU level. Main EU level regulation governing the use of non-personal data is Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. There is currently no other specific local law governing non-personal data usage in Cyprus.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Under the laws of Cyprus, digital representations of documents or record types are afforded the same evidentiary value as their original paper form counterparts. As such, there is no requirement to keep any particular document or record types in original paper form.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Documents or other record types that are collected for the purposes of compliance with anti-money laundering legislation must be retained for at least five years after the end of a business relationship with the customer or the conclusion of a one-off transaction. For tax compliance purposes, documentation and other records relevant to the calculation and imposition of taxation in Cyprus should be kept for up to seven years. Furthermore, considering the statutory limitation periods for bringing a civil claim under Cyprus law, which periods vary depending on the nature of the claim, it is advisable that documents or other record types that may be linked to a potential claim are kept for up to 10 years.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

Cyprus law provides for precautionary measures that should be taken by providers of publicly available electronic communications services to avoid data breaches and ensure cybersecurity. Such minimum precautionary measures require that providers must:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and
- ensure the implementation of a security policy with respect to the processing of personal data.

Essential services providers and critical infrastructure providers must implement measures relating to the annual risk assessment of their network information systems, their business continuity plans and disaster recovery plans, their compliance with standards adopted at EU level and ensure the business integrity of their networks.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Data breaches and relevant notification requirements are regulated under article 33 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)). The GDPR is supplementary to the Cyprus Law on Protection of Natural Persons against Processing of Personal Data and the Free Movement of such Data of 2018 (L.125(I)/2018) as amended (the Law). The national competent authority responsible for the enforcement of the GDPR and the Law in Cyprus, which accepts data breach notifications, is the Commissioner for the Protection of Personal Data (the DPC).

A controller must notify a personal data breach to the DPC without undue delay and, where feasible, not later than 72 hours after having become aware of it, or provide reasons for the delay. Furthermore, when the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also communicate the data breach to the data subject without undue delay in accordance with the provisions of article 34 of the GDPR.

Personal data breaches that result from cybersecurity breach incidents are also governed under national legislation that transposed Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union into Cyprus law. Under this legislation, essential services providers, digital service providers, providers of electronic communication services and networks must take appropriate security measures and notify serious incidents to the Digital Security Authority.

## Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Law enforcement authorities can access data for the purposes of investigating the perpetration of criminal offences. Such authorities include the Police, the Customs and Excise Department, the Tax Department and the Anti-Money Laundering Unit of the Attorney General. Data collected by law enforcement authorities are:

- processed lawfully and fairly;
- collected for specified, explicit and legitimate purposes and processed only in a manner compatible with these purposes;
- adequate, relevant and not excessive in relation to the purpose for which they are processed;
- accurate and updated where necessary;
- kept in a form that allows identification of the individual for no longer than is necessary for the purpose of the processing; and
- appropriately secured, including protection against unauthorised or unlawful processing, using appropriate technical or organisational measures.

Under Cyprus law, the Cypriot intelligence service can also access data, in the course of performing its duties. Any such access is subject to the requirements of the GDPR to the extent it concerns personal data.

Under certain circumstances, access to personal data by the authorities is subject to a requirement of prior court authorisation. This is the case where the access amounts to interception of private communications.

Any company that is a recipient of a request for information issued by the Police or the CIS is obliged to provide data to the authorities when presented with such request. With respect to orders for access to communications data, obliged entities include electronic communications service providers and electronic communications network providers.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

An online betting or gaming business is subject to authorisation by the National Betting Authority (NBA) of Cyprus. The NBA is the regulatory authority responsible for examining applications, licensing, auditing and supervising prospective betting shops and online betting operators in Cyprus. A particular licence may be granted by the NBA to authorise the provision of online betting services (excluding slot machines, online (live) casinos and online horseracing betting).

The following betting services, inter alia, are expressly prohibited in Cyprus:

- betting on horse races;
- limited betting games machines;
- spread betting; and
- betting on dog racing.

No one under the age of 18 can be registered to use online betting services offered under Cyprus law.

The following information must be obtained for the registration of a person to use online betting services offered under Cyprus law:

- confirmation that the player is over 18 years old;
- identification of the player;
- address of the player's residence;
- player's valid email address; and
- declaration that the player has been informed of the terms and the way of conducting the bet, including the remuneration that the player may potentially be called to provide.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Under applicable Cyprus law, any person advertising online betting or gaming must not do so in a way that:

- implies that it promotes or relates to social acceptance, personal or economic success or the resolution of any personal, economic or social problems;
- involves the endorsement of well-known personalities in a manner that implies that it is related to their success;
- may in any way influence minors to participate in it;

Read this article on Lexology

- promotes its conduct by using services provided by a person who is not a licensee of a type provided for under the relevant legal framework, or an authorised representative; or
- exceeds the bounds of honesty and propriety.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Outsourcing in non-regulated sectors is generally governed by the contractual arrangements concluded between the parties. If Cyprus law is the governing law of the outsourcing agreement, the following are some of the key considerations applicable to outsourcing relationships:

- liability and indemnity aspects;
- intellectual property rights that may reside in the software, equipment and documentation used for the outsourcing;
- intellectual property rights arising as a result of the outsourcing;
- compliance with processing of personal data requirements; and
- the applicability of the protection of employees' rights on transfers between undertakings.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

The Cypriot banking regulatory framework regulates outsourcing by credit institutions, namely agreements by which the service provider carries out a procedure, performs services or activities that would normally be undertaken, provided or exercised by the credit institution itself. Credit institutions are required to apply the European Banking Authority's Guidelines on outsourcing arrangements in relation to their outsourcing policy and processes.

A key aspect in outsourcing in the banking sector is that the credit institution that outsources any function always remains liable for compliance with its regulatory obligations and responsibilities towards its customers. Outsourcing by a credit institution entails varying reporting requirements (depending on whether a critical or important function is outsourced) and must contain specific contractual arrangements. Outsourcing must not hinder effective on-site or off-site supervision of the credit institution and shall not contravene any supervisory restrictions on services and activities.

In the financial and investment services sector, the European Securities and Markets Authority (ESMA) Guidelines on outsourcing to cloud service providers apply. Under the said guidelines, investment firms are required, among others, to:

- clearly assign responsibility for the documentation, management and control of cloud outsourcing arrangements;

- maintain sufficient resources to ensure compliance;
- adhere to specific requirements in respect of the outsourcing agreement when outsourcing critical or important functions;
- have a cloud outsourcing oversight function; and
- ensure that the cloud outsourcing written agreement does not limit the firm's and competent authority's effective exercise of the access and audit rights on the cloud service provider.

Insurance and re-insurance undertakings are subject to the European Insurance and Occupational Pensions Authority Guidelines on outsourcing to cloud service providers, which provide for similar requirements as the ESMA guidelines.

## Contractual terms

### 49 Does the law require any particular terms to be included in outsourcing contracts?

Sector-specific guidelines provide for specific terms to be included in outsourcing critical or important functions to a service provider. These guidelines include the European Banking Authority's Guidelines on outsourcing arrangements in relation to their outsourcing policy and processes, the European Securities and Markets Authority Guidelines on outsourcing to cloud service providers and the European Insurance and Occupational Pensions Authority Guidelines on outsourcing to cloud service providers, all of which are applicable in Cyprus.

Indicative matters that must be governed under the terms of the agreement in sector-specific outsourcing of critical or important functions include:

- the time frame of the outsourcing;
- the governing law of the agreement;
- provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data;
- agreed service levels that should include precise quantitative and qualitative performance targets for the outsourced function;
- reporting obligations of the service provider;
- taking out insurance;
- business continuity and contingency planning;
- locations; and
- exit and termination.

## Employee rights

### 50 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

Generally, outsourcing arrangements may be caught under the framework safeguarding employee rights in transfers of undertakings. Where this framework is found to apply, the transferor's rights and obligations as employer shall be transferred to the transferee undertaking. The transferor and transferee can agree that they shall be jointly and severally liable

in respect of obligations that arose before the date of transfer from a contract of employment or an employment relationship existing on the date of the transfer.

The transferor and transferee have a duty to inform all affected employees of the transfer and related matters. The transferor or transferee (or both) may be required to consult with affected employees or their representatives when they envisage they will take measures in connection with the relevant transfer.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

In the personal data domain, data subjects have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects that concerns them or significantly affects them. This right is subject to limited exceptions and is protected with strict safeguards – including the right to obtain human intervention to data that are subject to automated decision making (including profiling).

An impact assessment is required in the event where there is systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing (including profiling) and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.

In the wider artificial intelligence domain, the European Commission has tabled a proposal for a regulation on artificial intelligence (AI). The proposed regulation aims to ensure that AI systems placed on the EU market are safe and respect existing law on fundamental rights and EU values, ensure legal certainty to facilitate investment and innovation in AI, and facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Training data sets and software associated with artificial intelligence (AI) or machine learning may be protected by intellectual property rights, provided they meet the requisite originality requirements under applicable Cyprus law.

While Cyprus law does not expressly regulate intellectual property rights linked to AI, nor have such matters been tested in Cypriot courts, it is expected that AI-assisted works would be eligible to vest intellectual property rights to their creators. On the other hand, AI-generated creations would not be in a position to attract intellectual property right protection, as they would not meet the criterion of originality that is linked to a natural person and their personality.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Cyprus has developed guidance on ethics associated with AI or machine learning through the National Strategic Plan on AI which was developed by the Department of Electronic Communications of the Ministry of Transport, Communications and Works of the Republic of Cyprus (the DEC) in 2020 and is currently being implemented. This policy tackles matters on ethics associated with AI, including the need to protect the security, privacy and human rights of users and to ensure transparency on labelling requirements and traceability of AI software as well as the protection of the environment.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Income derived from trading in digital products and digital assets, including cryptoassets, is generally taxable. Profit achieved by companies in Cyprus is subject to a corporation tax of 12.5 per cent. Certain income may be tax deductible if the digital product concerned has been developed in Cyprus.

Cyprus entities' profit from qualifying IP assets may benefit from an 80 per cent tax deduction, resulting in an effective tax rate of 2.5 per cent or less. The regime, known as the 'IP Box', benefits software, patents, utility models and other intellectual property assets.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

The presence of servers in Cyprus or the operation of a metaverse out of Cyprus by a non-resident company does not in itself create tax residence in Cyprus, but may give rise to taxation depending on whether income is derived from such activity by a permanent establishment in Cyprus.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

Electronic invoices are equivalent to paper invoices under Cyprus law and businesses are free to issue electronic invoices subject to acceptance by the recipient. Cyprus law provides for mandatory electronic invoicing for all public procurement transactions (for both public and private suppliers). Copies of invoices, as part of the records kept in relation to a company's transactions in Cyprus, must be kept for a period of seven years.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no special courts in Cyprus dealing with online or digital disputes. Any claim for breach of applicable law in relation to online or digital services, such as claims arising from breaches of the electronic commerce legislation can be dealt with by the Cypriot courts.

Online/digital issues and disputes primarily regarding consumers such as, inter alia, claims arising from e-commerce transactions, claims regarding delivery of damaged goods, unfair practices, goods that fail conformity requirements and surcharges can be resolved through dispute resolution bodies accessed via the Online Dispute Resolution (ODR) platform provided by the European Commission for the online resolution of disputes between consumers and traders.

The ODR platform can be used to submit a request that will then be notified to the trader. Depending on whether the trader is willing to address the request and resolve the dispute, the dispute may be resolved without further recourse to dispute resolution bodies. The consumer and trader should reach an agreement within a maximum of 90 days, at the lapse of which the consumer can address a dispute resolution body (which can be agreed with the trader) or pursue any remedies in court.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

A consumer has the choice of using ADR to resolve a dispute with a trader in respect of an online transaction.

Traders who agree or are obliged (in the case of a regulated sector) to use ADR must inform consumers accordingly on their websites as well as in their general terms and conditions.

They must also inform consumers about ADR when a dispute cannot be settled directly between the consumer and the trader.

ADR bodies in Cyprus must have been approved by the competent authority. It is increasingly common in Cyprus for consumers to pursue the resolution of their dispute via ADR and for traders to agree to such dispute resolution process.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

Cyprus has several policy initiatives under implementation, which are expected to facilitate digital transformation, such as the Digital Strategy for Cyprus (2020–2025) and the Broadband Plan of Cyprus 2021–2025. EU instruments such as the Digital Markets Act and Digital Services Act are expected to have a major impact on business and transactions carried out online.

ANTONIOU McCOLLUM &CO.

Anastasios A Antoniou anastasios.antoniou@amc.law
Ifigenia Iacovou ifigenia.iacovou@amc.law
Orestis Anastasiades orestis.anastasiades@amc.law

9 Nikitara, Nicosia 1080, Cyprus
Tel: +357 22 053 333
www.amc.law

# France

Elisabeth Logeais, Corinne Khayat and Anne-Marie Pecoraro

UGGC Avocats

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

Digital transition is a key priority and focuses on innovative technologies, namely cybersecurity, quantum strategy, cloud and 5G, and artificial intelligence.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

The matrix law is French Law No. 2004-575 of 21 June 2004, for confidence in the digital economy.

Law No. 78-17 on information technology, files and freedoms is the founding national legislation on personal data.

Subsequent laws address liability of platforms and operators, online consumer protection and business sectors' digital regulation (banking, media, etc), often transposing new EU regulations and directives, namely the 2022 Digital Services Act and Digital Markets Act. In 2023, France enacted new regulations on whistleblowing and for the first time on commercial influence (Law No. 2023-451 of 9 June 2023).

### Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

Digital content and services are notably supervised by the Financial Markets Authority (AMF), the National Agency for the Security of Information Systems (ANSSI), the Online Gaming Regulatory Authority, the Regulatory Authority for Audio-visual and Digital Communication and the Electronic Communications, Postal and Print Media Regulatory Authority.

E-commerce practices are mainly monitored by the Competition Authority, the Directorate-General for Competition, Consumer Affairs and Fraud Control and the AMF. The main supervisors in the field of cyber criminality and data protection are the ANSSI and the National Commission for Information Technology and Civil Liberties.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Articles 42 and 46 of the Code of Civil Procedure and article L 721-3 of the Commercial Code are the basic articles on civil and commercial jurisdiction.

### Contract disputes

In contract disputes involving a French party and a non-EU-based defendant, the French court will have jurisdiction if the dispute relates to the delivery in France of the contractual product or service (or both). For online consumer contracts, the consumer may sue before the court of the place where he or she resided at the time the contract was concluded or at the time the harmful event occurred.

For international civil and commercial contracts involving parties domiciled in the EU, EU Regulation No. 1215/2012 of 12 December 2012 (article 7) applies, whereby the French plaintiff may sue in France the EU-based defendant targeting France. Contractual clauses on territorial jurisdiction can be enforceable between professionals but successfully challenged in consumer contracts.

### Tort

In tort matters, the court of the place where the harmful event occurred has jurisdiction. If the event originated in France, the French court will have full jurisdiction; if only the damage is suffered in France, the court may only compensate the damage suffered in France.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

A digital business targeting France through a website must display certain mandatory information: the legal form of the company or the identity of the individual entrepreneur; registration number; address; VAT number; contact details of the web host; and specific administrative permits (for trade of drugs, alcoholic beverages, banking, etc). A non-EU-based service provider of intermediary services must appoint a representative in an EU member state where it offers its services.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Electronic contracts are enforceable except in matters of family law and inheritance law where dematerialisation is restricted.

In business-to-consumer (B2C) online contracts, prior to any order, consumers must be provided with contractual terms and conditions. Consumers' consent is expressed by a double click confirming the order.

Since 31 May 2023, a consumer must also be able to end an electronic contract with one click.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

In international digital business-to-consumer (B2C) contracts, the law chosen by the parties will only be fully effective if it provides the consumer with an equal or higher level of protection, compared to the law of the consumer's country. A professional's online offer must provide certain information (article 1127-1 of the Civil Code).

The digital B2C contract must mention the term of the contract, the means of delivery of the digital content and the legal conformity warranty for digital goods, services and contents.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Article 1367 of the Civil Code recognises the electronic signature if the identity of the signatory and the integrity of the document are guaranteed. An electronic signature may be simple, advanced (no certification) or qualified where the person signing is certified by a certification authority or service provider.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

An operator of a commercial website must indicate in its general terms and conditions the contact information for its customer service and the option for the consumer to refer a dispute to the consumer ombudsman, or to mediation, for instance the 'mediator of electronic communications'.

The consumer may also alert the Directorate-General for Competition, Consumer Affairs and Fraud Control via the Signal Conso platform if the professional fails to comply with applicable regulations.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The Consumer Code prohibits any direct or indirect online advertising to potential or existing clients likely to be non-professionals (1) about investment services that are not admitted to trading on a regulated market or a multilateral trading facility, or (2) inviting a consumer through a contact form in order to offer digital asset services or to participate in a token offer, or both, unless the advertiser is licensed.

The Monetary and Financial Code mostly regulates advertisement and sale of financial services to businesses.

The supervision of banking and insurance practices is carried out mainly by (1) the French Prudential Supervision and Resolution Authority (ACPR), which monitors compliance with anti-money laundering and anti-terrorist financing measures; and (2) the Financial Markets Authority (AMF), which is responsible for protecting savings invested in financial products, informing investors and ensuring the proper functioning of markets.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

A comprehensive EU regulation of the digital unregulated currencies, called Markets in Crypto-Assets (MiCA), adopted on 31 May 2023, entered into force in June 2023 and purports to regulate the trade of crypto-assets (utility tokens, asset referenced tokens and stable coins and associated services). Notably, MiCA:

- requires providers of crypto-asset services (PSCA) to obtain authorisation from the competent national regulatory authority;

- provides a regulatory framework for the trade of cryptocurrencies;
- addresses the situation of non-fungible tokens (without regulating them so far); and
- compels reporting by digital asset service providers (PSANs) on the environmental and climate footprint of their dealings with crypto-assets.

## Digital and crypto wallets

### 12 Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

After the 2019 French *Pacte* law providing a legal status for initial coin offerings and the increase of PSANs, a new Law No. 2023-171 of 10 March 2023, which contains various provisions for adapting to European Union law in the fields of economics, health, labour, transport and agriculture (coming into force on 1 January 2024), strengthens the conditions and controls for the registration of PSANs with the AMF, focusing on enhanced security and internal control systems, management of conflicts of interest and new obligations for the custody of digital assets on behalf of third parties.

As at mid-July 2023, there are 90 registered PSANs for four approved activities to be carried out in France, these being:

- services of custody of digital assets;
- purchase or sale of digital assets in legal tender;
- exchange of digital assets for other digital assets; and
- operation of a trading platform for digital assets.

A new EU Regulation 2023/1114 of 31 May 2023 on cryptocurrencies not governed by current regulations on financial services, will come into force on 30 June 2024, allowing PSAN candidates to carry related activities of managing crypto asset wallets.

Distinct from crypto assets are digital wallets (e-wallets), which are electronic devices (smartphones, tablets) or online services allowing the holder to store funds, make electronic transactions and track payments. Providers are account aggregators who must obtain a licence from the ACPR to carry out their activities.

## Electronic payment systems

### 13 How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

The 2021 French Finance Act schedules the implementation of e-invoicing, as well as the reporting of certain invoicing data to the tax authorities (e-reporting). The roll-out was postponed to 1 July 2024, but the registration service for partner dematerialisation platforms opened on 2 May 2023 to process the first applications.

Banks are bound by the bank secret, but certain administrative entities (tax, social security, some control entities such as AMF, ACPR, and the National Commission for Information

Technology and Civil Liberties (CNIL)). CNIL may have access to data for control. Article 561-2 of the Monetary and Financial Code compels cooperation in the fight against money laundering and terrorist financing, including the providers of digital assets.

In the wake of EU Payment Services Directive 2 contemplating instant payment means, new omnichannel payment strategies are expanding involving various electronic means of payment and tools (phone, computer, credit card, electronic wallet, etc).

### Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

The KYC mandatory procedure can be carried out by service providers satisfying the requirements of the EU 5th Anti-Money Laundering Directive and the electronic identification and trust services (eIDAS) Regulation. Article R561-5-2 of the Monetary and Financial Code sets the requirements to carry out the distance KYC procedure and provides that payment service providers may use certified services that meet the requirements for security and ID verification.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

AFNIC is the French public entity that manages, through accredited registrars, the registration of domain names in France (.fr), and in specific cities or areas in France (.paris and .alsace) and overseas.

The registrant of a domain name under one of the top-level domains (TLDs) managed by AFNIC must have a registered office or main place of business or residence in one of the EU member states or in Switzerland, Lichtenstein, Norway or Iceland.

Disputes regarding domain names in TLDs monitored by AFNIC may be resolved through two ADR procedures, SYRELI and PARL EXPERT. Available since 2011, the Syreli procedure ends with a decision rendered by employees of AFNIC. The PARL EXPERT procedure, established in 2016, is a collaboration with the World Intellectual Property Organization (WIPO) whereby decisions are rendered by experts selected by AFNIC and WIPO. In both cases the decision is rendered within two months. The plaintiff must establish standing that the contested domain name:

- disrupts public order, morality or legal rights;

- infringes intellectual property (IP) rights or personal data; or
- is identical or relates to a national emblem or a public authority or entity.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Domain names can be copyrightable or registered trademarks. The owner of a trademark reproduced in a domain name can challenge the registration of the domain name. Similarly, a domain name reproducing a copyrightable word or expression may be challenged, but the burden of proof may be difficult.

Likewise, reproduction in an URL of an IP-protected expression may be challenged, for IP infringement or on grounds of unfair competition.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

Online advertising is regulated by various rules that prescribe, notably:

- identification of the advertiser and of the advertising nature of the message;
- transparency of the purchase price paid by the advertiser; and
- compliance with the EU General Data Protection Regulation (GDPR) and the National Commission for Information Technology and Civil Liberties (CNIL) guidelines.

Specific advertising restrictions include the prohibition of surreptitious advertising and subliminal techniques. The recommendations of the professional advertising regulatory authority (ARPP), notably on Digital Advertising, are usually followed. A new Law No. 2023-566 of 7 July 2023 setting a 'digital majority' at 15 years old and compelling websites to fight online hate will be notified to the EU Commission before implementation.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Targeted and online behavioural advertising are regulated by the general principles set out by the GDPR and by Law No. 78-17, as well as by the CNIL guidelines, sectoral regulations and the provisions of the new Digital Services Act focusing on children, sensitive data and 'dark patterns'.

Cookies are subject to express prior consent for each type of non-technically essential cookies. The CNIL recommends a brief presentation of the purposes of each type of cookies and an upfront choice to accept or reject cookies upon reaching the website.

Furthermore, a law of 9 June 2023 now compels influencers to mention 'advertising' activities, abstain from promoting various products, and be liable for unsuccessful completion of drop-shipping sales.

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

The French Consumer Code prohibits unfair (deceptive or aggressive) commercial practices, offline and online. Advertisers must be able to substantiate objectively verified and verifiable advertising content and thus secure all useful supporting information. An online advertisement must be clearly identified as such and indicate the individual or entity on whose behalf it has been published.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

The French *Evin* law totally prohibits tobacco advertising and subjects advertisements for alcoholic beverages to a highly restrictive regime. The Monetary and Financial Code also prohibits direct or indirect electronic advertising of some speculative trading services.

Specific advertising restrictions apply to products and services deemed dangerous (ie, firearms, medical devices, gambling, etc).

## Direct email marketing

### 21 | What regulations and guidance apply to email, SMS and other direct marketing?

Distance marketing is regulated by the Post and Electronic Communications Code, the GDPR and the guidelines issued by the CNIL.

All marketing communications must be concise, transparent, comprehensible. The issuer must be readily identifiable, and the recipient must be able to refuse easily any future solicitation.

To prevent telephone marketing, anyone can register his or her name on the Bloctel list operated by the government.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Web hosts are not liable for hosted content on behalf of a content provider if (1) they do not have actual knowledge of their unlawfulness, or (2) from the moment they become aware of such unlawfulness, they act promptly to remove the content or to prevent its accessibility.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

The liability regime for digital platforms and online content providers distinguishes online publishers and web hosts. While web hosts are not responsible for the content published by their intermediary, online publishers are liable for the content that they provide.

The French High Court held in 2023, ahead of the EU Digital Services Act (DSA), that the operator of an online sales site who hosts the data of other sellers and also provides them with a logistics service for manufacturing and delivering the products sold, may be held liable for infringement committed by these sellers (Cass. com. 13 April 2023 No. 21-20252). Furthermore, the DSA increases the liability of 'very large platforms', the criteria for which will likely be ascertained by courts.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Online content providers can set their own terms and conditions for removing content for specific reasons. Conversely, ISPs do not have a general obligation to monitor content. Both can be compelled to implement a court order providing for the shutdown of a litigious webpage.

Decree No. 2023-454 of 12 June 2023 enables an administrative entity, the Central Office for the Fight Against Crime Linked to Information Technology and Communication, to obtain court-ordered measures to block access to mirror sites.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

The French IP Code implements EU Directive 96/9/EC of 11 March 1996 on the Legal Protection of Databases, providing a dual protection: (1) copyright protection if the selection or arrangement of content is 'original'; and (2) sui generis protection of the content of the database if the producer can show a substantial investment in the constitution, verification or presentation of the data. The producer of a protectable database can prohibit substantial extractions and reuses of said content. Article 35 of the EU Data Act of 23 February 2022 sets aside the sui generis right for 'databases containing data obtained from or generated by the use of a product or a related service' (IoT devices). The boundaries of this exception will need further testing.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

The inclusion of a hyperlink to a website is, in principle, permitted. A link to inside content should respect the credits and sources and, as the case may be, the restrictions of the concerned website, and in any case the copyright protection of the linked content.

To assess possible infringement by linking, case law distinguishes whether the inclusion of the hyperlink is for profit or not.

Finally, where the work is only accessible to a restricted audience (eg, subscribers), setting up a hyperlink that circumvents these access restrictions is unlawful.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Any unauthorised reproduction, representation or distribution in whole or in substantial part by any means whatsoever of IP-protected features or content may amount to IP infringement. The IP Code (article L 122-5) provides only limited exceptions where use of copyrighted content by a third party is allowed, for instance:

- use of short quotations, press reviews and speeches;
- precise educational exceptions;
- parody, pastiche and caricature; and
- some scientific research purposes.

Besides, the copying or scraping of substantial chunks of content displayed on a third party's website or platform can be sanctioned under the sui generis right of the producer of the database.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Enforcement of IP rights in the metaverse, pursuant to existing rules on international jurisdiction, was demonstrated by the Birkin bag NFT case initiated by Hermès and decided on 8 February 2023 by a Manhattan federal court. In the EU, the Digital Services Act and the Directive on Copyright in the Digital Single Market address the liability scope of certain online content sharing service providers. Basically, a litigious platform 'targeting' French internet users on the basis of the 'accessibility criterion' of the platform in France and the existence of a 'sufficient, substantial or significant link with the French territory' will ground jurisdiction of French courts.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Pursuant to the exhaustion of IP rights, the holder of an IP right who places on the EU market, or indirectly with his or her consent, IP-protected tangible products, may no longer control the subsequent circulation of the products in the EEA (now excluding the United Kingdom). Pursuant to a judgment of the ECJ (C-263/18 of 2019, *Tom Kabinet*), online first distribution of digital products protected by copyright are not subject to the exhaustion principle. Still, the scope of the exhaustion of IP rights-protected products made available online compels a careful distribution strategy in a diverse digital environment (non-fungible tokens, metaverses, social networks, etc).

## Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

French authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP rights infringement:

- criminal law allows searches at a counterfeiter's premises supervised by a police officer;
- civil law allows an IPR holder to obtain an ex parte court order allowing a seizure by a bailiff on the premises of an alleged infringer and to obtain information on the source and distribution network of the infringing goods for further use in court; and
- customs law empowers other administrative authorities to carry out investigations and seizures of counterfeit goods.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

When IP infringement is alleged, a civil court may order the destruction of the infringing goods, prohibit further infringing acts, subject to penalties, award damages (lost profits, infringer's profits, moral prejudice), and order publication of the judgment at the infringer's expense.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Law No. 78-17, updated in 2018, is the founding text on the processing of 'personal data', which is construed as any information relating to an identified or identifiable natural person, and gives a definition of 'sensitive personal data'.

'Pseudonymous/anonymous' data are construed by the the National Commission for Information Technology and Civil Liberties (CNIL) by reference to the definition in the EU General Data Protection Regulation (GDPR).

A further 2019 decree summarises (1) the broad regulatory, enforcement powers of the CNIL, (2) the exercise of individual rights, and (3) the processing of health data for R&D purposes.

the CNIL investigates various sectors and has been enforcing a strict policy on cookies and other trackers online since 2020. In 2023–2024 it will focus on the use of 'augmented cameras', health records and mobile apps.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Businesses and individuals do not need to register with a public authority because they process personal data in France, without prejudice to mandatory declarations in certain regulated professions. However, a data protection officer (DPO) must be appointed: (1) when the processing is carried out by a public authority or body; (2) when there is a monitoring of data subjects on a large scale; or (3) when there is a large-scale processing of sensitive personal data, such as those related to crimes and offences. The DPO must register with the CNIL.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

Law No. 78-17 applies to overseas French lands.

An organisation (excluding public authorities) or individual established outside the EU which processes personal data of persons in France or in the EU (whatever their nationality or residence), in the course of offering them goods and services or monitoring their behaviour in France, must appoint a representative in the EU (articles 3 and 27 of the GDPR).

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

Each data processing must rely on a legal basis (article 6 of the GDPR and article 4 of Law No. 78-17), such as consent, performance of a contract, legitimate or vital interest, legal requirement or public interest.

Transfers within the EU (to and from an EU-based entity) are free. Transfers to non-EU countries are mostly based on subcontracting relationships, intragroup links, M&A, R&D agreements, etc.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Intra-EU transfers of personal data between controllers and processors established in the EU are deemed GDPR compliant. International transfers outside the EU can be based on several grounds, mainly:

- an adequacy decision that the non-EU recipient state complies with the GDPR principles;
- intra-group agreements (binding corporate rules);
- standard contractual clauses and approved codes of conduct; and
- derogations for specific situations that are narrowly construed.

The CNIL carries out periodic compliance audits (21 in 2022) on security of health data, direct marketing, retention periods, cookies policies, etc, and applies heavy fines in cases of non-compliance (more than €100 million in 2022).

On 10 July 2023, the EU Commission adopted an adequacy decision finding that the USA provides a level of protection substantially equivalent to that of the EU, thus allowing,

under certain conditions, the transfer of personal data to this country, without additional requirements.

Overall, operators based in France and involved in sensitive areas such as national defence, health and essential infrastructures are advised to host their data in France or the EU.

## Sale of data to third parties

### 37 May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

The sale or licensing of personal data (in the form of client files) often occurs in mergers and acquisitions. Pursuant to CNIL's 2022 guidelines on commercial sales of customer files, data of active clients may only be transferred with their consent and the purchaser must secure evidence of their consent. In any event, the concerned person has the right to oppose the use of his or her email(s) and further prospection by third-party providers.

## Consumer redress

### 38 What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Natural persons enjoy eight main rights regarding their personal data:

- to be informed;
- to have access;
- to rectify;
- to be forgotten;
- to restrict processing;
- to transport their data;
- to object to processing; and
- to object to automated decision-making and to profiling.

Basically, any natural person can request the protection of the GDPR or French law when:

- a data controller or processor established in the EU processes the personal data of natural persons, regardless of their nationality and presence in the EU; or
- a data controller or processor not established in the EU targets natural persons when they are in the EU, even temporarily, with offers of goods and services or by monitoring their behaviour while they are in the EU (article 3 (1) and (2) GDPR);

The concerned person may complain to the appointed representative in the EU of data controllers and processors not based in the EU (article 27 GDPR), and in any case to the CNIL.

Following an ECJ decision in 2022, EU member states may acknowledge the right of consumer associations to contest violations of personal data.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

The use of non-personal data is regulated at EU level by EU Regulation No. 2015/1807 of 14 November 2018.

Non-personal data is protected in France through various texts addressing certain categories of data, for instance, texts on business secrets and privacy; genetic and certain health data; national defence information; certain administrative data and public registries held by public authorities.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

The requirement to hold an original paper document has disappeared in the business environment (article 1174 of the Civil Code), with the exception of certain documents in inheritance and family law. An NF 42-026 standard defines the specifications of 'faithful digitisation services of documents', allowing an equivalence between the paper medium and the digital format of a document.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Commercial contracts, invoices and correspondence, contracts concluded by electronic means and accounting books and records must be kept for 10 years. Bank documents must be kept for five years.

Customs declarations must be kept for three years.

Documents that the Fiscal Administration can investigate and control must be kept for six years from the date of the last transaction mentioned (article L102B Book of Fiscal Procedures).

Regarding personal data, the National Commission for Information Technology and Civil Liberties has released very precise guidelines on the retention periods for personal data, as follows:

- two years for active databases;

- intermediate archiving for a limited term and restricted access to meet legal obligations or risks (administrations' control or possible litigation until expiry of the statute of limitations); and
- final archiving of anonymised data or final deletion.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

The French regulatory framework on security of data comprises:

- a set of measures for 'critical infrastructure information protection';
- the transposition into French law of the 2016 NIS Directive (first EU legislation on security of network and information cybersecurity);
- guidance (by the National Commission for Information Technology and Civil Liberties), for instance on the conduct of privacy impact assessments; and
- several sectoral laws.

Operators in sensitive economic sectors (eg, banking, health, communications) must comply with specific security obligations. Two main security reference documents are the standards ISO/IEC 27001 and ISO/IEC 27002, in addition to those mentioned on the website of the National Agency for the Security of Information Systems.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

The CNIL sets the procedure for management of data breaches, which entails mandatory notification by the data controller to the CNIL within 72 hours of the discovered breach:

- the scope of concerned data and data subjects;
- the measures to stop or mitigate the consequences; and
- the information provided to the concerned persons if there is a serious risk regarding privacy.

Web hosts of sensitive data are subject to higher scrutiny and to a specific accreditation, as is the case for web hosts of health data collected in France, as explained on the website of the French Digital Health Agency.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

The authorities having a right of access to personal data, on a need-to-know basis, are as follows:

- the tax, social security, unemployment and customs administrations;
- bailiffs;
- judicial authorities; and
- administrative authorities (eg, the Financial Markets Authority, the authority responsible for the prudential supervision of the banking and insurance sectors (ACPR), the CNIL, and the French anti-money laundering unit (TRACFIN)).

The ECJ reiterated in a recent decision that preventive legislation in support of public security does not justify an overly broad impairment of business activity (ECJ, 5 April 2022, C-140/20).

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Law No. 2010-476 of 12 May 2010 authorises, with restrictions, betting on sports (eg, horse racing) and poker on the internet only by operators accredited by the French National Gaming Authority (ANJ). Any other form of gambling, betting or its offer by an unlicensed operator is illegal.

The authorised operator, before opening a player's account, must verify his or her personal information, including age beyond 18 and credit capacity.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Advertising or providing access to an online betting or gaming business located in another jurisdiction or in a metaverse is permitted, provided that the online betting or gaming business fulfils certain requirements and is accredited by the ANJ.

Advertising is subject to various restrictions for online gambling and games of chance, for example, the inclusion of a warning message and the prohibition of advertising to minors.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

The key legal issues in outsourcing agreements are:

- the relevant calibration of the provider's obligations;
- the scope of licences and sub-licences granted to the provider and its contractors;
- the grant back of intellectual property and data developed by the provider or jointly;
- the legal status of consultants and employees dedicated to the project; and
- the drafting and implementation of the reversibility plan.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

Foreign investments in certain fields must be approved by the French government, such as:

- activities carried out in the information systems security sector for a public or private operator managing vital facilities;
- R&D and export in critical technologies (cybersecurity, artificial intelligence, quantum technologies, etc); and
- cryptology activities.

Sectoral recommendations may impact the use of outsourcing. For instance, in the banking sector, the European Banking Authority has published Guidelines on Outsourcing Arrangements in force since 31 December 2021.

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

In spite of the various fields of outsourced services, there is a common set of provisions that are recommended by professional associations (eg, Syntec) regarding, for instance: service level agreements; hosting and export of personal and non-personal data; management of intellectual property rights; reporting and monitoring tools; staff management; and disaster recovery and reversibility plans.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

The service provider in an outsourcing agreement makes available some of his or her employees to work on the client's project. As outsourcing agreements may last for several years, attention must be paid to article 1224-1 of the French Labour Code. This article provides that in cases of substantial changes in the operation of a business entailing a transfer of an 'economic autonomous entity', there is an automatic transfer of the employment contracts to the third party ensuring this continuity. In this context, the transferred employee keeps all their rights and benefits obtained with their former employer.

However, in a specific context of avoiding the closure of one or several establishments and to accept a takeover offered by a third party, certain small companies may negotiate a job protection plan allowing it to maintain the necessary employments and to terminate the others pursuant to economic redundancy prior to the transfer.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

On 21 April 2021, the European Commission published a draft EU regulation on artificial intelligence (AI).

In May 2023, the National Commission for Information Technology and Civil Liberties (CNIL) released its action plan on AI. In June 2023, the EU Parliament adopted a common stance on how AI should be regulated in the EU and should ensure non-discrimination, liability and IP protection for AI-developed inventions and creations.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

AI questions intellectual property ownership as AI-assisted human creation moves towards independent AI creation. So far, the status of inventor has not been convincingly attached to AI. Regarding copyright in AI-generated artworks, a 2020 report by the French Intellectual

and Artistic Property Board contemplates the creation of a specific author's right, as is the case for software databases.

In June 2023, the EU Parliament adopted a common stance on how AI should be regulated in the EU, providing objectives and prohibitions. The definition of an AI scheme for Europe should, therefore, progress in the coming months.

France carries its AI development strategy with a 2018–2025 plan.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Several countries and international organisations (eg, UNESCO) are attempting to design ethic rules for the use of AI. In 2021 the EU Parliament adopted a resolution defining AI and issues of military use and international public law. In June 2023, the EU Parliament adopted its negotiation strategy on AI and decided the creation of a specific entity for AI issues.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

The sale of digital products, other digital tokens and online services is subject to taxation in France.

As these transactions constitute the supply of goods or services, VAT rules apply. For software, the applicable rules differ depending on whether the transfer of software is qualified as a transfer of goods or a supply of services.

There are specific tax laws for fungible crypto assets, including a flat-rate capital gains tax (single flat-rate levy at a rate of 30 per cent).

Regarding taxation of non-fungible tokens, there is no text or administrative doctrine that makes it possible, to date, to determine with certainty their tax regime.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Digital intermediation services are considered to be provided in France when one of the users entering into a transaction is located in France or, in the absence of a transaction,

when one of the users has an account opened from France and is able to access these services, regardless of the location of the server.

Providers of video on demand for private use by the public are subject to the payment of a tax (even if located outside France).

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

Electronic invoicing applies to dealings between companies subject to VAT and established in France (business-to-business dealings) through a dematerialisation (demat) platform, which can be the demat public portal (Chorus Pro) or another demat platform (an approved partner demat platform). Several transactions exempted from VAT are not subject to use of electronic invoicing and include services in health education, real estate transactions, and banking, insurance and other financial transactions. The coming into force of the new regulation on e-invoicing has been postponed until July 2024.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

Civil and commercial courts deal with online digital disputes. IP-based disputes are usually decided by specialised civil courts, and commercial courts hear most other online-related disputes. The Paris Commercial Court has two international chambers specialising in international business disputes.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

ADR is available and often provided in consumer contracts – and increasingly in commercial contracts.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

Important trends and concerns in France regarding digital business address the following:

- the completion of a financial regulatory framework regarding safe trade with digital currencies;
- the boost of the French artificial intelligence programme, which pools its top scientific expertise;
- the design of workable cross-border flows of data; and
- the growth of technologies addressing climate change.

UGGC AVOCATS

Elisabeth Logeais elo@uggc.com
Corinne Khayat ckh@uggc.com
Anne-Marie Pecoraro amp@uggc.com

47 Rue de Monceau, 75008 Paris,France
Tel:+33 1 56 69 70 00
www.uggc.com

# Germany

Jens Borchardt, Franziska Ladiges, Elisabeth Noltenius, Stefan Peintinger and Johannes Schäufele*

SKW Schwarz

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The German government is continuously focusing on aspects of digitalisation as growth factors for the German economy, seeking to facilitate entrepreneurship and development.

Parallel to several European initiatives, a trend remains that both the legislator and specific developments in case law shift focus on the legal responsibility and liability of online platforms creating the commercial link between businesses and consumers.

Influencer marketing and data privacy has been an area of enforcement that has seen much activity and publicity recently.

New technologies such as blockchain and artificial intelligence are also keeping German legislators busy.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

The main source of specific sector law is the Telemedia Act (TMG), which implements and incorporates a general regulatory framework relevant for e-commerce including liability rules, information duties (both rooted in the eCommerce Directive), certain commercial practices, etc. Alongside the TMG, the new German Telecommunications-Telemedia Data Protection Act specifically regulates data protection in telemedia and telecommunications; it also contains the essential data protection rules for the use of cookies. Of utmost importance for any marketing and digital business activities is the Act on Unfair Commercial Practices. Activities of audiovisual media services and a broad variety of (media content) online platforms are governed by state treaties, such as the Media State Treaty, formerly known as the State Treaty on Broadcasting, and the Network Enforcement Act (NetzDG), which applies to social media platforms. Consumer protection laws and a variety of specific product and service regulations, for example, in financial services, insurance and product distribution, and the General Data Protection Regulation (GDPR) form other important sources of law for digital business. Also important are the European legislative initiatives such as the upcoming Digital Services Act (DSA), which mainly affects business-to-online platforms and search engines, and the Digital Markets Act (DMA), which establishes competition rules for very large tech companies (called 'gatekeepers').

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

Various new authorities are currently being established under the DSA. In the meantime, there are no authorities or public administrative bodies that are specifically endowed with powers to regulate e-commerce. Rather, authorities that oversee specific sectors enforce against unlawful conduct within their respective legal remit, most notably through the federal media authorities, federal data protection authorities, as well as the Federal Ministry of Justice and Consumer Protection, which is competent for the NetzDG, and the Federal Network Agency for telecommunications and access tariffs.

Extensive regulatory activity is done within the market itself, under civil law. Privately organised bodies such as consumer protection associations and competition protection associations have the power to enforce against unlawful conduct of business, typically via cease-and-desist claims, but also for damages and skimming off profit. This is a matter of civil litigation based on the specific acts (namely, the Act Relating to Actions for Injunctions in the Case of Breaches of Consumer Protection and Other Laws) and the Act against Unfair Competition.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

As a result of its ubiquity rules, the key tests are based on the EU's Rome I and Rome II Regulations and also Brussels 1a. The test is typically whether a certain activity was aimed at the German market or its participants, and in certain cases courts require (in addition) a 'commercial effect'. Within the EU, this may be subject to certain, but limited and often sector-specific country-of-origin principles.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

As regards establishing a business, the rules for online businesses do not vary substantially from those applicable to brick-and-mortar businesses. Depending on the place of establishment, a general permit to do business or sector-specific licences, for example, for offering financial services or for linear broadcasting activities, may be required. Such requirements may be subject to exemptions based on the European freedom of services, for example, by allowing passporting or relying on licences from other EU or EEA member states.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

The validity of electronic contracts is based on the same principles as the validity of contracts in general. A contract is formed where one party makes an offer and another party accepts this offer. Actual activity is needed to express a declaration of will to contract. Click-wrap contracts are a common standard. Crucial elements to consider regarding consumer contracts are special formal requirements for due formation – the button solution from the EU Consumer Rights Directive – and that general terms and conditions can duly be taken note of prior to the contracting process and are duly agreed to apply.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Yes, the choice of governing law, language of the contract and forum for disputes is limited with regard to business-to-consumer contracts. Mandatory consumer information must generally be given in the German language. Choices can be made more freely in business-to-business contracts.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

The law generally allows free form of contracting, including digital or e-signatures. However, certain types of contracts per statute require a specific form. Typically, these requirements are tied to specific types of transactions with high impact, like acquiring shares in companies or purchasing property. If the form requirement is not met, the contract is invalid.

Where statutory law requires a specific form, such as written form or notarial form, electronic contracts are typically not sufficient to form a valid contract. However, a required statutory written form can be replaced by certain electronic means as well (the qualified electronic signature according to section 126a BGB), unless not explicitly prohibited by statutory law. The technical requirements for a qualified electronic signature are set out in Regulation (EU) 910/2014 of 23 July 2014 (the eIDAS Regulation) and the Trust Service Provider Act (VDG). Providers are qualified and licensed under the eIDAS Regulation and VDG.

The same general principles apply to signing of digital information.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

Consumers can use the European Commission's online dispute resolution platform to submit claims. However, participation in online dispute settlement proceedings in front of a consumer arbitration board is generally not required for businesses. There are no special remedies for the breach of electronic contracts.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The Federal Financial Supervisory Authority supervises this area. Competition protection associations may in addition seek to enforce market behaviour rules and also against unfair consumer terms, where consumer interests are affected.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Electronic money, digital assets or use of digital currencies are primarily regulated under the Directive (EU) 2015/2366 on payment services in the internal market (PSD2) rules. Operating marketplaces trading electronic money, digital assets or digital currencies may require a licence. Also, it is in dispute whether loyalty programmes' units may qualify as e-money in certain circumstances – which they usually do not. This may give rise to the application of the respective regulatory framework with its various complexities.

### Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

There are certain rules, in particular, around crypto depositing. Crypto depositing is defined as:

> *the depositing, management and safeguarding of crypto securities or private cryptographic keys used to hold, store or dispose of crypto securities for others and the safeguarding of private cryptographic keys used to hold, store or dispose of crypto securities for others to hold, store or dispose of.*

Crypto depositing is deemed a financial service requiring a licence.

**Read this article on Lexology**

Mere providers of hardware or software that enable users to store their private keys themselves using self-hosted or non-custodial wallets are not regarded as crypto depositors insofar as the providers have no intended access to the crypto values or private cryptographic keys stored with them by the user. Information obligations may also apply to crypto depositors.

### Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Electronic payment systems are primarily regulated under the PSD2 rules. The respective implementation laws also include rules governing third-party access to digital information in bank accounts.

### Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Third parties can be used. However, certain rules apply under the German Money Laundering Act stating, for example, that the responsibility under the law cannot be passed on to third parties.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

Certain registries are responsible for the allocation of a second-level domain under a top-level domain. For the geographical top-level domain .de, this is DENIC. DENIC registers the domain if it meets the requirements for registration contained in the domain guidelines and is not already registered for a third party. The domain holder has a transferable right of use under the contract with DENIC. In the case of a transfer of a .de-domain, a document containing the parties, domain and price is sufficient.

It is possible to register a country-specific domain name without being a resident in the country.

There are no restrictions around the use of URLs to direct users to websites, online resources or metaverses. In exceptional cases, however, a link to another website, online

resource or metaverse may be problematic if illegal content is made available on the linked website, online resource or metaverse and the company using such link adopts this content as its own, which could also be the case by implied action.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

In principle, domain names or URLs (ie, the term or combination of terms used in the domain name) can be subject of trademark or copyright protection under German law. However, due to the stringent requirements for a copyright-protected work, copyright protection is only conceivable in exceptional cases, if at all, while trademark protection is likely to be much more frequent in practice.

Under certain circumstances, the owner of a trademark (or a copyright, although this case is likely to be much rarer) may take action against a conflicting – identical or similar – domain. However, such an action is usually only promising if goods or services are offered on the domain which are identical or similar to the goods and services protected by the trademark. An exception only applies if the trademark has reputation in Germany or is a well-known mark. It is important to note that, as a rule, only injunctive relief can be demanded; a claim to transfer the domain exists only in exceptional cases.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

Advertising on the internet must comply with the Act on Unfair Commercial Practices (UWG), which regulates the market behaviour of individual companies. This Act determines that 'unacceptable nuisance' to market participant is illegal. An unacceptable nuisance is always assumed where advertising uses a medium that is suited to distance marketing and through which a consumer is persistently solicited, even if they have expressed an objection. An unacceptable nuisance is also assumed if advertising uses a medium:

- where the identity of the sender on whose behalf the communication is transmitted is concealed or kept secret;
- that violates section 6(1) of the Telemedia Act (TMG);
- that prompts the recipient to visit a website that violates section 6(1); or
- that provides no valid address to which the recipient can send an instruction to cease sending them further messages of that nature, without incurring costs other than transmission costs pursuant to the basic rates.

This means that advertising must always be labelled as such. If AdWords, banners and pop-ups are used, they must correctly disclose their commercial character and may need

to be appropriately labelled. Influencer marketing and viral marketing (eg, refer-a-friend schemes) should not be surreptitious advertising. Electronically supported refer-a-friend schemes have been extensively restricted in recent case law.

Digital businesses must also comply with data protection laws and the TMG. This particularly applies to tracking for advertising purposes and retargeting analysis of cookies, as well as to the use of 'like' buttons or Facebook custom audiences. In principle, it is necessary to obtain the prior express consent of the users in order for the processing of data to be lawful. In addition, the consumer must always be informed about the purpose of the data processing.

In addition, the same laws apply to online advertising as to print advertising – for example, copyright, personal and publicity rights or information obligations regarding guarantees under the Civil Code, Battery Act or Electrical Act.

## Targeted advertising and online behavioural advertising

### 18 What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

According to a European Court of Justice ruling (Case C-673/17 – *Planet49*), the prior express consent of the users is required both for the use of cookies (exception: technically necessary cookies) and the use of analysis tools such as Google Analytics. The requirement of prior express consent regarding cookies, targeting with or without cookies or other tracking technologies has now also been legally implemented in Germany, namely, in section 25 of the German Telecommunications-Telemedia Data Protection Act.

However, the individual requirements of such consent have not yet been conclusively clarified. Particularly, the General Data Protection Regulation (GDPR) requires informed consent, which means that users must know what they are consenting to. Therefore, comprehensive information must be provided on the specific use of cookies or other analysis tools. In practice, user consent is usually obtained via 'cookie banners'.

Importantly, the area of targeted advertising and online behavioural advertising will be subject of an European regulation, the ePrivacy Regulation, which will establish uniform requirements throughout Europe. However, it is not yet foreseeable when this regulation will be adopted and enter into force.

## Misleading advertising

### 19 Are there rules against misleading online advertising?

The handling of misleading online advertising is governed by the UWG. Advertising is therefore misleading if it contains untrue or other information that could be misleading about certain circumstances. Prior proof in advance confirming the advertising statement is not required. It requires proof of the correctness of the statement to be provided only in court proceedings. This, in turn, must be subject to high standards. If studies are provided as evidence, they must be carried out and evaluated according to recognised rules and principles of scientific research.

Read this article on Lexology

In some cases, there are industry-specific regulations that are applicable in addition to the UWG. For example, within the framework of the Therapeutic Products Advertising Act, scientific evidence is required for advertising claims whose alleged therapeutic efficacy is disputed by experts, or for advertisers who do not have scientifically substantiated research results.

### Restrictions

**20** Are there any digital products or services that may not be advertised online?

In principle, any digital product can be offered online. However, in some cases, sector or product-specific laws must be observed. For example, media (films, photos, games, etc) that glorify violence, are pornographic or contain other content that is subject to the protection of minors may not be offered online without the appropriate permissions. Consequently, any business seeking to sell products online should ensure that the products are advertised and offered according to such sector or product-specific law.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

The recipient's prior express consent is required for advertising using an automated calling machine, a fax machine or email (see section 7(2) No. 3, UWG). This applies regardless of whether the recipient is a consumer or another market participant. The consent of an email recipient should be verified for the purpose of proof (double opt-in). Email marketing without consent is only permitted in an existing customer relationship, if certain conditions are met (see section 7(3), UWG). Neither the sender nor the commercial character of the message may be concealed (section 6, TMG). In addition, the requirements of the GDPR must be met.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

The liability of providers is regulated in the Telemedia Act (TMG). According to this, providers are only responsible for their own content (section 7(1), TMG). Hosting providers are generally not responsible for the content. It would be unreasonable to expect them to check all content. However, as soon as indications of infringements have been given, the host provider is obliged to block the infringing content and to prevent similar infringements (section 10, TMG). Website providers and other telemedia providers are fully responsible for their own content. They are also responsible for the content of third parties (eg, when using user-generated content). These providers are also liable for links to illegal content, at least at the time they become aware that the content is illegal.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

The liability of providers is regulated in the TMG. According to this, providers are only responsible for their own content (section 7(1), TMG). Hosting providers are generally not responsible for content – it would be unreasonable to expect them to check all content. However, as soon as indications of infringements have been given, the host provider is obliged to block the infringing content and prevent similar infringements (section 10, TMG). The online platforms or content providers are not liable if they have implemented a functioning notice and take-down procedure according to these principles. There are no prior obligations to post any notices in this regard.

Website providers and other telemedia providers are fully responsible for their own content. They are also responsible for the content of third parties (eg, when using usage-generated content). These providers are also liable for links to illegal content, at least at the time they become aware that the content is illegal.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Providers can generally remove defamatory or infringing content without permission if it is legally established that the content is illegal, unless, for example, the content is protected by secrecy of telecommunications.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

In principle, databases and compilations can be protected under German copyright law if the selection or arrangement of the individual elements constitutes a personal intellectual creation. However, the purely technical, schematic or routine selection or arrangement of data is not sufficient. Also, the simple sequencing of data does not constitute a personal intellectual creation. Databases that do not constitute a personal intellectual creation enjoy minor protection if the database was accompanied by a high capital investment. The protection, however, covers only the database in its entirety or substantial parts of it and only for 15 years after its creation. The rights holder can legally stop other people from using a protected database by means of notices (cease-and-desist letter). If the infringing party refuses to sign a cease-and-desist declaration, the rights holder may file for an interim injunction at a competent court. The court may grant the injunction with the cease-and-desist injunction combined with an obligation to pay a penalty for future infringements. The

rights holder may also claim damages suffered by the infringement for the use of databases without a valid licence, which are calculated via a licence fee analogy. In addition, the rights holder may assert claims for information, which are very burdensome in practice. Practically, the rights holder can protect works by technological measures pursuant to section 95a et seq of the German Copyright Act (UrhG). Technological measures are technologies, devices and components that, in the normal course of their operation, are designed to prevent or restrict acts, in respect of protected works or other subject matter protected pursuant to the Act on Copyright and Related Rights, that are not authorised by the rights holder. Examples of technological measures include encryption technologies, filter systems, digital rights management systems, geo-blocking measures, etc. According to section 95a UrhG, there is a prohibition on circumventing technological measures, which is accompanied by a prohibition of corresponding preparatory and support actions.

## Third-party links and content

### 26 Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

A simple link to a third-party website does not infringe copyright or competition law and therefore requires no permission if the content is public and not protected (ie, by a paywall). The nature of a hyperlink is not to reproduce the linked content, but to provide simple access to it.

Exceptions are external links – that link a source directly (deep link), are not marked or cannot be identified as such and thus give the impression that the linked content originates from the owner's website.

### 27 Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Open content can be used on websites without express permission from the third-party content provider as long as the use complies with the terms of the licence in question (ie, Creative Commons). Furthermore, the automated use of digital content must not be expressly prohibited, as regulated by section 44b UrhG. However, such a prohibition must be stored in machine-readable form.

The use of content protected under IP rights without a licence may lead to legal action by the rights holder. In a first step, the rights holder will usually send a cease-and-desist letter. There is no immediate fine associated with receiving cease-and-desist letters. The only monies to be paid, initially, are legal and administrative fees by the rights holder prior to any court proceedings. The cease-and-desist letter usually requests the website owner to stop the infringement and sign an undertaking promising to pay a contractual penalty in case of culpable infringement with a penalty clause. If the website owner signs an undertaking and pays up the legal costs involved (usually between €300 and €2,000), the complaint will most likely not result in a court action as the claim will lose its substance. If the website owner signs a cease-and-desist declaration with a penalty clause and nevertheless continues its practice, then the contractual stipulated penalty or an amount established by the court of typically around €5,000 for the first infringement (also depending on scope, impact and

gravity of the infringement) is due and payable to the contracting partner. If the website owner refuses to sign the cease-and-desist declaration, the rights holder may file for an interim injunction at a competent court. The court may grant the injunction with the cease-and-desist injunction combined with an obligation to pay a penalty for future infringements. The rights holder may also claim damages suffered by the infringement for the use of the content without a valid licence, which are calculated via a licence fee analogy. In addition, the rights holder may assert claims for information, which are very burdensome in practice.

If the infringement was intentional, the consequences can even be of a criminal nature, with an impending penalty of up to three years in prison.

Particularly in the case of automated scraping, data protection issues can arise when personal data is reproduced or further processed. This is only permissible with explicit consent or a legitimate interest.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

In theory there is no difference in establishing or defending copyright, database rights and trademarks on a metaverse. From a practical point of view there might be a problem regarding the enforceability of rights, as it might be hard to find out who is responsible for the metaverse. Therefore, it might be difficult to engage in court proceedings with the responsible entity or person.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Yes, all IP rights are subject to the concept of exhaustion or first-sale doctrine. It is a prerequisite that the product containing the IP rights has been placed on the market by the owner of the IP rights or with his or her consent in Germany, in one of the other member states of the European Union or in another state party to the Agreement on the European Economic Area. The concept of exhaustion or first-sale doctrine is explicitly also applicable to software. There is no similar provision for other digital products, therefore there is no concept of exhaustion or first-sale doctrine.

Whether the concept of exhaustion or first-sale doctrine applies to digital products placed on a metaverse therefore depends on whether the rights are embedded in software. Placing digital products on a platform in another territory does not affect the legal situation in Germany.

### Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Criminal justice authorities can order freezing injunctions, as well as the search of premises and the confiscation of evidence in criminal investigation proceedings in connection with IP infringements.

Measures conducted by customs authorities, in particular border seizure procedures, are also of great practical importance.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Civil remedies include, in particular, claims for injunctive relief, removal and damages. Injunctive relief is often granted on an interim basis by preliminary injunction, which can be issued ex-parte within a few days after filing. German law also provides for a legal instrument comparable to freezing orders under British law if there is a real likelihood of assets leaving the country (arrest). However, this legal remedy is rarely applied in IP disputes.

In addition, legal remedies are available to the rights holder to counteract potential difficulties in gathering evidence: the information claim includes entitlement to demand information on the provenance and distribution channel of the infringing goods; the inspection claim includes entitlement to demand the submission of documents and the inspection of objects, provided there is a 'reasonable likelihood' of an infringement.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

The term 'personal data' is defined in the General Data Protection Regulation (GDPR) as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Beyond that, sensitive data (ie, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership or data concerning health) occupies a special position. The processing of sensitive data is only permitted under certain strict conditions.

## Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Data controllers themselves do not have to register with any regulator; however, the controller shall designate a data protection officer if they constantly employ as a rule at least 20 persons dealing with the automated processing of personal data. The data protection officer has to be named to the competent supervisory authority.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

Yes, the GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or the monitoring of their behaviour as far as their behaviour takes place within the EU.

Where the above-mentioned applies, the controller or processor seated outside the EU shall designate in writing a representative in the EU. This representative shall be established in one of the member states where the data subjects concerned are resident.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

The question is difficult to answer because there are no statistics in this respect. From our experience, data processing is often based on the fulfilment of the contract, legal obligations or the legitimate interest of the controller. In addition, consent is obtained in many cases, unless another reason for processing is apparent.

In addition, the transfer to third countries is usually based on the standard contractual clauses of the European Commission or adequacy decisions.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

When transferring data to another jurisdiction, a distinction must be made between EU member states and other jurisdictions. The transfer of data to other member states is

based on the same rules as a data transfer within Germany. In the case of a transfer outside the EU, the corresponding provisions of the GDPR (article 44 et seq) must also be observed. In addition to the fundamental legality of the data processing, it must also be checked for the transfer to the respective country. Various options are available here. As a rule, the transfer to third countries is based on an adequacy decision of the European Commission or the Standard Data Protection Clauses. In addition, international corporations can introduce binding corporate rules. In individual cases, further legal processing options are available.

No general rules exist that require data, data servers or databases to remain in the German jurisdiction.

## Sale of data to third parties

### 37 | May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

There is no specific German rule on selling personal data. The GDPR neither allows nor explicitly permits the selling of data to a third party. Licensing data requires a legal basis for the data processes. Consent might work. The debate is ongoing, if legitimate interest works regarding selling data, for example, as part of an M&A asset deal, if certain requirements are met. The party's liability is that they might violate the GDPR.

## Consumer redress

### 38 | What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Individuals have the right to information, access, rectification, erasure, restriction of processing, data portability, object and not to be subject to a decision based solely on automated processing (articles 13 to 22, GDPR) in relation to the processing of their personal data. Damages resulting from an infringement of the GDPR have to be compensated (article 82, GDPR). These rights have to be complied with by all controllers or processors in the EU, regardless of the nationality of the individual or where the data is processed. They apply to all individuals who are in the EU when offering products or services towards them.

## Non-personal data

### 39 | Does the law in your jurisdiction regulate the use of non-personal data?

Under German data protection law, section 25 of the German Telecommunications-Telemedia Data Protection Act (TTDSG) applies to the protection of non-personal data. This section is the German implementation of article 5 (3) of Directive 2002/58/EU (the Cookie Directive).

In accordance with section 25 (1) of the TTDSG, the storage of information in the end user's terminal equipment or access to information already stored in the terminal equipment shall only be permitted if the end user has consented on the basis of clear and comprehensive information. The information to the end user and the consent shall be provided

in accordance with the GDPR (especially articles 7, 12, 13 and 14). 'Information' can be personal or non-personal data.

In accordance with section 25 (2) of the TTDSG, consent is not required if:

- the accessing or storing (or both) of information is solely necessary to carry out the transmission of a message over a public telecommunications network; or
- the accessing or storing (or both) of information is absolutely necessary for the provider of a telemedia service to be able to provide a telemedia service expressly requested by the user.

In addition, in Germany, the EU Data Act will regulate the use of non-personal data, once it is in force.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

In general, documents can be archived digitally. The most common laws and regulatory guidelines with regard to archiving of documents do not explicitly require documents to be archived in paper form. However, there are laws that require documents to be archived in their original form, which therefore may require the documents to be archived in paper form. This is most prominently the case for annual financial statements, opening balance sheets and certain documents in customs procedures (information to the customs authorities and supporting documents required for the application of the provisions governing the customs procedure), according to section 147(2) of the German Fiscal Code.

In explicitly listed cases, the law requires documents to be notarised in order to become valid, in particular regarding the acquisition of real estate, the founding of particular legal corporations (GmbH) or the transfer of shares in such a legal corporation. The German legislator has provided new regulations that all notarised deeds have to be archived additionally in an electronic vault of deeds. Still, this will not remove the obligation to archive the original deed as well.

Original digital documents such as electronic invoices must be kept in the digital original; they may not be changed or deleted within the retention period, and a tax auditor must be able to evaluate them mechanically.

The question of the obligation to retain certain documents as original documents must be distinguished from the probative value of documents. Under German procedural law, the probative value of original documents is often considered higher than that of electronic copies (presentation of the original or certification of a copy may be required). For this reason, it might be advisable to (additionally) retain the original documents even if there is no obligation to retain them.

Read this article on Lexology

The probative value should especially be considered with regard to contracts, which are subject to the written form requirement according to section 126 of the German Civil Code. While the written form ('wet ink on paper') as required by respective laws and contracts can basically be replaced by a qualified electronic signature according to section 126a of the German Civil Code, there are technical aspects regarding the archiving of such documents that need to be considered.

Any archiving of documents should always be in line with the banking authorities' principles of proper accounting.

## Retention

### 41 Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

The most important laws regarding the archiving of documents are section 147(3) of the German Fiscal Code and section 257(4) of the German Commercial Code. They require archiving of documents for six or 10 years. However, data privacy laws may require you to block access to these documents during the retention periods, in case they contain personal data which are not eligible to be accessed by everyone after a certain period of time.

According to German tax law, all business documents that are of importance for understanding and verifying the records required by law must be kept for either six or 10 years. Section 147(1) of the German Fiscal Code lists the individual documents that must be kept, namely:

- accounts and records, inventories, annual financial statements, situation reports, the opening balance sheet and the operating instructions and other organisational documents needed for their comprehension;
- trade or business letters received;
- reproductions of trade or business letters sent;
- accounting records;
- information to the customs authorities and supporting documents required for the application of the provisions governing the customs procedure; and
- other documents to the extent that these are of relevance for taxation.

According to section 257 of the German Commercial Code, the retention period for books and records, annual accounts, inventories, management reports, opening balance sheets, accounting vouchers, documents required to be attached to a customs declaration made by means of a data processing technique where the customs authorities have waived their presentation or returned them after presentation, and invoices shall be 10 years. All other business documents subject to retention shall be retained for six years. The period always begins with the expiry of the calendar year in which the last entries, changes or actions were made in the respective documents, or commercial letters were received or dispatched. In the case of contractual documents, the period begins after the expiry of the contract.

In addition to the central tax law provision of section 147(1) of the German Fiscal Code, German law contains further retention obligations in special laws (ie, banking laws) that

apply to specific documents and specific industries. In this respect, an examination of the individual case is always necessary.

Further documents that are required for the assertion of legal claims can and should be archived for at least three years (regular statute of limitations).

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

All companies must protect personal data according to the General Data Protection Regulation (GDPR), and in accordance with the German Telecommunications-Telemedia Data Protection Act (TTDSG).

This also applies to internet transactions. Encryption is not mandatory, but it is regularly a suitable measure according to article 32 of the GDPR. In addition, providers of internet or telecommunications services (for example, internet service providers) must take appropriate technical measures to protect against disruptions (section 19(4), TTDSG; section 165, German Telecommunications Act).

With regard to the implementation and maintenance of appropriate measures, the state of the art must always be taken into account; in other words, the requirements automatically increase with technical progress. However, German law does not specify details, such as encryption algorithms or key lengths.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

The general rules of the GDPR regarding data breach notification apply for e-commerce as well. In particular, article 4 (defining a breach and personal data), article 32 (setting the rules for IT security to be followed), articles 33 and 34 (setting the rules for notifications and communication about personal data breaches) and article 82 (implementing a damage claim for affected data subjects), as well as article 83 (imposing severe fines for infringing the applicable rules), are applicable. Moreover, in Germany, the German Federal Data Protection Law of 25 May 2018, in particular section 29 (regarding a limit to the information duties of the controller), section 64 (providing a list of required technical and organisational measures that have to be implemented to ensure the security of data processing; directly applicable only to law enforcement and judiciary but indirectly also to their private sector data processors or as mutually adopted contractual obligations for private sector

controllers) and section 83 (implementing the data subject's right to claim immaterial damages in addition to other damages and regulatory fines), has to be respected.

Data breaches have to be reported whenever there is a risk that somebody from outside or inside an organisation has gained access to the personal data of an EU citizen that has not been authorised by the law or the consent of that person; the controller or processor has to scrutinise the incident as well as the potential consequences.

Any such violations of the privacy of personal data have to be notified to the supervisory authorities unless the risks for affected persons are excluded (eg, due to encryption). The reporting has to take place within 72 hours with concrete information as well as additional documentation of the incident and the countermeasures taken.

If there are in addition high risks to the rights and freedoms of natural persons (eg, financial and social harm, identity theft or professional secrecy), the controller has to inform the person concerned immediately, unless technical protection against the risks (eg, encryption) is provided. The supervisory authority may order the publication of a public notice of the incident.

A breach of reporting obligations in the event of data breaches can be sanctioned with a fine of up to €10 million or 2 per cent of the annual turnover achieved worldwide. Moreover, data subjects affected by the data breach are entitled to claim material and even immaterial damages caused by the controller's failure to report to the regulators and inform the data subjects in a timely manner.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Authorities cannot require users to reveal their private keys used for encrypted communications. Certification authorities are permitted. Their operation is regulated by the Regulation (EU) 910/2014 of 23 July 2014 (the eIDAS Regulation) and supplementary national law, in Germany the Trust Services Act. Liability is regulated in articles 11 and 13 of the eIDAS Regulation. If the trust service provider contracts with third parties, liability is increased according to section 6 of the German Trust Services Act.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

In Germany, any kind of gambling, including online betting and fortune-based gaming business, is generally forbidden, with only specific exceptions that are heavily regulated under

the State Treaty on Gambling and require a state licence to operate in the German market. By definition under the State Treaty, gambling requires any kind of consideration for participation (betting or gambling for free or without wager therefore does not fall under the regulatory scheme). After a long period of legal uncertainty due to European jurisdiction regarding the old State Treaty, Germany finalised its new State Treaty on Gambling, which entered into force in July 2021. Under the new State Treaty, it is now generally possible to also acquire licences for online casinos, online poker and virtual slot machine games (besides lotteries, sports betting and horse betting). The State Treaty on Gambling stipulates a multitude of prohibitions and requirements for the acquisition of an official licence. Requirements of any such licence under the State Treaty include participation in a digital prevention system, extensive monetary securities and background checks. Any advertisement for unlicensed gambling is strictly forbidden and may also constitute a criminal offence (as can the operation of any unlicensed gambling activity). The same may apply to payment service providers in regards to unlicensed gambling of any kind. The competent authority in Germany is, at the moment, the regional council of Darmstadt.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

It is only permissible to advertise, or provide access to, an online betting or gaming business in the German market that is licensed in Germany. Licences of other jurisdictions do not hold any validity in Germany in this regard, since the new State Treaty on Gambling came into force in July 2021. If the respective metaverse is considered to address the German market, the same applies. However, if online betting or gambling businesses in other jurisdictions are accessible from Germany but do not address the German market, German regulation might not apply.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

It is highly important to define the exact scope of the services and the quality. The quality is normally provided in service level agreements. The agreement has to contain specific provisions as to the cooperation obligations of the customer. Other key issues are provisions regarding the migration of data and the cooperation of the service provider after termination of the contract to switch to a new service provider.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

As far as data is concerned, where there is a professional secrecy obligation or where sensitive data according to the General Data Protection Regulation is concerned, additional rules have to be complied with. Banking is the other area in which additional requirements have to be complied with (eg, MaRisk).

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

As there is no general outsourcing law, there is no such requirement. However, there are sector-specific regulations – for example, in banking there are requirements as to the minimum regulations an outsourcing agreement has to contain (eg, European Banking Authority Guidelines, MaRisk).

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

If an operation or part of an operation is moved to the service provider, the employment contracts of the relevant employees are moved to the service provider by power of law. The employees have to be informed in advance. The employees have the right to object to the transfer of their employment.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

There are, as at the time of writing, no specific regulations governing artificial intelligence (AI). However, the general legal framework provided by German law also applies to the development, training, deployment and use of AI:

Training data in particular may be protected by copyright under the German Copyright Act (UrhG). Using any such data thus usually requires a license by the copyright holder. Also, certain data may be subject to statutory or contractual confidentiality obligations, and thus not be suitable for being used as training data.

Where personal data are used in the development or training of an AI system, the requirements and restrictions provided by data protection law, particularly under the General Data Protection Regulation (GDPR) apply and must be adhered to. Given that data used for training an AI model cannot be extracted or deleted from the trained AI afterwards, obtaining an individual's consent (article 6, paragraph 1, lit a, GDPR; article 9, paragraph 2, lit a, GDPR) often is not a viable option in practice, given the right to withdraw such consent at any time. Establishing a legal basis for the processing of personal data to train AI can hence be challenging.

Furthermore, article 22 of the GDPR must be complied with. According to the principle established in article 22, paragraph 1, data subjects shall not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. While article 2, paragraph 2 of the GDPR provides a few exceptions, it is often doubtful whether the requirements of these exceptions are met in practice.

According to article 35, paragraph 1 of GDPR, the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, where a type of processing – in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons. In particular, an assessment shall be required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural persons, or similarly significantly affect the natural persons.

The EU is currently working on a regulatory framework to provide binding rules for safe and transparent AI (the AI Act) that particularly addresses the development, distribution and use of AI Systems in the European Union. The proposal provides certain rules for the development of AI systems that are distributed and used in the EU based on the level of risk a given AI model may pose or individuals and society, and also sets forth specific requirements for the data that is used to train an AI model. Under the current proposal for the AI Act providers of high-risk AI systems are obliged to provide comprehensive information on how the AI model was developed.

## IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Training data can be protected by the UrhG as a representation of a scientific or technical nature according to section 2, paragraph 1, No. 7 of the UrhG, as a database according to section 4, paragraph 2 of the UrhG, section 87a et seq of the UrhG, and the German Trade Secrets Act.

Read this article on Lexology

However, the protection of products created by AI is problematic under the current legal framework. This is best illustrated using the example of German Copyright Law: according to section 2, paragraph 2 of the UrhG, copyright exists only for personal intellectual creations. For the copyrightability of a product, it is therefore decisive whether and to what extent it can be traced back to the creative activity of a natural person. Thus, pure AI works are not works within the meaning of section 2, paragraph 2 of the UrhG. However, if the AI work is edited by a natural person and thus achieves a corresponding level of design, it can enjoy copyright protection. Consequently, the more autonomously the AI works on such a creation, the less likely it is that it will be protected by copyright. While there is a discussion in German legal literature, whether prompts (eg, prompts entered in AI-powered chatbots or large language models) may lead to some kind of copyright in the results returned by the AI, the prevailing view is that this is not the case.

## Ethics

### 53 Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

No, there are currently no statutory rules in place in Germany on ethics of AI or machine learning.

However, the EU's current proposal for an AI Act is somewhat based on an ethic ruleset. The AI Act follows a risk-based approach that categorises AI systems into four classes, each of which is subject to a different level of regulation: low, limited, high and unacceptable risk.

AI systems that are considered an unacceptable risk are prohibited in the EU. Examples are, based on the current proposal, real-time biometric remote identification AI systems in publicly accessible spaces and AI systems used for social scoring that lead to discrimination in social contexts.

For the remaining three risk classes, the higher the risk, the more extensive the legal requirements. For example, AI systems that are considered high-risk are not prohibited but are subject to stringent requirements with respect to their development, distribution and deployment. The AI Act imposes various obligations onto developers and distributors, including with respect to quality and risk management, technical documentation, and oversight, robustness, safety, and accuracy of the AI system. According to the current proposal, any such AI system must be registered in an EU-wide database.

For AI systems with limited or low risk, the AI Act primarily provides for certain transparency requirements and notification obligations.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Regarding Income Tax and Corporate Income tax, there are no special rules; the permanent establishment approach applies. The ordinary Income Tax or Corporate Income Tax rate applies for profits derived from those transactions if they are made from a German permanent establishment.

Regarding value-added tax (VAT), it is necessary to distinguish: in the case of online sales (e-commerce), the decisive factor is whether the complete process is carried out via the internet (ie, ordering and delivery of the article), or whether only the order is placed via the internet and delivery is carried out in the conventional way. Only in the first case are sales 'online sales' according to section 3a, abs 4, No. 14 of the USTG (VAT); in the second case, it is a matter of normal mail order business in the form of moving goods (offline sales).

Both sales are subject to taxation. The download of software is an electronic service, which is basically carried out at the place of residence of a private person in an EU country and is subject to VAT according to local law. This results from section 3a, abs 5 of the USTG (applicable since 1 January 2015). Accordingly, a download by a German citizen from a server in another EU country is subject to German VAT.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

A server establishes a permanent establishment, which is taxable within its jurisdiction, if the functions performed on the server or place are 'significant and essential' or attributable to the core part of the entity's operations.

The tax authorities assume this significant and essential function if there is not only a secondary or ancillary activity.

Hence, a foreign company with a dedicated server physically placed on German soil (still) creates a permanent establishment in Germany. However, vice versa, running a platform for the German market or a virtual market is not sufficient for creating a permanent establishment in Germany if there is no physical link to German soil.

Nevertheless, regarding VAT, serving the German market might be sufficient for triggering German VAT (see above).

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The Value Added Tax Act contains a detailed regulation dealing with the requirements for invoices. The law explicitly states what information has to be shown in an invoice. Regarding e-invoicing, there are no special requirements or formats to be fulfilled. However, for e-invoices the same requirements apply as for paper invoices: the business must ensure that the content of the invoice cannot be changed. It is the business owner's choice how he or she does that, for example by internal controls enabling a tracking path. In any case, it must be possible to explain and prove who the issuer of the invoice is.

For e-invoicing generally, the consent of the other party is necessary and should be asked for in advance.

Copies of all (types of) invoices have to be kept in the books and records of the business, and must be presented to the auditor in tax audits. Meanwhile, tax audits generally take place via electronic access to the files and records.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no such specialist courts. There are also no special chambers in the ordinary courts for these issues.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

If goods or services are sold online to consumers, the merchant can use the online dispute resolution platform of the European Commission. The merchant must inform the consumer before concluding the contract whether he or she is willing to participate or not. However, ADR is not very common in Germany, though certain sector-specific initiatives exist.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

Significant legislative changes have come into force in recent years (Digital Markets Act, Digital Services Act, New Deal for Consumers, etc) and, with the EU's declaration in December 2022 of its Digital Decade policy programme, many more are yet to come. The programme will include numerous legislative initiatives aimed at driving digital transformation in Europe up until 2030. One major topic will be Artificial Intelligence (AI) and AI-generated content (see the Artificial Intelligence Act and the AI Liability Directive). The EU's aim is to regulate AI in an attempt to harness the potential of this technology while ensuring the safety and trust of EU citizens.

* *The following authors have also contributed to this chapter: Oliver M. Bühr, Lara Guyot, Maximilian König, Christoph Krück, Moritz Mehner, Daniel Messmer, Matthias Orthwein, Corinna Schneiderbauer, Heiko Wunderlich.*

SKW Schwarz

| | |
|---|---|
| Jens Borchardt | j.borchardt@skwschwarz.de |
| Franziska Ladiges | f.ladiges@skwschwarz.de |
| Elisabeth Noltenius | e.noltenius@skwschwarz.de |
| Stefan Peintinger | s.peintinger@skwschwarz.de |
| Johannes Schäufele | j.schaeufele@skwschwarz.de |

Ludwig-Erhard-Strasse 1, Hamburg 20459, Germany
Tel: +49 40 334 010
www.skwlaw.de

# Gibraltar

Michael Nahon, Andrew Montegriffo, Tim Garcia, Claire Pizzarello and Hannah Lopez

Hassans

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The Government of Gibraltar is proactive and firmly committed to developing this space. It is keen to position Gibraltar as a leading hub for online and digital commerce (as evidenced by, for example, its pioneering approach to distributed ledger technology/blockchain legislation, and development and nurturing of the remote gambling industry).

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

The following form the key body of law in this field:

- Consumer Rights on Contracts Regulations 2013;
- Unfair Terms in Consumer Contracts Act 1998;
- Consumer Protection;
- Unfair Trading Act 2008;
- Misleading and Comparative Advertising Act 2002;
- The Electronic Commerce Act 2001;
- Gambling Act 2005;
- Financial Services Act 2019;
- Communications (Personal Data and Privacy) Regulations 2006;
- Gibraltar General Data Protection Regulation and Data Protection Act 2004;
- Communications Act 2006; and
- Civil Contingencies Act 2007.

### Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The following are the regulatory bodies responsible for this area:

- Gibraltar Regulatory Authority;
- Gibraltar Financial Services Commission;
- Business Licensing Authority;
- Office of Fair Trading; and
- Gambling Commissioner.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

The applicable rules and tests will differ depending on the domicile of the parties. Where the defendant is domiciled in an EU member state, the Gibraltar courts will apply Regulation (EU) No. 1215/2012 on Jurisdiction and the Recognition and Enforcement of Judgments (Brussels Recast Regulations). This forms part of Gibraltar's retained EU law. The Brussels Recast Regulations state that parties can agree jurisdiction clauses in their private contracts and this will be upheld by the courts. However, should the party bringing proceedings or the defendant be a consumer, regardless of any exclusive jurisdiction clauses agreed between the parties, the consumer may bring proceedings in the courts of the place where he or she is domiciled. Should a legal entity bring a claim against a consumer, the proceedings must be brought in the courts where the consumer is domiciled. Other regimes that may be applied (depending on the domicile of the defendant) are the Lugano Convention 2007, the Hague Convention on Choice of Court Agreements 2005 on exclusive choice of courts agreements, and the common law regime, all of which are likely to have a similar outcome to the EU regime as explained above. These rules have not yet been applied by the courts in relation to the metaverse.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

The regulatory and procedural requirements governing the establishment of digital businesses are found in the Companies Act 2014 and Fair Trading Act 2015. There are no differences between the requirements and procedures governing them and the establishment of brick-and-mortar businesses. The Consumer Rights on Contract Regulations 2013 and the Electronic Commerce Act 2001 provide rules and requirements for the sale of digital content in Gibraltar. These cover, for example, information that must be provided prior to concluding a distance contract, how distance contracts must be confirmed and cancellation periods.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

This is possible, however section 5(2) of the E-Commerce Act 2001 specifically prohibits contracts in connection with any of the following from being concluded through electronic means:

- conveyancing or transferring land or any interest in real property;
- rights of succession under a will or other testamentary instrument; and
- categories excluded by regulations made by the Minister.

Caution also needs to be taken when a signature needs to be witnessed. For example, it is not clear whether a document can be notarised via video conference.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

There are no laws that limit this.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Section 8(2) of the Gibraltar Electronic Identification and Trust Services for Electronic Transactions Regulations 2017 define electronic signature as:

> *anything in electronic form that–*
>
> *(a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and*
> *(b) purports to be used by the individual creating it to sign.*

There is no requirement for digital or e-signature providers to be registered or licensed in Gibraltar; however, the EU Electronic Identification Regulation (eIDAS), which forms part of Gibraltar's retained EU law, sets out various types of electronic signatures. Qualified electronic signatures are said to have the equivalent legal effect as a handwritten signature. Article 3(12) of eIDAS defines a qualified electronic signature as an advanced electronic signature that is created by a qualified electronic signature creation device, and which is

based on a qualified certificate for electronic signature. The qualified certificate must be issued by a verified, qualified trust service provider and their credentials must be recorded in a trusted list.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

None particular to Gibraltar, although parties are free to submit to their agreed choice of alternative dispute resolution, including online dispute resolution providers of their choice by mutual consent.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

Yes, it is regulated by the Gibraltar Financial Services Commission (GFSC) pursuant to the Financial Services Act 2019 (FSA). The FSA restricts the circumstances in which it is possible for persons who are not authorised or exempt to advertise or otherwise encourage others to enter into agreements with persons carrying on regulated activities. For example, a person must not, in the course of business, communicate an invitation or inducement to enter or offer to enter into an agreement the making or performance of which by either party constitutes the carrying on of a regulated activity.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Yes, the FSA sets out a general prohibition that no person may carry on a 'regulated activity' in or from Gibraltar, or purport to do so, unless the person is an authorised person or an exempt person. Issuing electronic money and using distributed ledger technology (DLT) for storage or transmission of value belonging to another, by way of business, are 'regulated activities'.

The Proceeds of Crime Act 2015 (Relevant Financial Business) (Registration) Regulations 2021 prohibit certain businesses, namely, those that are not subject to supervision by a relevant supervisory authority and not registered with the GFSC, from:

- receiving proceeds in any form, whether on their own account or on behalf of another person, from the sale of tokenised digital assets involving the use of DLT or similar means of recording a digital representation of an asset; and
- exchanging, arranging or making arrangements with a view to exchange, by way of business, virtual assets for money, money for virtual assets or one virtual asset for another.

Read this article on Lexology

Other relevant pieces of legislation are:

- Financial Services (Electronic Money) Regulations 2020;
- Financial Services (Distributed Ledger Technology Providers) Regulations 2020;
- Proceeds of Crime Act 2015; and
- Proceeds of Crime Act 2015 (Transfer of Virtual Assets) Regulations 2021.

## Digital and crypto wallets

### 12 Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Yes, the FSA prohibits persons from carrying on the 'regulated activity' of using DLT for storage or transmission of value belonging to another, by way of business, in or from Gibraltar, or purporting to do so, unless the person is an authorised person or an exempt person. The Financial Services (Distributed Ledger Technology) Regulations 2020 set out the application process for obtaining the relevant permission to carry out a 'DLT Provider's business' (as defined in the DLT Regulations) and the regulatory principles that a DLT Provider must comply with.

The Proceeds of Crime Act 2015 (Relevant Financial Business) (Registration) Regulations 2021 prohibit certain businesses, namely, those that are not subject to supervision by a relevant supervisory authority and not registered with the GFSC, from:

- receiving proceeds in any form, whether on their own account or on behalf of another person, from the sale of tokenised digital assets involving the use of DLT or similar means of recording a digital representation of an asset; and
- exchanging, arranging or making arrangements with a view to exchange, by way of business, virtual assets for money, money for virtual assets or one virtual asset for another.

Other relevant pieces of legislation are:

- Proceeds of Crime Act 2015; and
- Proceeds of Crime Act 2015 (Transfer of Virtual Assets) Regulations 2021.

## Electronic payment systems

### 13 How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Electronic payment systems are regulated by the GFSC under the FSA and its subsidiary legislation, the Financial Services (Payment Services) Regulation 2020. Carrying on an activity that relates to payment services, by way of business, in or from Gibraltar, is a 'regulated activity' under the FSA.

The Financial Services (Payment Services) Regulations 2020 regulate third-party access to payment accounts for information services.

**Read this article on Lexology**

### Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Yes, the Proceeds of Crime Act 2015 (POCA) sets out rules to enable 'relevant financial businesses' to:

- rely on a person who falls within section 23(2) of POCA; or
- apply customer due diligence measures by means of an outsourcing service provider or agent, provided that the relevant person remains liable for any failure to apply such measures.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

There are no Gibraltar laws or regulations in place to regulate the licensing of domain names. However, Gibraltar's local provider of domain names reserves domain and subdomain names inclusive of '.gi', which is the country code top-level domain for exclusive use by Gibraltar-registered businesses and organisations, which may only use it for their own local services and purposes.

There are no restrictions around the use of URLs to direct users to websites, online resources or metaverses.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Domain names or URLS may be capable of being the subject of a trademark, and will assist in challenging a competitive use or registration of a similar domain name or URL. However, copyright is unlikely to subsist in a URL or domain name.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

The Electronic Commerce Act 2001 regulates information society services, providing rules on advertising and selling goods and services online. The Consumer Protection (Unfair Trading) Act 2008 applies to all commercial practices that happen before (through advertising or marketing), during and after a transaction has taken place in respect of the purchase of goods or services in Gibraltar, and bans aggressive or misleading commercial practices – this includes breaching or omitting information and advertising rules relating to a number of EU directives. There are currently no self-regulatory codes that apply. In addition, the Misleading and Comparative Advertising Act 2002 will apply. Regulated activities, such as gaming and financial services, will each have their own advertising restrictions.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Targeted and behavioural advertising involve the processing of personal data. As such, the Gibraltar General Data Protection Regulation will apply. Similarly, the use of cookies or other tracking technologies is prohibited unless they conform to the Communications (Personal Data and Privacy Regulations) 2006.

### Misleading advertising

**19** Are there rules against misleading online advertising?

Yes. This is covered by the Misleading and Comparative Advertising Act 2002, and by the Consumer Protection (Unfair Trading) Act 2008, which applies to business-to-consumer transactions. Essentially, advertising that provides false or untruthful information, deceives or is likely to cause the consumer to take a decision they would not otherwise have taken, is deemed to be a misleading practice and is not allowed. Under the Misleading and Comparative Advertising Act 2002 an advertiser can be required by a court to produce evidence of accuracy in respect of factual claims made.

### Restrictions

**20** Are there any digital products or services that may not be advertised online?

Any online advertising relating to illegal content, services or activity is unlawful; for example, under the Crimes Act 2011 it is an offence to advertise certain dangerous and indecent items.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

Direct marketing – namely, to individuals – must comply with the rules set out in the Communications (Personal Data and Privacy Regulations) 2006. The rules cover marketing via email, SMS, fax and telephone.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

There is no liability, assuming the host falls within the definition of intermediary service provider.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

Under the Electronic Commerce Act 2001, an intermediary service provider will not be subject to criminal or civil liability in respect of information published, provided they are not the originator of the material, have no actual knowledge of the offending material, have not modified it and upon discovery the offending material is removed and authorities notified. Further, since English common law applies, the *Byrne v Dean* principle will also be followed.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Yes. Section 9 of the Electronic Commerce Act 2001 obliges an intermediary service provider to remove such information as soon as possible after acquiring actual knowledge of its existence, to stop providing services in respect of that information as well as to notify the authorities with relevant facts, including where possible the identity of the individual behind it.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

Yes. These are covered in the Intellectual Property (Copyright and Related Rights) Act 2005.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Hyperlinking to online content is a communication to the public. Therefore, if the content is protected by copyright, permission from the owner is usually required.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Where scraped data comprises copyrighted work, this can lead to infringement including a breach of database rights. In addition, where the scraped data contains personal data, there may also be issues in regard to the Gibraltar General Data Protection Regulation.

### Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Potential difficulties could be encountered when trying to enforce copyright in a decentralised environment; trademarks offer protection in the relevant territory of the registered mark, and it may be challenging to demonstrate that any infringement occurred in the relevant territory. UK case law would apply, which suggests the adoption of a targeted approach, namely, whether the use in the metaverse was targeted towards consumers in a real-world territory where the trademark is protected.

### Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Yes, while the concept of exhaustion of rights exists under Gibraltar law, there would be challenges in applying this to digital assets following the ruling by the Court of Justice of the European Union in *Tom Kabinet* in December 2019.

### Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Yes. Under the Intellectual Property (Copyright and Related Rights) Act 2005 a magistrate may, on information given under oath by a constable, issue a warrant allowing entry and search of a premises using reasonable force to seize articles that evidence an offence. Injunctions can also be made against service providers where the service provider has actual knowledge of another person using their service to cause a copyright infringement.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

The following remedies are available: interlocutory relief, injunctions, damages or profits on account, delivery up.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Personal data is any information relating to an identified or identifiable living individual. It also includes special categories of personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data (for identification purposes), data on health, sex life and sexual orientation as well as crime-related data.

Where special category data is processed in addition to a lawful basis under the Gibraltar General Data Protection Regulation (GDPR), a controller also needs a Gibraltar GDPR article 9 lawful basis.

In addition, controllers will usually require an appropriate policy document that sets out additional safeguards followed when processing special category data. While anonymised data is not personal data and therefore outside of the GDPR rules, pseudonymised data is considered personal data and therefore should be treated in the same way as personal data.

## Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

There is no need for organisations that process personal data to register with the Gibraltar data protection supervisory authority – the Gibraltar Regulatory Authority (GRA). However, where processing requires the appointment of a mandatory data protection officer, the data protection officer must be registered with the GRA.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The Gibraltar GDPR (which retained in Gibraltar law the EU GDPR following the end of the Brexit transition period on 31 December 2020, with some local modifications) applies to the processing of personal data in Gibraltar. It sits side by side with Gibraltar's Data Protection Act 2004 and provides local exemptions and derogations to the Gibraltar GDPR. It applies to organisations established in Gibraltar and has extraterritorial provisions that apply to organisations not established in Gibraltar but which satisfy either the 'goods and services' test (ie, they offer goods or services to Gibraltar) or the 'monitoring' test (ie, they monitor the behaviour of individuals in Gibraltar). Where organisations are not established in Gibraltar, but because of their processing activities the Gibraltar GDPR applies via its extra-territorial provisions, they need to appoint a Gibraltar representative under Gibraltar GDPR, article 27.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

Article 6 of the Gibraltar GDPR sets out the lawful bases available to controllers in order to process personal data. These include: consent, contractual necessity, compliance with a legal obligation, public interest reasons and legitimate interests of the data controller or third party. Note consent should be avoided in an employment context, and where legitimate interests are relied on a legitimate interests assessment is needed before processing begins. Transfer of personal data to third countries outside Gibraltar is prohibited unless the transfer complies with the Gibraltar GDPR, Chapter V safeguards. Transfers to the EEA or the UK are not considered third-country transfers requiring safeguards, as are transfers to countries which if made from the UK would be permissible. Typical acceptable safeguards are the use of EU model clauses. However, where a country has no adequacy, it is recommended to carry out a country-specific Transfer Impact Assessment to ensure the country in question adequately protects personal data.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Following Brexit, the application of the Free Flow Non-Personal Data Regulation in Gibraltar was revoked and not replaced. While there are no general rules regarding specific data-localisation laws in Gibraltar, there is the possibility of sector-specific data localisation conditions being attached to Gibraltar licences conducting regulated business.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

The sale or transfer of personal data to third parties is permissible, provided that the seller and buyer both comply with applicable data protection legislation and intellectual property rights relating to databases in the Intellectual Property (Copyright and Related Rights) Act 2005. Depending on the seller's title to the database, the transaction can proceed by way of outright sale or under licence. Breaches of the Gibraltar GDPR (eg, failing to have a lawful basis or to comply with transparency requirements) can lead to fines amounting to the higher of €20 million or 4 per cent of global turnover for multinationals. Remedies for breach of database rights, including copyright, are interlocutory relief, injunctions, damages or profits on account, delivery up and criminal proceedings, among others.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Data subjects whose data has been processed in breach of the Gibraltar GDPR can complain to the GRA, being the data protection supervisory authority in Gibraltar. In addition, they have the right to bring a judicial action for damages through the Gibraltar courts. These rights are not limited to Gibraltar citizens and apply to any data subject the processing of whose personal data falls within the scope of the Gibraltar GDPR.

## Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

No, unless the business requires a sector-specific licence or regulatory oversight in which case it may be possible to regulate such data as part of the licence or regulatory requirements.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

No. However, Part III of the Electronic Commerce Act confirms that where there is a legal requirement to present or retain original documents, that requirement is met if a document is stored in electronic form provided that integrity and legibility assurances are met. In addition, where there is a statutory requirement to produce a document in paper form, that requirement is met if it is produced in electronic form.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Gibraltar law does not have any uniform and comprehensive legislation on records retention. Generally, documents are retained until the risk of litigation passes (eg, six years under the Limitation Act 1960 for actions in respect of simple contracts or tort), unless they need to be kept for title reasons such as title deeds or to comply with statutory or regulatory retention requirements, in relation to, for example, company books and accounts, the Income Tax Act, pension schemes, the Financial Services Commission and the Proceeds of Crime Act 2015.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

Article 32 of the Gibraltar General Data Protection Regulation (GDPR) sets out the standards required for security of processing personal data – a context-specific, risk-based approach. It requires organisations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing, taking into account state of the art, cost of implementation and the nature, scope, context and purpose of processing.

Similarly, the Civil Contingencies Act 2007 sets out security standards for essential services and digital service providers. Essential service providers need to take appropriate and proportionate measures to prevent and minimise impact of security incidents affecting their networks and information systems to ensure continuity of service appropriate to the risk posed, having regard to the state of the art available.

Read this article on Lexology

In addition, regulated businesses under the Financial Services Act 2015 are required to submit corporate governance arrangements, and this invariably requires cybersecurity measures to be included.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

There are mandatory data breach notification requirements regarding personal data under the Gibraltar GDPR. Where a breach poses a likely risk to individuals, organisations have up to 72 hours to notify the Gibraltar Regulatory Authority. In addition, if the breach is likely to pose a high risk to individuals, they need to be informed without delay. Under the Civil Contingencies Act 2007, where an organisation is designated as an essential service, mandatory notification requirements to local authorities exist regarding incidents that have a significant impact on continuity of the essential service. Similarly, digital service providers are required to make a mandatory breach notification to the authorities in the event of any incident having a substantial impact on the provision of services.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

There are no laws that allow bulk interception or acquisition of communications data. Applications must be made to the court by the attorney general, or on oath by a police officer, requesting a warrant specific to a particular offence. Similarly, regulators (such as the Information Commissioner, Gambling Commissioner and Gibraltar Financial Services Commission) have powers of entry and inspection on application to the court for a warrant.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

It is only permissible to operate an online betting or gaming business from Gibraltar with an appropriate remote gambling licence issued by the Government of Gibraltar. Gibraltar is a highly regarded and well-established hub for remote gambling activity, with many of the industry's leading companies based and licensed there. Regulatory standards are high, with detailed provisions and requirements relating to player protection, underage gambling, safer gambling, etc.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Gibraltar licences and regulates gambling on a point-of-supply basis. There is no restriction on external gambling companies providing gambling services or advertising to Gibraltar residents. It is not, however, permissible to provide access from Gibraltar to online betting or gaming services to customers based in another jurisdiction (or in a metaverse) without a Gibraltar remote gambling licence.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

If dealing with personal data, the outsourcing agreement should conform to the Gibraltar General Data Protection Regulation (GDPR) requirements. In particular, where there is a controller-processor arrangement the outsourcing agreement must have in place article 28 processor clauses. If outsourcing to a jurisdiction outside Gibraltar, the controller needs to ensure compliance with Chapter V of the GDPR and third-country transfers. Typically, model contractual clauses are used.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

Outsourcing restrictions apply in respect of 'material activities' of regulated entities, including digital financial services. If to an entity in a foreign jurisdiction, the outsourcing will only be allowed if the jurisdiction has at least equivalent regulation and supervision as Gibraltar. From a gambling regulatory perspective, functions and services can generally be outsourced but only with the prior approval of the gambling regulator.

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

Yes. As regards regulated activities, Gibraltar Financial Services Commission rules require outsourcing to be governed by a written contract incorporating specific terms.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

Where the outsourcing falls within scope of the Transfer of Undertaking Rules, consultation rights exist as do compensation where consultation is not done properly or the employee(s) not transferred.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

The Gibraltar General Data Protection Regulation (GDPR) sets out the rules relating to automated decision making or profiling. In addition to general compliance with GDPR principles, there are enhanced rights. For example, the right not to be subject to decisions based purely on automated processing if it produces a legal effect or significantly affects the individual. There is also an additional right to challenge any decision made and require human intervention in the decision-making process, and the right to object to such processing. There are also enhanced transparency rights requiring a meaningful explanation of the logic involved to be given to the individual before the processing begins. Because profiling is deemed to be high risk, it also triggers the need to carry out a data protection impact assessment before the activity takes place.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Copyright is capable of subsisting in literary, dramatic, musical or artistic works that are artificial intelligence (AI) or computer-generated. For patents, Gibraltar operates a secondary registration regime based on UK certificates. Current UK case law means that only persons can apply for patents. However, were this to change so that AI-generated material can be the subject of UK patents, these could be extended to Gibraltar via the local registry.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

There are none.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

It can be and will invariably turn on facts. The basis for taxation in Gibraltar for a company is (with some modifications) that a company must have income 'accrued in or derived from' Gibraltar. There is no need for a permanent establishment or taxable presence, merely that the income falls into the 'accrued and derived' category. There is no tax on capital gains, but non-taxability is dependent on our tax authorities considering a gain as capital in nature rather than trading income, including by reference to 'badges of trade' tests. Net (minus agreed deductible expenses) royalty income and inter-company interest income accrued to or received by (or both) a Gibraltar-registered company is subject to Gibraltar corporation tax (presently 12.5 per cent) irrespective of source (automatically deemed to have accrued in and be derived from Gibraltar). Inter-company interest income is subject to a de minimis £100,000 or equivalent per annum threshold. A business whose underlying activity that results in the income is such an activity that requires a licence and regulation under any law of Gibraltar is also subject to corporation tax.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Potentially yes. Invariably it will turn on facts, including what and where the underlying business activity that generates the income is, what type of income is generated and whether the activity is licensed and licensable in Gibraltar.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

Section 12 of the Consumer Rights on Contracts Regulations 2013 sets out all of the information that needs to be provided to consumers after the conclusion of distance contracts, where such information has not already been provided. This is not necessarily an e-invoice;

however, the confirmation of the price of the goods or services must be included. There are no specific rules on providing e-invoices to a tax authority or other agency.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

No.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

There is nothing specific to the online digital space, although access to online dispute resolution is possible for consumers.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

There is significant interest in Gibraltar in non-fungible tokens, new forms of digital games (including those involving crypto/P2E features), esports and crypto currency payment solutions.

A Command Paper for a new Gambling Act has been published and is currently in the consultation phase. This will replace, update and modernise Gibraltar's legislative and regulatory framework for gambling.

Hassans
International Law Firm Limited

| | |
|---|---|
| Michael Nahon | michael.nahon@hassans.gi |
| Andrew Montegriffo | andrew.montegriffo@hassans.gi |
| Tim Garcia | tim.garcia@hassans.gi |
| Claire Pizzarello | claire.pizzarello@hassans.gi |
| Hannah Lopez | hannah.lopez@hassans.gi |

PO Box 199 Madison Building, Midtown Queensway,
Gibraltar GX11 1AA, Gibraltar
Tel: +350 20079000
www.gibraltarlaw.com

# Hungary

Endre Várady and János Tamás Varga
VJT & Partners

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The government is proactive with regard to internet issues. It makes efforts to keep pace with technological developments and prepare Hungary for digital transformation. The government has adopted numerous strategic digitalisation plans.

The government has been also focusing on the responsibility of big platforms. Its digital white paper tackles issues affecting big platforms such as the taxation of digital services, data protection, copyright and the jurisdictional matters of tech giants. This could be a basis for future omnibus digital regulation in relation to platforms.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

The Hungarian E-Commerce Act and the Hungarian Civil Code set the main legal framework for the Hungarian digital business. In business-to-consumer (B2C) relations, special consumer protection regulation applies, including the regulation of unfair consumer practices and B2C contracts. In relation to platforms, special additional rules apply, including the implementation of the Copyright Directive and Audiovisual Media Services Directive. A wide variety of sector-specific regulations also apply depending on the nature of the digital product (eg, fintech regulation or the on-demand media regulation).

### Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The supervision of the digital business area is allocated among different regulatory bodies depending on the type of legal field. The main regulatory bodies include the following:

- the Data Protection Authority (data protection);
- the Consumer Protection Authority (digital consumer protection);
- the Hungarian Competition Authority (digital consumer protection/digital competition); and
- the Media and Infocommunications Authority (internet access tariffs /anti-spam, digital content, and telecoms).

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

It depends on the nature of the relationship:

- In business-to-business relations, parties have the freedom to agree on the jurisdiction.
- In business-to-consumer relations, in principle, the jurisdictional clause of the general terms will be invalid.

In the latter case, the default rules of private international law apply:

- In EU cross-border selling, while businesses may file a proceeding against a Hungarian consumer only in a Hungarian court, the consumer may bring the proceeding against the business in a Hungarian court or the court of the EU member state where the business is domiciled.
- In non-EU cross-border selling (when the business is domiciled outside of Hungary), the jurisdiction is determined based on Hungarian national private international law.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There is no substantial difference between the establishment of online businesses and brick-and-mortar businesses.

In general, there is no general permit requirement for pursuing online business, but like any other commercial activity it must be reported to the notary based on the business' registered office. In addition, for certain online businesses (eg, fintech companies, video-sharing content providers) additional sector-specific notifications and licences may apply.

It is important to highlight that some products (such as tobacco, veterinary medicine and dangerous products) may not be sold online.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Yes, it is possible. In the case of exchange of email or other equivalent individual communications, the contract is formed when one party clearly declares its offer (indicating the key terms) and the other party approves the offer. In the case of other forms of distance contract, the business must acknowledge the user's order within 48 hours by electronic means (otherwise the user is relieved from any contractual commitment).

'Click-wrap' contracts are generally enforceable if the user can review the terms and give their affirmative acceptance (eg, by ticking the checkbox).

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

#### Choice of law

In general, based on the Rome I Regulation, digital contracts may not derogate from the Hungarian mandatory provisions with regard to choice of law where business-to-consumer (B2C) contracts apply, and the overriding Hungarian mandatory provisions where business-to-business (B2B) contracts apply.

#### Language

With regard to B2C contracts, the Hungarian consumer protection authority requires the Hungarian language based on the general fairness principle. With regard to B2B contracts, the Hungarian language is not a requirement, but in the case of platform-to-business contracts, it is possible that the competent Hungarian authority will require the Hungarian language based on the fairness and transparency principle.

#### Forum

It depends on the nature of the relationship:

- in business-to-business relations, parties have the freedom to agree on the jurisdiction; and
- in business-to-consumer relations, in principle, the jurisdictional clause of the general terms will be invalid.

In the latter case, the default rules of private international law apply:

- in EU cross-border selling, while businesses may file a proceeding against a Hungarian consumer only in Hungarian court, the consumer may bring the proceeding against the business in Hungarian court or the court of EU member state where the business is domiciled; and
- In non-EU cross-border selling (when the business is domiciled outside of Hungary), the jurisdiction is determined based on Hungarian national private international law.

## Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

A legal document will be qualified as written if (1) it can be proved that the content of the document is unchanged, (2) the signatory is identifiable, and (3) the time of signature is identifiable. Where a written form is required (such as sale agreements or copyright agreements), parties shall primarily use a qualified electronic signature and time stamp or advanced electronic signature and time stamp. As a general rule, other forms of agreement such as agreements made via DocuSign or AdobeSign, exchange of emails or clicking an acceptance button, shall not be qualified as 'written' agreements.

E-signature services must be provided by a trusted service provider registered in Hungary or another EU country.

## Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

In the context of business-to-consumer online sales, consumers may withdraw from an electronic contract within 14 days. Businesses must adequately inform consumers about this right, otherwise the withdrawal deadline will be extended up to 12 months.

Based on the Hungarian implementation of EU Directive 2019/770 and 771, effective from 1 January 2022, consumers have new special remedies in the context of non-conformity of goods with digital elements, digital content and digital services (hereinafter: digital products). The consumer may ask to bring the digital products to conformity (unless it is impossible or would impose disproportionate costs). If the business fails to do so, the consumer may request a proportionate reduction in price or terminate the contract. The rule of reversal of burden of proof (ie, the consumer does not have to prove that the item was defective at the time of supply, as it is assumed by law) is extended from six months to one year in the case of digital products.

There is no special forum for dispute resolution available for the breach of digital contracts.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The Central Bank of Hungary supervises this area. Apart from the general Hungarian advertising law, additional sector-specific rules apply to some bank products such as credit or advisory services (eg, in commercial communication any wording should be avoided that could create false expectations for the consumer about the availability or cost of credit, and bank-tied agents may not use the term 'adviser' in the commercial communication). The Central Bank of Hungary has the power to ask electronic communication service providers to block websites on which unauthorised financial services are advertised.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Hungary has implemented the E-Money Directive (EMD2) (2009/110) and Payment Services Directive (PSD2) (2015/2366), based on which customers may initiate transactions via their fintech providers instead of traditional banking industry players. Fintech providers' services are subject to heavy Hungarian financial regulation (such as compulsory authorisation by the financial regulator and rules on strong customer authentication). As it is challenging for fintech providers to fully adjust to Hungarian legal requirements, the Hungarian financial regulator, the Central Bank of Hungary created a regulatory sandbox in which fintech providers can test their services in a controlled environment under the regulator's supervision.

### Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

There is no specific local regulation on the provision or use of crypto wallets or other methods of digitally storing value.

But as from January 2022, Hungary introduced personal income taxation on profits made in crypto currencies. Such profits are qualified as separately taxed income based on a 15 per cent personal income tax rate.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

There is no unified law on electronic payment transactions – the rules are scattered in various sector-specific financial regulations, as there are separate rules for various e-payment solutions such as instant payment, point-of-sale terminal payment and contactless payment. The implementation of the Payment Services Directive ((EU) 2015/2366) (PSD2) in Hungary and the introduction of multi-factor authentication significantly enhanced the security of electronic payment.

As of January 2021, merchants operating online cash registers are obliged to provide consumers with the possibility of electronic payment.

The volume of electronic payment transactions in Hungary is constantly growing. The Central Bank of Hungary aims to stimulate electronic transactions by bringing continuously new packages of legislation. It aims to reduce cash transactions in Hungary below 50 per cent by 2030.

Regarding third-party access to digital information in bank accounts, the rules on bank secrecy must be observed.

## Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

The client's identity may be checked online by the third party if the customer due diligence requirements set out in the AML Act are observed.

If the third party is established outside the EU, the third-party customer due diligence report may be accepted only under specific conditions (eg, the third-party service provider applies the customer due diligence requirements set out in the AML Act and is supervised in accordance with the requirements).

The service provider may not accept the customer due diligence report of the third party if that party is established in a non-EU country with high risk.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

In a nutshell, the process is the following (in the below chronological order):

- check the availability of the domain name;
- choose the registrar who will be the service provider for the applicant;
- conclude the contract with the registrar;
- pay;
- accept the domain registration policy;
- check the technical requirements;
- check the fulfilment of the domain registration policy;
- grant the right conditionally (within one business day); and
- grant the final right of domain (if no complaint has arrived within eight days of granting the right conditionally).

Citizens of any country can apply for a second-level public domain name. For a first-level domain name, only citizens and legal entities from certain countries can apply. There is an official .hu domain name registry with information on the domain registration process and the list of countries from which a domain can be registered directly under .hu.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Domain names do not automatically confer any additional IP rights.

There is no obstacle to the registration of a domain name as a trademark, but the registered domain name does not itself constitute a legal basis for obtaining trademark protection without any further conditions. For the registration of the domain name as a trademark, a separate proceeding must be completed in line with the Trademark Act.

Further, domain names are rarely copyrightable as they are usually too short to qualify as copyrightable works.

A trademark holder may challenge a competitive use or registration of a similar domain name. The same applies to a copyright holder (although this is a more theoretical possibility, as the connection between copyright and domain is rather limited).

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

The main legal framework is set in the Advertising Act, which applies to both traditional offline and online advertising. Electronic communication as a form of commercial advertising is subject to additional anti-spam regulation set out in the E-Commerce Act. Online editorial content is also subject to additional sector-specific advertising rules of the Hungarian media regulation. The Unfair Commercial Practice Act sets out the rules against misleading advertising. The Hungarian Advertising Association is a self-regulatory organisation with its own Code of Advertising Ethics.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

The law does not define targeted advertising and online behavioural advertising, but it does define electronic communication. The Hungarian E-Commerce Act defines electronic communication broadly as any commercial ads or notices relating to social aims communicated via an information society service or electronic communication service. In general, an advertisement does not have to be strictly separated from online editorial content, but the advertisement must be clearly recognisable in the online content.

A prior notice about the electronic communication is required – this notice must highlight in a clear manner:

- the fact that it is an electronic communication;
- the advertiser; and
- promotional offers or games (if applicable).

Under the E-Commerce Act, consent for receiving electronic communication is required. However, the Data Protection Authority recognises electronic marketing communication based on opt-out possibility in the case of offering products to existing customers.

### Misleading advertising

**19** Are there rules against misleading online advertising?

The rules of misleading online advertising are set out in the Unfair Commercial Practice Act. In principle, these rules apply centrally, but there are also some related industry-specific rules (eg, in the pharma and financial industries). The burden of proof depends on whether the supervisory authority examines the advertising based on the truthfulness of the information or the capability of the information to mislead consumers. In the former case, the business must prove that the information in the advertisement is correct.

### Restrictions

**20** Are there any digital products or services that may not be advertised online?

Hungarian advertising law has restrictions and bans (such as banning tobacco adverts and, under certain conditions, alcohol and gambling adverts); however, in principle, all products that may be advertised offline may be advertised online as well. An exception applies to reminder advertising of over-the-counter medicinal products or therapeutic medical devices that are not supported by social security, and as such reminder advertising may not be carried out via the internet.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

In general, electronic marketing (via email, fax or SMS) is allowed only based on consent. However, the Data Protection Authority recognises electronic marketing communication based on opt-out possibility in the case of offering products to existing customers. Regarding voice-to-voice calls, the individual may be called only if he or she has not objected to such communication in the Hungarian publicly available phone directories (eg, no "§' sign or other mark in the directories, showing that the person cannot be called for marketing purposes). In case of automated calls, the holder of the phone number must give their prior explicit consent for the call (eg, in the phone subscription contract).

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Both content providers and ISPs (host providers) can be liable for unlawful advertisements if they are qualified as a publisher of advertisements. A publisher of advertisements is an entity that has the technical means to publish the advertisements.

Content providers as publishers will be liable if they could have had knowledge of the nature of the content before publishing the advertisement.

ISPs as publishers will be liable only if they did not remove the unlawful advertisements forthwith upon becoming aware of their illegal nature. However, ISPs providing video-sharing services can be also liable if they do not comply with their obligation to filter out certain commercial communications.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

As a general rule, as long as the website provider is a content provider and not an ISP (such as a host, search engine or cache provider), it is liable for any of its own content made available on its site. This liability cannot be removed with a unilateral disclaimer notice. The website provider is also liable for third-party content, but it can avoid such liability under certain conditions (eg, it has a proper notice-takedown mechanism for inappropriate user comments, or it re-publishes defamatory content, but marking the source and allowing the possibility for the other party to react).

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

It depends on the nature of the content. The ISP is not in a position to determine the truth of the allegation as it cannot take the role of judge. On the other hand, the truth defence is not relevant when, irrespective of whether the statement is correct or not, it unjustifiably breached the personal right of the person (eg, posts an offensive comment) and the ISP became aware of such statement. In this case, the content is 'manifestly unlawful' and the ISP must remove such content without further consideration.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

The database can be qualified as a copyrighted work if the selection, arrangement or editing of its content is of an individual and original nature. In this case, the website provider can protect its database based on regular copyright protection.

The website provider as the maker of the database also has sui generis rights. These rights apply if a substantial investment has been required to obtain, verify or present the content of the database. Based on sui generis rights, the website provider could also prevent the reproduction of its database.

## Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

This must always be assessed on a case-by-case basis. In general, if the third-party website targeted all internet users and was not protected (eg, subject to a paywall), a link to a third-party website is permissible. Users shall always have the clear ability to identify the original source and to understand that the website owner merely links to a third-party website (without having any relationship with the third-party website). If the linked third-party website contains unauthorised content, the website owner may be also liable.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

A website owner may only use third-party content on its website without permission if there is some specific permitted case of fair use (citation, free lecture, parody, orphan works, etc) to the extent it is used within the specific limits of fair use as set out in the Copyright Act. Otherwise, the website owner's unauthorised use of third-party copyright work can constitute copyright infringement, and the potential consequences can be civil in nature as well as criminal.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Considering its virtual nature, the metaverse poses a lot of practical difficulties with establishing or defending intellectual property (IP) rights in Hungary (like in any other jurisdiction) – for example, how to deal with copyright in a setting with no defined territorial boundaries, how to protect copyright content without a clear takedown mechanism and, in the case of trademarks, how to assess the level of similarity between real-world and virtual goods and services. These are just some of the IP issues seeking answers. The scope of Hungarian intellectual property protection in relation to the metaverse is still unclear as it has not yet been tested, and the Hungarian Intellectual Property Office has not issued any guidance on this.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Hungarian law recognises the first-sale doctrine. The Copyright Act states that if the copy of the work has been put into circulation within the European Economic Area by the copyright holder or another person (expressly authorised by the copyright holder), then the copyright

holder's or authorised person's right to control the distribution shall later be exhausted with regard to that copy.

In general, the first-sale doctrine applies only to physical (tangible) products, not digital products.

However, the landmark decision of the European Court of Justice in UsedSoft GmbH v Oracle International Corp (Case No. C-128/11) strengthened the argument that if the copyright holder makes the software available for download on the internet for an appropriate fee, then the first-sale doctrine could apply to the software purchased by the person who downloaded it if, in the course of resale, it is ensured that the original copy does not remain with the licence holder/reseller. As Hungarian copyright law needs to be interpreted in line with EU copyright law, the conclusions of this decision could apply, mutatis mutandis, to Hungary.

## Administrative enforcement

### 30 Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

The Hungarian Tax and Customs Administration has jurisdiction when an IP infringement constitutes a criminal offence, and it can order dawn raids and freezing injunctions. In litigation civil courts can also order freezing injunctions.

In the online context, if the IP infringement constitutes a crime, the criminal court can order the online host provider to remove the unlawful content within one day.

## Civil remedies

### 31 What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Various civil remedies are available to IP owners via both final court decisions and interim injunctions, including:

- the right to claim damages;
- the right to request cessation of the infringement;
- the right to claim recovery for unjust enrichment of the infringer;
- the right to claim seizure or destruction of infringing goods;
- the right to request a public court order or a public statement with appropriate content and form;
- the right to request removal of the infringing goods from the market; and
- the right to request information about the parties involved in the performance of services affected by the infringement as well as about the business network established by the infringing acts.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Personal data may be any data by which the individual can be directly or indirectly identifiable. Anonymisation techniques can be used to avoid Hungarian data protection regulation as long as the connection between the personal data and the individual is lost forever. In the case of sensitive personal data, the Hungarian Data Protection Authority expects controllers to be able to prove that an additional legal ground has been fulfilled under article 9 of the General Data Protection Regulation (GDPR) (apart from the six main legal grounds under article 6 of the GDPR).

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Parties involved in the processing of personal data are no longer required to register with the Hungarian data protection authority to process personal data; instead they shall maintain their internal records of processing in line with article 30 of the GDPR. However, the GDPR's notification obligations (such as data breach or data protection officer notification) are directly applicable in Hungary.

### Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

Hungarian data protection laws apply to organisations outside of Hungary if the data processing operation of such organisations relates to offering goods and services to individuals located in Hungary or to monitoring individuals' behaviour that occurs in Hungary. In this case, a foreign national who is residing in Hungary has the same protection under Hungarian data protection law as Hungarian citizens.

### Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

In the Hungarian digital world, apart from consent, performance of contract and legitimate interest are very common legal grounds for processing personal data.

Businesses may use performance of contract to the extent it is connected to the provision of service. In any other case, where the data processing operation is not directly connected to the provision of service (eg, improving a website or marketing), performance of contract is not the appropriate legal ground.

Businesses may also use legitimate interest, if they carry out and document the legitimate interest test in which they explain why the business's interest to process the data for a specific purpose overrides the right of privacy of customers. In the case of legitimate interest, the customer must be informed prior to the data processing that he or she has the right to object to it (eg, a proper opt-out mechanism must be ensured).

Consent is the primary legal ground in the case of electronic marketing. The consent must be informed (ie, the customer is properly informed about the data processing via a privacy policy), freely given (eg, if there are more data processing purposes a separate checkbox shall be provided for each data processing purpose) and explicit (eg, consent is not explicit if the checkbox is ticked by default).

In the case of transferring or exporting personal data to jurisdictions outside the European Economic Area, as a general rule, transfer or export is possible only if it is compliant with adequate safeguards based on the General Data Protection Regulation and *Schrems II* decision (Case No. C-311/18) of the Court of Justice of the European Union.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Certain critical service providers and operators of essential services set out in the Information Security Act may store personal data, but only within the European Economic Area.

Online betting servers must maintain their servers in Hungary, meaning that the data remain in Hungary as well.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

The Hungarian data protection authority is strict about the sale of data. The broker must inform the data subject that their data will be used for sale of data and the data subject must have the possibility to review the privacy policy of the database buyer and give consent to such transfer. This means that if there are several buyers, the data broker shall make available the privacy policy of each buyer, and ensure that data subjects can freely decide to which buyer their data can be transferred (eg, by checkbox mechanism).

On the other hand, the Hungarian data protection authority recognises the transfer of databases in M&A transactions based on legitimate interest of the seller.

**Read this article on Lexology**

### Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Individuals have the right to exercise rights set out in the GDPR, including the right to ask for information, access, erasure, restriction of processing, object to processing, data portability and not to be subject to automated decision-making (articles 13–22 GDPR). Individuals have the right to claim damages in the case of breach of their rights under the GDPR. These rights are equally granted to Hungarian citizens and foreign individuals to the extent the Hungarian data protection law applies.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

Regulation (EU) 2018/1807 on the free flow of non-personal data applies directly; there is no specific national legislation on the use of non-personal data.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Transaction documents in family law and inheritance law cannot be exclusively electronic – paper-based documents and wet signatures are statutory in these procedures, irrespective of the issuance of electronic documents signed by electronic signatures.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

As a general rule, online contractual documentation subject to bookkeeping must be retained for eight years.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

In general, companies and ISPs are free to decide on their security measures, but such measures must be in line with article 32 of the GDPR. For service providers of critical infrastructure and organisations falling under the scope of the NIS2 Directive (EU Directive No. 2022/2555), an additional set of Hungarian cybersecurity rules apply. There is no explicit requirement to make encryption mandatory in case of internet transactions, but it is desirable to avoid personal data breaches.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

The provisions of the GDPR on data breach notification and data security are directly applicable, but there are also some sector-specific Hungarian laws.

Electronic communication service providers must notify the data breach to the Hungarian Media and Infocommunications Authority (first notification within 24 hours, second notification within 72 hours after obtaining knowledge about the breach).

Hungary has also implemented the NIS2 Directive (EU Directive No. 2022/2555), based on which certain organisations falling under the scope of the NIS2 Directive must report security breaches (including data breaches) that have a significant impact on the provision of their services.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Hungarian law enforcement authorities usually access electronic communication via data disclosure requests. Some law enforcement authorities (such as the police and national security) may also intercept the content of communication carried out by means of electronic communications networks or devices or any information system under certain conditions.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

It depends on the type of gambling:

- Online betting is permissible, but a licence for operating is required. Hungarian incorporation is also required (for EEA applicants, having a Hungarian branch is sufficient).
- Lotteries may not be performed (as raffles may not be performed online, and other lottery games are subject to state monopoly).
- Online casinos may be organised only by the entity that has the concession right to run casinos in Hungary as brick-and-mortar premises.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

It is permissible to advertise or provide access to online gambling business if the business has a valid licence for operation.

Most gambling activities require a Hungarian licence, and many times those licences are given to companies that have state monopoly (or concession right). The only liberalised field is online betting. Namely based on the ECJ decision C-3/17, Hungary has liberalised remote gambling. This means that EEA-based gambling operators may also apply for online betting. However, this is far from full liberalisation as such gambling operators need to establish a Hungarian branch, obtain a Hungarian licence (remote foreign licences are not recognised) and pursue the activity from Hungarian servers only.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

The contract rules of the Hungarian Civil Code set the general framework for outsourcing. In some specific industries such as financial or energy) sector-specific outsourcing rules also apply. Outsourcing also raises important employment issues especially in respect of control rights and transfer of employees. Taxation is also an important aspect of outsourcing deals as it needs to be checked whether the outsourcing transaction is subject to taxation. In the case of involvement of low-cost jurisdictions, anti-avoidance rules shall be also taken into account.

## Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

As a general rule, there are no digital business services that cannot be outsourced. However, if the digital businesses fall within specific industries (such as the financial or energy industries), outsourcing is possible only if the requirements of the sector-specific legislation are observed.

## Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

The outsourcing contract shall reflect the data processing agreement requirements set out in article 28 of the General Data Protection Regulation. If the outsourcing contract is a cloud computing contract, it is also advisable to comply with EU data protection best practices for cloud computing (eg, WP29 Opinion 05/2012 on Cloud Computing and Sopot Memorandum).

In the cases of certain financial industries (eg, banking and insurance), the outsourcing contract must include the mandatory elements set out in the applicable financial-specific regulation.

## Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

In general, in the case of business transfers, the employment relationship is transferred to the transferee. Employment terms (including salary) remain unchanged at the time of the transfer. The transferee must maintain the collective agreement's terms for one year. The transferee may suggest amendments of the terms, but the employee may refuse such suggestions and the employer may not terminate the agreement based on such refusal. Prior consultation with a works council and employee notification is also a mandatory part of the process.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

Artificial intelligence (AI) is not yet specifically regulated in Hungary, but it is highly recommended to comply with the General Data Protection Regulation (GDPR) requirements and carry out an impact assessment. In February 2022, the Data Protection Authority issued its record GDPR fine of 250 million forints against a bank for its improper automatic AI analysis of recordings of customer service calls. The authority, among others, found that the bank did not address the proportionality of the data processing and its potential risks, and that data subjects did not get meaningful information about the voice analysis. The case could be important for similar AI technologies used across the Hungarian market.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

There is no Hungarian law or guidance that explicitly concerns the ownership of intellectual property (IP) created by AI or machine learning systems.

Under Hungarian IP laws, the bottom line is that the creator of the IP can only be a natural person. Thus, the IP cannot be protected if it is solely created by AI.

If the work is created by humans with the help of AI, the work can be copyrightable under certain conditions – for example, if the author uses an AI tool or technology, and the role of the AI is only to support the creative process, while the human creator makes free and creative decisions and enjoys the freedom of creativity.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

No local rules or guidance relating to the ethics of artificial intelligence and machine learning have been issued.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

In general, distance sales are subject to Hungarian taxation if the product is delivered to Hungary. Similarly, digital services (eg, software downloaded from a website) are subject to Hungarian taxation if the service is performed in Hungary.

In the case of EU cross-border distance sales (business-to-consumer relations) the general rule is that the sale is taxed in the country in which the consumer is established (based on the implementation of the new EU VAT e-commerce package).

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

If the company is incorporated outside of Hungary and its place of management is not in Hungary, the company will not be a Hungarian tax resident. However, the company can be still subject to Hungarian corporate tax on income earned in Hungary if the server is placed within Hungary and the company carries out its business activity in Hungary in whole or in part via this server. Hungarian VAT can apply under certain conditions (eg, the place of supply is in Hungary) irrespective of where the servers are located.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

In Hungary, businesses must provide copies of e-invoices to the tax authority. Simultaneously, they must report invoicing data electronically in XML format to the tax authority. These notifications are made to the tax authority's online invoice system interface.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no special courts or other venues in Hungary that specifically deal with online/digital issues and disputes.

**Read this article on Lexology**

## ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

The most common ADR form is the proceeding before the Hungarian conciliation body. Businesses must inform consumers about their right to turn to the conciliation body, but businesses do not have to commit to the conciliation procedure. Parties also have the possibility to resolve the matter via an online dispute resolution platform set out in EU Online Dispute Resolution Regulation (524/2013).

# UPDATE AND TRENDS

## Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

There has been a major overhaul in the Hungarian e-commerce regulation, after the recent implementation of several important EU directives:

- Hungary implemented EU Directive 2019/770 and 771, effective from 1 January 2022, based on which consumers have new special remedies in the context of non-conformity of goods with digital elements, digital content and digital services.
- Hungary implemented the Omnibus Consumer Protection Directive, effective from May 2022, which imposes various additional consumer protection obligations (eg, additional obligations on online marketplaces to inform consumers, such as ranking parameters and the extension of mandatory consumer protection rules to services provided in return for personal data).
- Hungary implemented the NIS2 Directive by which it imposed a set of cyber security requirements to a broader circle of organisations.
- Based on the implementation of the Copyright Directive, content-sharing service providers now have increased liability for making available copyright works without authorisation.
- Based on the implementation of the AVMS II Directive, video-sharing platforms now have some monitoring and filtering obligations (in contrast with the rule that ISPs do not monitor online content) in the case of certain content (such as terrorism, content that would be incitement to crime, and user-generated commercial communications violating the Hungarian media advertising rule).

The Hungarian government has also issued its digital white paper. The white paper tackles issues typically affecting big platforms such as the taxation of digital services, data protection, copyright and the jurisdictional matters of tech giants. This could be a basis for future omnibus digital regulation in relation to platforms.

Endre Várady varadye@vjt-partners.com
János Tamás Varga vargajt@vjt-partners.com

Kernstok Károly tér 8, 1126 Budapest, Hungary
Tel: +36 1 501 9900
www.vjt-partners.com

# Iceland

Haflidi Kristjan Larusson
BBA//Fjeldco

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The government's long-standing attitude and approach is to encourage the use of digital services, promote online business and facilitate digital transformation.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

Such legislation is twofold, namely: (1) legislation that not only applies in the digital arena (although it may contain rules which apply specifically to digital matters), such as the Contracts Act No. 7/1936, the Consumer Contracts Act No. 16/2016, the Electronic Communications Act No. 70/2022, the Copyright Act No. 73/1972, the Data Protection Act No. 90/2018 and the Criminal Code No. 19/1940; and (2) legislation specifically governing digital matters, in particular the Act on Electronic Commerce and other Electronic Services No. 30/2002 and the Act on Act on Electronic Identification and Trust Services for Electronic Transactions No. 55/2019.

In general, most Icelandic legislation that applies in the digital arena is based on corresponding EU legislation.

Generally, Icelandic legislation is available in Icelandic only.

### Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The main regulatory bodies are as follows:

- the Electronic Communications Office;
- the Consumer Agency;
- the Data Protection Authority; and
- the Competition Authority.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

In relation to international electronic contracts, the nature of the contractual parties determines the jurisdiction, namely whether the underlying transaction is a B2B or a B2C transaction.

In relation to B2B transactions within the EEA, the general rule is that the parties are free to choose the jurisdiction (or arbitration or other alternative dispute resolution for that matter). If the contract between the parties does not specify the jurisdiction or ADR, then the rule is that the local courts of the place of the performance of the contract have jurisdiction. In the context of the metaverse and the delivery of digital 'goods' and services, there is an obvious question where, indeed, the place of the performance of the contract is situated. Today, there exists no Icelandic case law that provides how to determine this issue in the digital world.

In relation to B2C transactions within the EEA and regardless of any jurisdiction clauses in the relevant contract, the consumer has the choice between suing the other party before the local courts where the consumer is domiciled or before the other party's local courts. In contrast, the other party can only sue the customer before the local courts where the consumer is domiciled.

In relation to B2B and B2C transactions between an Icelandic party and an entity or individual domiciled outside of the EEA, the legal position is not as clear, although the Icelandic courts are likely to follow the broad principles set out above.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

The Act on Electronic Commerce and other Electronic Services No. 30/2002 stipulates that a service provider that carries out business in a permanent establishment in Iceland must adhere to Icelandic law regarding the establishment and operation of the services. The Act further stipulates that the provider of digital services must make certain information about itself available to the public and provide certain information to consumers before any transactions are entered into, as well as sending the consumer an electronic confirmation when an order has been received.

There are no procedural requirements that are specific to establishing a digital business in Iceland. The establishment of such a business would have to adhere to the same rules as establishing other businesses, such as registering with the Companies Registry and obtaining a VAT number.

**Read this article on Lexology**

As Iceland is a member of the EEA, businesses established in an EEA member state may, as a general rule, provide services or goods in Iceland under the same conditions as in their home country. However, the establishment of a branch or a subsidiary in Iceland must comply with the procedural requirements set out in Icelandic law.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

A general principle of Icelandic contract law is the freedom of form. It is therefore possible to form and conclude contracts electronically, such as by email by using online forms and digital signatures.

The general principles provided by Icelandic contract law (including the Contracts Act No. 7/1936) apply to digital contracts.

Certain exceptions to this general rule are set out in the Act on Electronic Commerce and other Electronic Services No. 30/2002. Contracts in the field of family law, contracts that create or transfer rights over real estate and lastly public registrations and notarial deeds are not valid if concluded digitally.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

The Act on Law Applicable to Contractual Obligations No. 43/2000 limits the choice of governing law when a contracting party is a consumer. If certain conditions are met, a clause on the choice of law in a contract will not limit the protection that the consumer enjoys according to the mandatory rules of the EEA State where the consumer is domiciled. The exception does not apply to all consumer contracts (eg, when services are purchased that are to be provided entirely in a country other than the consumer's home country).

The Act contains a similar provision that also applies to B2B contracts. The provision states that parties can not restrict the application of the mandatory rules of Icelandic law, if a case is conducted in Iceland, regardless of which country's law is otherwise to be applied to the contract.

In relation to B2C transactions and regardless of any jurisdiction clauses in the relevant contract, the consumer has the choice between suing the other party before the local courts where the consumer is domiciled or before the other party's local courts. In contrast,

the other party can only sue the customer before the local courts where the consumer is domiciled.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

The Act on Electronic Identification and Trust Services for Electronic Transactions No. 55/2019 governs the use and effect of e-signatures. It is based on EU Regulation No. 910/2014. When a signature is required by law or for other reasons, a valid e-signature will satisfy this requirement.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

There are no special forums that distinguish between the breach of digital contracts and other contracts. Apart from the Icelandic court system, consumers can send complaints to a special administrative body called 'The Complaints Board regarding the Purchase of Goods and Services'.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The Act on Remote Sales of Financial Services No. 33/2005 regulates the advertising and selling of financial services. The Financial Supervisory Authority of the Central Bank of Iceland supervises the implementation of the Act.

The EU Markets in Financial Instruments Directive II and Markets in Financial Instruments Regulation have been implemented in Iceland, among other EU legislation that regulates investment services. This legal framework regulates providers of investment services in Iceland and these providers must establish a branch or a limited company in Iceland and obtain an operating licence from The Financial Supervisory Authority. The Financial Supervisory Authority can authorise such a provider established outside the EEA to provide investment services by establishing a branch in Iceland. However, providers of investment services that have a licence and are under supervision of another EEA state are allowed to conduct activities in accordance with Icelandic law without the establishment of a branch.

## Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

The Act on Issuance and Handling of Electronic Money No. 17/2013 (which is based on the EU Second Electronic Money Directive) applies to the issuance and handling of electronic money in Iceland and it regulates domestic electronic institutions and the activities of foreign electronic money institutions in Iceland. The issuer must issue electronic money at nominal value. When requested, the issuer must redeem the monetary value of the electronic money without delay and at the nominal value. The issuer is not allowed to grant interest or any other benefit related to the length of time during which the holder holds the electronic money.

The issuer must obtain a permit as an electronic money institution from The Financial Supervisory Authority of the Central Bank of Iceland. An institution established outside the EEA can, in some cases, receive a permit to operate in Iceland through a branch if the institution has a licence to conduct similar activities in its home country and if a cooperation agreement has been concluded between the Financial Supervisory Authority and the competent authorities in that country. Electronic money institutions established within the EEA can, however, apply to operate in Iceland without establishing a local branch.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

A service provider that offers a digital wallet must be registered with the Icelandic Financial Supervisory Authority, in accordance with the Anti-Money Laundering and Terrorist Financing Act No. 140/2018. This Act is based on EU anti-money laundering legislation.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

The Payment Services Act No. 114/2021 implements the EU Second Payment Services Directive No. 2015/2366. Among other things, the Act regulates third-party access to digital information in bank accounts. Such a party is called an Account information service provider.

### Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

There are currently no restrictions regarding the use of third parties to satisfy KYC or AML identification requirements. Such services exist in Iceland.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

ISNIC - Internet á Íslandi hf. manages and operates the registry and technical infrastructure for the '.is' country-code top-level domain. The registration of a domain confers rights to the use of the domain name according to current ISNIC rules, but does not confer ownership of the domain itself.

Foreign individuals and entities can register '.is' domain names.

There are no restrictions around the use of URLs to direct users to websites, online resources or metaverses.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Domain names would rarely be considered copyrighted work. Domain names may however create certain IP rights as an unregistered trademark right. For a domain name to be considered a trademark, having established trademark rights by use, it has to fulfil certain requirements (eg, distinctiveness of a mark for particular goods or services).

Ownership of a trademark or copyright would assist in challenging a competitive use or registration of a similar domain name or URL.

Domain names are often registered as trademarks as well (without the <.is> ending) and may, if the domain name is considered to be trademark, be supporting evidence in an opposition case.

## ADVERTISING

### Regulation

**17** | What rules govern online advertising?

The Act on Electronic Commerce and other Electronic Services No. 30/2002 stipulates that a service provider must ensure that any marketing material, which is a part of or constitutes electronic services, is presented in such a way that it is easy to identify the individual or legal entity behind the marketing.

The Act on the Surveillance of Unfair Business Practices and Market Transparency No. 57/2005 governs online advertising that is intended to have an effect in Iceland. This Act, together with Rules No. 160/2009 on business practices that are considered unfair under all circumstances, contains numerous rules on advertising. Most of these rules can also be applied to online advertising.

### Targeted advertising and online behavioural advertising

**18** | What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Primarily, the Icelandic Data Protection Act No. 90/2018 applies in this context.

Further, The Code of Conduct of the Association of Icelandic Advertising Agencies (as a self-regulating tool within the advertising industry) contains various guidance that governs direct advertising (eg, in relation to children).

### Misleading advertising

**19** | Are there rules against misleading online advertising?

The Act on the Surveillance of Unfair Business Practices and Market Transparency No. 57/2005 prohibits misleading advertising. Online advertising falls under the scope of the Act, as it applies to any agreements, terms and actions that is intended to have an effect in Iceland. Specific sector regulations issued by the relevant authorities may provide additional provisions (eg, advertising relating to medicine or financial services).

Advertising claims must be substantiated and any advertising that is likely to deceive consumers, or is such that consumers are provided with false information with the intention of influencing their decision to do business, is prohibited.

### Restrictions

**20** | Are there any digital products or services that may not be advertised online?

There are special rules providing restrictions for advertising certain types of services and products such as alcohol, tobacco, financial services, prostitution, gambling and food supplements. No distinction is made between online advertisements and other advertisements.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

Pursuant to the Act on Electronic Commerce and other Electronic Services No. 30/2002, a service provider who advertises directly or indirectly must make it clear what is being advertised and who the advertiser is. As laid out in Act No. 70/2022 on Electronic Communications, it is not permitted to use email, fax or other corresponding means of communication for marketing unless the consumer has specifically agreed to it. The sender must check who has requested to not receive telemarketing with the Registers Iceland. It is permitted to send one promotional email to those who are not on the Registers Iceland register if the consumer is asked to inform the advertiser whether he or she allows continued reception of promotions. If the consumer does not accept the continued marketing, the advertiser is not allowed to continue the communication. The Data Protection Act No. 90/2018 also applies in this instance.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Under the Act on Electronic Commerce and other Electronic Services No. 30/2002, in principle content providers and other intermediaries such as ISPs are not liable for the relevant content. (The Act implements the 'mere conduit', 'caching' and 'hosting' principles of the EU E-Commerce Directive No. 2000/31.)

Currently, Iceland is in the process of implementing the EU Directive on Copyright and Related Rights in the Digital Single Market No. 2019/790, including its provisions on hosting liability.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

If the provider directly inserts the incorrect information or otherwise interferes with the information so that it becomes incorrect (eg, by making part-deletions), the provider may become directly liable for such incorrect information. In this context, it is advisable that the provider includes standard notices or disclaimers.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Yes, upon a relevant notification.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

For a work to be protected by copyright law, it must meet a certain minimum requirement of originality and independent creation. Depending on the nature of the 'data', it may be protected by copyright. However, in most cases, the nature of the data is such that the data is not protected by copyright. In contrast, the databases themselves may enjoy a 'specific protection', that is a specific sui generis database right exists under the Copyright Act The condition for databases to enjoy this protection is that a substantive investment has been made to acquire, verify or present the content of the database. This is to be assessed taking into account the volume or importance of the work.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Icelandic legislation is for the time being silent on online content providers linking to third-party websites or platforms without permission. However, the Court of Justice of the European Union has dealt with this issue and its case law, see, for example, C-348/13 – *BestWater International*, should be considered to be the applicable law in Iceland.

The jurisprudence is that linking to content that has already been made public is not as infringement as long as the users of the platform that communicated the link could have accessed the works directly on the site containing the copyrighted material.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Icelandic legislation is for the time being silent on this issue. The implementation of EU Directive 2019/790 on Copyright and Related Rights in the Digital Single Market is in progress and it remains to be seen how this issue will be addressed.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

No.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

The concept of exhaustion of rights when copyrighted work is distributed for the first time within the EEA is recognised under Icelandic law. The distribution of copies that have been transferred to the internal market from a country outside of the EEA without the consent of the right holder is not permitted.

The exhaustion is only relevant in the case of distribution of tangible media, and not in the case of intangible objects or digital products. The electronic sharing of media does thus not exhaust rights.

## Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Yes, these remedies are available to authorities.

## Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Civil remedies available to IP owners in the case of breach of their rights include freezing injunctions and search orders. IP owners also have the right to compensation, both for financial and non-financial losses.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

´Personal data' is any information that relates to an identified or identifiable individual. 'Sensitive data' is any data that reveals an individual's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and personal data concerning a person's health and sex life. 'Pseudonymous personal data' is any data where any information that could be used to identify an individual has been replaced with a pseudonym or a value that does not allow the individual to be directly identified. 'Anonymous personal data' is any data that does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In relation to sensitive personal data, various stricter rules apply in relation to the processing of such data. In relation to pseudonymous personal data, general rules apply, although pseudonymisation is used to reduce the risk of processing personal data. If anonymisation is done correctly, 'anonymous data' is not personal data and data protection law does not apply to the processing of such data.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

No such registration requirements exist.

Data protection officers must be appointed if the processor (1) is a public body; (2) carries out a systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (3) processes personal data on a large scale of sensitive personal data, or of personal data relating to criminal convictions and offences; or (4) conducts a systematic monitoring of a publicly accessible area on a large scale.

### Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

Yes, but there is no requirement to appoint a representative in Iceland.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

As a general rule, personal data can be transferred freely from Iceland to any other EEA state and to any third country that the EU has recognised as having an adequate level of data protection. In contrast, any transfer of personal data to other third countries must meet specific requirements. The commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction is for general business and marketing purposes.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

As a general rule, personal data can be transferred freely from Iceland to any other EEA state and to any third country which the EU has recognised as having an adequate level of data protection. In contrast, any transfer of personal data to other third countries must meet specific requirements. The commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction are for general business and marketing purposes.

Export control rules may restrict or ban the international transfer of specific data, data servers or databases to remain in your jurisdiction.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

This would usually be subject to the specific consent of the individuals in question.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Both local and foreign individuals enjoy the same rights under the Data Protection Act No. 90/2018. Individuals have a broad range of rights and remedies in this context, including the right to be informed of any processing of their personal data, the right to request that personal data be destroyed, the right to send written complaints to the Data Protection Authority and the right to claim damages for certain unlawful processing of their personal data.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

Answer in progress.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

For a District Commissioner to register a document (such as conveyance documents), the document must in an original paper form. There are no other rules that require particular documents to be kept in original paper form, other than rules that apply to public bodies.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Accounting books, supporting documents and other accounting data, including data stored in computerised form, must be stored in a safe and secure manner for at least seven years from the end of the fiscal year. It is noted that it may be necessary to keep a certain part of the accounting for longer than seven years for VAT purposes.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

This is mainly governed by the Data Protection Act No. 90/2018 and the general principle that companies must have adequate technical and organisational measures in place to guarantee the cybersecurity of data. Specific rules also apply to individual sectors, such as the telecommunications sector and the financial services sector. The most commonly used cybersecurity standard is the ISO/IEC 27001 standard.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

The Data Protection Act No. 90/2018 would apply in this instance. Generally, the Data Protection Authority must be notified of any such data breach. The affected individuals must also be notified if the data breach is likely to result in a high risk to their rights and freedoms.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

This could happen in very limited cases, namely in the interest criminal investigations and where an appropriate court order has been obtained.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Simply put, betting and gaming operations are illegal in Iceland. The operation of lotteries is also prohibited unless strict conditions are met and subject to a specific official permit.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

The business located in another jurisdiction looking to provide online betting in Iceland would have to adhere to the local law. As local law prohibits gambling and betting, this would not be permissible.

An entity established within the EEA could not provide such services in Iceland on the basis of the freedom of services, as the Act on Services in the Internal Market No. 76/2011 excludes betting and gaming services.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

No specific legislation applies to outsourcing services or outsourcing contracts and there are no key legal issues as such that arise in this context.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

This mainly relates to financial services and where the Financial Supervisory Authority of the Central Bank of Iceland has issued guidelines (Guidelines No. 6/2014 on Outsourcing by Regulated Entities). The guidelines set out basic conditions and requirements regarding the outsourcing (and chain outsourcing) by regulated entities.

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

No such requirements exist in general. Regarding outsourcing by regulated entities in the financial sector, the Financial Supervisory Authority of the Central Bank of Iceland has issued guidelines (Guidelines No. 6/2014 on Outsourcing by Regulated Entities), which contain guidance on specific terms to be included in outsourcing agreements by such entities.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

No such specific rights exist in relation to outsourcing.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

The Data Protection Act No. 90/2018 (which implements the General Date Protection Regulation) contains provisions regarding automated decision-making and profiling and when impact assessments may be required in that context. No other legislation applies in this context.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

No specific rules exist that govern intellectual property rights in the context of artificial intelligence or machine learning. Training data sets and other data associated with artificial intelligence or machine learning can enjoy protection, mainly as a database right or under the law of confidentiality. There are no particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Answer in progress.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Entities and individuals resident in Iceland are liable for tax on all their income, including the sale of digital products and services. A foreign seller of digital products or services to a buyer in Iceland might be taxed in Iceland depending on where the services are provided and, in some instances, depending on the relevant double taxation treaty.

**Read this article on Lexology**

Any sale of services or activities performed in Iceland is subject to taxation. All persons who receive income in Iceland from the sale, rental, use or licensing of products, patents, rights or expertise must pay income tax on that income. The general principle is that these sales or royalties are taxed where their recipient is resident. However, special withholding rules may apply if such is stipulated in the relevant double taxation treaty.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

All persons who operate a permanent establishment in Iceland are subject to tax on the income stemming from the establishment. The placing of servers, a platform or a metaverse in Iceland may constitute a permanent establishment and, thus, be subject to taxation in Iceland.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

E-invoicing is widely used in Iceland. There is no general legal obligation to use e-invoices, but, for instance, public bodies now only accept e-invoices in relation to their purchases of goods and services. There is no requirement to provide copies of e-invoices to a tax authority or other agency.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

No.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

No such specific ADR methods exist.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

Currently, there are no emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online.

Being an EEA state, Iceland will generally implement EU legislation in this field, which will further enhance and promote digital transformation and doing business online in Iceland.

BBA // FJELDCO

Haflidi Kristjan Larusson haflidi@bbafjeldco.is

Katrínartún 2, 19th floor, Reykjavik 105, Iceland
Tel: +354 550 0500
www.bbafjeldco.is

**Read more from this firm on Lexology**

**Read this article on Lexology**

# India

Hardeep Sachdeva, Priyamvada Shenoy and Shagun Badhwar

AZB & Partners

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

In India, regulated entities operating in sensitive sectors, such as financial services, banking, insurance and telecommunications have exhibited higher standards of cybersecurity preparedness and awareness, partly due to regulatory intervention as well as voluntary compliance with advanced international standards. Sectors such as e-commerce, IT and IT enabled services that have seen FDI infusion have also proactively deployed robust cybersecurity frameworks and policies to counter the evolving nature of cyber frauds as they have borrowed advanced cybersecurity practices and procedures from their parent entities in US, EU or other matured jurisdictions.

The 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre), a part of the Indian Computer Emergency Response Team (CERT-In), has been set up by the government to analyse bots and malware characteristics and provide information and enable citizens to remove bots and malware. In addition, Cyber Swachhta Kendra strives to create awareness to secure data, computers, mobile phones and devices such as home routers. The Cyber Swachhta Kendra collaborates with industry and academia to detect systems infected by bots. It also collaborates with internet service providers to notify end users regarding infection of their system and provide them assistance to clean their systems.

India supports a multi-stakeholder approach in matters relating to internet governance. India's strengths in the sector are its industry and human resources, which can be leveraged in a multi-stakeholder approach. The multi-stakeholder approach will also align with India's investment strategy for digitalisation and will help India participate in the vast business opportunity of internet industry. India has supported the multi-stakeholder model of internet governance mechanisms, which would involve all stakeholders and help to preserve the character of the internet as a unified, dynamic engine for innovation, and encourage equity and inclusion.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

The Information Technology Act 2000 (the IT Act), read with the rules and regulations framed, is the principal legislation regulating the digital space in India. The IT Act not only provides legal recognition and protection for transactions carried out through electronic data interchange and other means of electronic communication, but also contains provisions that are aimed at safeguarding electronic data, information and records, and preventing unauthorised or unlawful use of a computer system. Some of the cybersecurity crimes that are specifically envisaged and punishable under the IT Act include hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft.

Some of the relevant rules framed under the IT Act that help govern business on the internet in the context of cybersecurity include:

- the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the SPDI Rules), which prescribe reasonable security practices and procedures to be implemented for the collection and processing of personal or sensitive personal data;
- the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018 (the Protected System Rules), which require specific information security measures to be implemented by organisations that have protected systems, as defined under the IT Act;
- the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (Intermediary Rules), which require intermediaries to implement reasonable security practices and procedures for securing their computer resources and information contained therein in terms of the SPDI Rules. The intermediaries are also required to report cybersecurity incidents (including information relating to such incidents) to CERT-In.

Other laws that contain cybersecurity-related provisions include the Indian Penal Code 1860 (IPC), which punishes offences, including those committed in cyberspace (such as defamation, cheating and criminal intimidation), and the Companies (Management and Administration) Rules 2014 (the CAM Rules), framed under the Companies Act 2013, which require companies to ensure that electronic records and security systems are secure from unauthorised access and tampering. There are also sector-specific regulations issued by regulators such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India Act 1999 (IRDA), the Department of Telecommunication (DOT) and the Securities Exchange Board of India (SEBI), which mandate cybersecurity standards to be maintained by their regulated entities, such as banks, insurance companies, telecoms service providers and listed entities.

The Digital Personal Data Protection Act, 2023 was passed by the Parliament of India on 9 August 2023 to create a new regime for the processing of digital personal data within India where such data is collected online, or collected offline and is digitised. It will also apply to such processing outside India if it relates to the offering of goods or services in India. The provisions of the bill have not yet been notified and implemented by the government.

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

There are several relevant government agencies responsible for the regulation of e-commerce, data protection and internet access tariffs and charges, etc.

The Department of Industrial Policy and Promotion Department for Promotion of Industry and Internal Trade (DPIIT) regulates foreign direct investment (FDI) in e-commerce. The Press Note dated 12 December 2018 issued by the DPIIT (PN2) is a significant development

as it provides clarity to the existing framework for foreign direct investment concerning the e-commerce sector.

Further, the Ministry of Consumer Affairs, Food and Public Distribution has notified the Consumer Protection Act, 2019 (CPA 2019) and the Consumer Protection (E-Commerce) Rules 2020 (the E-Commerce Rules). The term 'consumer' is defined under the CPA 2019 as any person who buys goods or services for consideration but excludes any person who makes a purchase for 'commercial use', with the exception of goods bought for the purpose of earning livelihood by means of self-employment. The CPA 2019 addresses issues in respect of digitisation and e-commerce. The E-Commerce Rules, formulated under the CPA 2019, regulate e-commerce entities and provide a framework to regulate the marketing, sale and purchase of goods and services online. The E-Commerce Rules also apply to entities that are not established in India but systematically offer goods or services to consumers in India. The Central Consumer Protection Authority (set up under the CPA 2019) regulates matters relating to violation of rights of consumers, unfair trade practices and false or misleading advertisements which are prejudicial to the interests of public and consumers and to promote, protect and enforce the rights of consumers as a class.

The payment systems for online e-commerce transactions, and the usage of payment instruments for facilitating e-commerce and mobile commerce are regulated by the Reserve Bank of India (RBI). RBI has also issued Foreign Exchange Management (Transfer or Issue of Security by a Person Resident outside India) (Amendment) Regulations 2019 dated 1 February 2019, to make it consistent with the revised legal framework stipulated under PN2.

The Ministry of Electronics and Information technology (MeitY) together with the Ministry of Communications has been entrusted to promote the internet, IT and e-commerce in India. A team to respond to cybersecurity incidents, and to undertake emergency measures in relation to such cybersecurity incidents has been established under MeiTY – the Computer Emergency Response Team (CERT-In). Simultaneously, the RBI regulates payment systems and online e-commerce transactions.

Telecom service providers in the country (including ISPs) are licensed by the Department of Telecommunication (DoT) under the Ministry of Communications. Further, in accordance with the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 (the CERT Rules), CERT-In has been established as the nodal agency responsible for the collection, analysis and dissemination of information on cyber incidents and taking emergency measures to contain such incidents. The access charges and tariffs in relation to the aforementioned service providers are regulated under their licence from the DoT and the tariff orders and regulations issued by the Telecom Regulatory Authority of India from time to time.

The Telecom Regulatory Authority of India (TRAI) has been established to regulate telecom services, including the fixing or revision of tariffs for telecom services that were earlier vested with the central government. One of the main objectives of TRAI is to provide a fair and transparent policy environment that promotes a level playing field and facilitates fair competition. The directions, orders and regulations issued cover a wide range of subjects including tariffs, interconnection and quality of service.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

In view of the judicial precedents, cause of action is the key element in determining the jurisdiction by Indian courts. The Indian courts have jurisdiction to adjudicate where the cause of action arises in India and the goods and services are being provided from outside the country.

Where a defendant sells goods or provides services from outside India, it has been seen that the Indian courts have adjudicated in cases involving deficiency in goods or services under the consumer protection laws. Now, the E-Commerce Rules specifically recognise and apply to entities that are not established in India but systematically offer goods or services to consumers in India. Accordingly, courts may exercise jurisdiction where the E-Commerce Rules apply to offshore entities, however, jurisprudence in this space is still evolving. On the other hand, if services are provided by resident entities, it may be stated that the appropriate Indian courts will exercise jurisdiction. As a matter of public policy, Indian courts may not permit their jurisdiction to be ousted in a contact between an Indian service provider and service recipient. If, however, the service provider is not from the territorial boundaries of India, then in such a case, the E-commerce Rules contemplate extraterritorial jurisdiction. The E-Commerce Rules specifically recognise and govern entities that are not established in India but systematically offer goods or services to consumers in India such as offshore online marketplaces.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

The procedure and manner of establishing digital businesses may vary from case to case. Mentioned below are some of the key pieces of legislation in India that govern the regulatory and procedural requirements for establishing digital businesses in India:

- the IT Act;
- the Foreign Exchange Management Act 1999;
- the Intermediary Rules;
- the Payment and Settlement Systems Act 2007 (the PSS Act);
- the Companies Act 2013; and
- the Trademarks Act 1999.

The marketing and promoting strategies for brick-and-mortar stores and e-commerce platforms may be different. Brick-and-mortar stores tend to rely on conventional forms of marketing and promotion, including but not limited to radio commercials, television channels, newspapers and billboards.

**Read this article on Lexology**

With regard to e-commerce platforms, while marketing and promotion may be done through traditional methods, such means may not be as effective as social media and digital advertising. Since e-commerce operates in the online space, digital marketing and promotion has proven to be more effective and efficient.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Yes, it is possible to form and conclude contracts electronically in terms of section 10-A of the Information Technology Act 2000 (the IT Act). Further, click-wrap contracts are enforceable in India. As long as the essentials of a valid contract under the Indian Contract Act 1872 are met, an online contract is valid and enforceable under Indian law. The IT Act provides validity to a contract where the contract has been accepted in electronic form. However, in the absence of a digital signature, the burden of proof in respect of the authenticity of such electronic contract is on the party claiming such contract to be a valid contract.

The usage of digital signatures for the execution of contracts in India is not as common as its usage for filing the relevant filings with authorities such as the Registrar of Companies.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

In India, the provisions of the IT Act and the Indian Contract Act 1872 govern digital contracts. Additionally, the Indian Evidence Act 1872 governs admissibility of electronic records and contracts, and states that any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer will be deemed a document of proof and will be admissible in any proceedings, without further proof or production of the original; provided certain prescribed conditions are satisfied.

Further, the following rules under the IT Act govern the digital execution of a contract:

- the Information Technology (Certifying Authorities) Rules 2000;
- the Digital Signature (End Entity) Rules 2015; and
- the Information Technology (Use of Electronic Records and Digital Signature) Rules 2004.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

The IT Act provides legal recognition to electronic signatures and lays down the framework that governs their use. It expressly includes 'digital signature' as a form of electronic signature, subject to its adherence to the authentication requirements prescribed under the IT Act. An electronic signature may be used at any place where any law provides for the use of a signature for authentication. Usage of digital signature is very common for e-filing with the Ministry of Corporate Affairs, and goods and services tax authorities. An 'electronic signature' refers to the authentication of an electronic record by a subscriber by means of the prescribed electronic technique, and includes digital signatures.

As per the IT Act read with the Information Technology (Certifying Authorities) Rules 2000, an entity proposing to issue digital signatures (as recognised under the law) requires a licence, namely, a digital signature certificate from the Controller of Certifying Authorities. While the IT Act recognises electronic signatures, only an electronic contract with a digital signature certified in terms of the IT Act and the rules thereunder can be admissible as evidence in the court proceedings (akin to a physically signed contract), without the necessity to prove the integrity and authenticity of such electronic contract.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

The remedies available under the Indian Contract Act 1872 for breach of a contract may also be availed of for electronic contracts. There are no specific remedies prescribed for the breach of an electronic contract in India.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

Yes. The Securities and Exchange Board of India is responsible for curbing malpractices or other deceptive activities related to the sale or advertising of financial services products like mutual funds and other securities.

The Insurance Regulatory and Development Authority of India is responsible for undertaking similar activities related to insurance products. To provide a specific example, the Securities and Exchange Board of India (Mutual Funds) Regulations 1996 require advertisements in relation to mutual fund investment schemes to be in accordance with the advertisement code prescribed under the regulations.

Recently, the Securities and Exchange Board of India has also permitted mutual funds to accept investments from their investors through e-wallets (pre-paid payment instruments) in accordance with certain conditions prescribed by it.

Additionally, the Reserve Bank of India regulates various financial products and services that are offered to consumers, or as services to businesses, through an electronic payment interface. Such products and services include prepaid payment instruments (such as wallets and gift cards), and loans by regulated entities on digital platforms (digital lending). The RBI issues guidelines and directions from time to time for regulated entities that offer such products and services.

For the advertisement and promotion of virtual digital assets (VDAs), namely cryptocurrencies or NFTs, the Advertising Standards Council of India, on 23 February 2022, issued guidelines applicable from 1 April 2022 (Guidelines) which are applicable to all VDA-related advertisements released on or after 1 April 2022. As per the Guidelines, advertisers and media owners are required to ensure that any earlier advertisements that are in non-compliance with the Guidelines must not appear in the public domain after 15 April 2022. The Guidelines, among other things, prescribe certain disclaimer-related requirements for all advertisements for VDA products and VDA exchanges, or featuring VDAs, due to the fact that '[c]rypto products and NFTs are unregulated and can be highly risky. There may be no regulatory recourse for any loss from such transactions'.

## Electronic money and digital assets

### 11 Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

With the rise of digital payments, cybercrimes involving payment transactions in the online space have significantly increased and become complex. While the RBI has been active in requiring companies operating payment systems to build secure authentication and transaction security mechanisms (such as 2FA authentication, EMV chips, PCI DSS compliance and tokenisation), given that these payment companies often offer real-time frictionless payments experiences to their consumers, it leaves less time for banks and other entities operating in the payment ecosystem to identify and respond to cyberthreats. There is an increased need to identify and develop cybersecurity standards commensurate with the nature of information assets handled by them, and the possible harm in the event of any cybersecurity attack, to ensure that these emerging risks are mitigated.

The payment and settlement systems in India are governed by the Payment and Settlement Systems Act 2007 (the PSS Act), read with the Payment and Settlement System Regulations 2008. In terms of the PSS Act, the commencement or operation of a payment system in India shall be subject to authorisation by the Reserve Bank of India (RBI).

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Presently, India does not have a dedicated law for regulating cryptocurrencies and crypto wallets.

In March 2023, the Ministry of Finance via a notification introduced the concept of VDAs within the purview of the Prevention of Money-laundering Act 2002 (PMLA). The PMLA is the central legislation of India that deals with measures and safeguards for money laundering activities.

Pursuant to the notification, the following activities have been brought within the purview of the PMLA:

- exchanging VDAs with fiat currencies;
- exchanging one VDA with another VDA;
- transferring VDAs between two persons or legal entities;
- safekeeping or administering VDAs or instruments enabling control over VDAs; and
- participating in and providing financial services related to the offer and sale of VDAs.

Such VDAs are required to undertake necessary compliance, disclosure and reporting to the authorities to aid measures to prevent money laundering and comply with the provisions of the PMLA.

Similarly, in April 2022, CERT-In issued certain directions to service providers, intermediaries, bodies corporate, virtual asset service providers, virtual asset exchange providers, custodian wallet providers, etc, mandating reporting of certain specified cyber incidents to CERT-In, and maintaining and retaining logs of all their information and communications technology systems for a rolling period of 180 days within India.

Separately, the Master Directions on Prepaid Payment Instruments have been issued by the RBI for prepaid payment instruments (PPIs) (eg, cards and wallets), regulating payment instruments that facilitate the purchase of goods and services against the value stored on such instruments. The issuers of PPIs are subject to an authorisation requirement under the PSS Act.

Further, the Finance Budget 2022, discussed aspects relating to the transfer of cryptocurrency in India and taxation on the income arising therefrom. Pursuant to the budget, the Indian Ministry of Law and Justice notified the Finance Act 2022, which amended various provisions of the Income Tax Act 1961 (Income Tax Act), in order to, inter alia, introduce the concept of virtual digital assets (VDAs) and taxation on the income arising from the transfer of such asset.

As per the Income Tax Act (as amended by the Finance Act 2022), the term 'virtual digital asset' has been defined to include, inter alia, any information, code, number or token (not being Indian currency or foreign currency) generated through cryptographic means or otherwise,

by whatever name called, that provides a digital representation of value exchanged with or without consideration, with the promise or representation of having inherent value, or that functions as a store of value or a unit of account including its use in any financial transaction or investment, but not limited to investment schemes, and that can be transferred, stored or traded electronically.

The Income Tax Act (as amended) further provides that income tax at the rate of 30 per cent shall be levied on the income arising out of the transfer of a VDA.

Further, tax deducted at source (TDS) shall be levied upon the transfer of a VDA, at the rate of 1 per cent of the consideration of such transfer. However, such TDS is not to be levied if the consideration payable on the transfer of such VDA does not exceed (1) 50,000 Indian rupees in a financial year (in cases where the consideration is payable by certain persons as specified under the Income Tax Act), and (2) 10,000 Indian rupees in a financial year (in cases where the consideration is payable by any person other than a specified person).

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

In India, the payment and settlement systems are regulated by the PSS Act. Under the PSS Act, a 'payment system' is defined to mean a system that enables payments to be effected between a payer and a beneficiary and involves clearing, payment or settlement services, or all of them.

The nodal department for regulating the activities of payment systems is the RBI. On 17 March 2020, the RBI issued guidelines regulating the activities of 'payment aggregators' that are 'payment system operators' (PA-PG Guidelines). As per the PA-PG Guidelines, the payment system operators are required to apply to the RBI for authorisation under the PSS Act.

The RBI has periodically issued directions, guidelines, regulations and circulars requiring banks to maintain the confidentiality and privacy of customers.

## Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

The RBI has issued Master Direction – Know Your Customer (KYC) Directions 2016 (as amended from time to time) (KYC Master Directions), to regulate, inter alia, the customer identification procedures to be followed by the RBI-regulated entities (REs) while undertaking a transaction. The KYC Master Directions provide, inter alia, that for the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, REs shall, at their option, rely on customer due diligence done by a third party, subject to certain conditions, including the following:

- records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry;
- adequate steps are taken by REs to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay;
- the third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the Prevention of Money-Laundering Act 2002;
- the third party shall not be based in a country or jurisdiction assessed as high risk; and
- the ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the RE.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

Any person in India or abroad may register country code top level domain names (CCTLDN) with the domain name registrar accredited with the '.in' registry. CCTLDN are regulated by the '.in' registry as per the directions of the National Internet Exchange of India. The '.in' registry has been tasked with maintaining the '.in' country code and to ensure the operational stability and security of the domain.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

In view of the judicial precedents in India, the courts have construed domain names as similar to trademarks, and have upheld trademark infringement and passing-off claims filed by trademark owners against users operating with the same or deceptively similar domain names.

## ADVERTISING

### Regulation

**17** | What rules govern online advertising?

While there are no specific rules or regulations governing advertising on the internet, in terms of the Information Technology Act 2000 (the IT Act), it should be ensured that any advertisement published or transmitted through any website on the internet does not contain any obscene material, any material containing sexually explicit acts or conduct, and any material depicting children in an obscene, indecent or sexually explicit manner. In addition to the above, the Advertising Standards Council of India prescribes the code for self-regulation in advertising (the ASCI Code), which may be adopted by persons publishing advertisements on the internet. Compliance with such code is voluntary with respect to online advertising and not mandated by law. However, with respect to content on television, adherence to the ASCI Code is mandatory under the Cable Television Regulation Act 1995 (the Cable Television Act).

In addition, there are certain laws and guidelines that prohibit the advertising and publication of certain specific types of content. A violation of these laws will entail consequences under those respective laws, including imprisonment. An illustrative list of such regulations is:

- the Indian Penal Code 1860 prohibits any person from selling, advertising or otherwise distributing any obscene material (such as books, pamphlets, drawings, paintings and representations). It also prohibits any person from distributing, circulating or advertising any picture or any printed or written document that is grossly indecent;
- the Indecent Representation of Women (Prohibition) Act 1986 prohibits publishing or taking part in the publication of any advertisement that contains 'indecent representation of women' in any form;
- the Infant Milk Substitutes, Feeding Bottles and Infant Foods (Regulation of Production, Supply and Distribution) Act 1992 prohibits advertising of infant milk substitutes, feeding bottles or infant foods for the purposes of distribution, sale and supply;
- the Cigarettes and other Tobacco Products (Prohibition of Advertisement and Regulation of Trade and Commerce, Production, Supply and Distribution) Act 2003 prohibits all direct and indirect advertising of tobacco products in all media;
- the Flag Code of India 2002 prohibits the use of the Indian national flag in any form of advertisement;
- the Legal Metrology Act 2009 imposes certain prohibitions and restrictions upon the advertisement of prepackaged commodities and certain other products;
- the Drugs and Magic Remedies (Objectionable Advertisements) Act 1954 prohibits the advertisement of certain drugs and of misleading advertisements;
- the Prize Chits and Money Circulation Schemes (Banning) Act 1978 prohibits advertisements relating to prize chit and money circulation schemes;
- the Transplantation of Human Organs Act 1994 prohibits any advertising inviting persons to supply, or offering to supply, any human organ for payment;
- the Young Persons (Harmful Publications) Act 1956 prohibits advertisements relating to any harmful publication (ie, any publication that tends to corrupt a person under the age of 18 years by inciting or encouraging him or her to commit offences or acts of violence or cruelty or in any other manner whatsoever);

- the Drugs and Cosmetics Act 1940 prohibits advertisements for any drug or cosmetic from using reports of tests or analysis of the Central Drugs Laboratory or by a government analyst;
- the Cable Television Network Rules 1994 prohibit any advertisement promoting the production, sale or consumption of cigarettes, wine, liquor or other intoxicants through the cable service; and
- the Food Safety and Standards Act 2006 prohibits advertisement relating to the standard, quality, quantity or grade composition, and no representation concerning the need for, or the usefulness of, any food can be made that is misleading or deceiving or that contravenes the provisions of the food safety laws.

## Targeted advertising and online behavioural advertising

### 18 What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

The term 'online advertising' has not been specifically defined under Indian law. However, laws that regulate publication or advertisement of content in physical form are medium agnostic and are equally applicable to content over the internet. Further, as per section 2(1) of the Consumer Protection Act, 2019 (CPA 2019), 'advertisement' means any audio or visual publicity, representation, endorsement or pronouncement made by means of, inter alia, electronic media, internet or website and includes any notice, circular, label, wrapper, invoice or such other documents. Accordingly, advertisements need to comply with the CPA 2019, in addition to other laws that regulate advertising.

## Misleading advertising

### 19 Are there rules against misleading online advertising?

Yes. In addition to certain industry-specific laws, the CPA 2019 prohibits, inter alia, the following trade practices used for the purpose of promoting the sale, use or supply of any goods, or the practice of making any statement that:

- falsely represents that the goods or services are of a particular standard, quality, quantity, style or model;
- falsely represents any re-built, second-hand, renovated, reconditioned or old goods as new goods;
- represents that the goods or services have sponsorship, approval, performance, characteristics, uses or benefits that such goods or services do not have;
- makes a false or misleading representation concerning the need for, or the usefulness of, any goods or services;
- gives to the public any warranty or guarantee of the performance or efficacy of a product that is not based on proper tests; and
- permits the publication of any advertisement for the sale of goods or services at a bargain price that are not intended to be offered for sale at such price.

Given that there are no separate rules that regulate online advertising, the relevant provisions of the IT Act and CPA 2019 are applicable to misleading advertising in the online space too. As per section 2(28) of the CPA 2019, an advertisement that (1) falsely describes such

product or service; (2) gives a false guarantee to, or is likely to mislead the consumers as to the nature, substance, quantity or quality of such product or service; (3) conveys an express or implied representation that, if made by the manufacturer or seller or service provider thereof, would constitute an unfair trade practice; or (4) deliberately conceals important information, will be construed as a misleading advertisement in relation to any product or service. Misleading advertisements are not permitted under the CPA 2019.

The Advertising Standards Council of India (ASCI) may call upon advertisers and advertising agencies to substantiate all descriptions, claims and comparisons that can be objectively ascertained. For instance, with respect to food and beverages, the ASCI Code mandates that advertisements should not be misleading or deceptive. Specifically, advertisements should not mislead consumers to believe that consumption of the product advertised will result directly in personal changes in intelligence, physical ability or exceptional recognition. Such claims, if made in advertisements, should be supported with evidence and with adequate scientific basis. In the context of misleading advertising, the ASCI has recently issued guidelines for celebrities in advertising (the Celebrity Guidelines). These Celebrity Guidelines have been developed to ensure that claims made in advertisements featuring celebrities or celebrity endorsements are not misleading, false or unsubstantiated. The Celebrity Guidelines impose certain obligations on the advertiser as well as the celebrity, for example:

- it is the duty of the advertiser to make sure that the celebrity they wish to engage in an advertisement is aware of the ASCI Code and such advertisements should not violate any guidelines of the ASCI Code;
- celebrities should not participate in advertising any products that, by law, require a health warning;
- celebrities should also not participate in advertising products, treatments or remedies that have been banned under the Drugs and Magic Remedies (Objectionable Advertisements) Act 1954 and Drugs and Cosmetics Act 1940 and the rules thereunder;
- endorsements, representations of opinions or preference of celebrities in the advertisement must reflect their genuine opinion and must be based upon adequate information or experience with the product or service being advertised; and
- celebrities should do their due diligence to ensure that all descriptions, claims and comparisons made in the advertisement they appear in or endorse are capable of being objectively ascertained and capable of substantiation and should not mislead or appear deceptive.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

Yes. Advertising of products such as cigarettes, tobacco and its derivatives, alcohol, infant milk substitutes, certain drugs, firearms and lotteries are prohibited under different laws, whether on the internet or otherwise. Note that there is no specific prohibition with respect to advertisements in the online space. These restrictions and prohibitions are medium agnostic.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

There are no regulations in India regulating marketing activities undertaken through email or other similar distance marketing methods. However, in relation to SMS, the Telecom Commercial Communications Customer Preference Regulations 2018 (TCCPR) prohibit the sending of unsolicited commercial communications (UCC) in India. UCC is defined under the TCCPR to mean any commercial communication (which includes a call or SMS for promoting products or services) that is not as per the consent or the registered preferences of the recipient of the call or SMS. The responsibility to ensure compliance with the TCCPR is imposed on the telecom service provider. Any person required to share commercial communications is required to obtain services of the telecom services provider and comply with codes of practice (CoP) published by such telecom service provider. These CoP prescribe processes for, inter alia, registering consent of the customer and whitelisting templates for transactional and promotional messages.

The Insurance Regulatory and Development Authority of India has also issued sector-specific Guidelines on Distance Marketing of Insurance Products to regulate the distance marketing activities of insurers/brokers and corporate agents (with approval of insurers) at the stages including offer, negotiation as well as conclusion of sale.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

The primary obligation under Indian law is cast upon the content providers to ensure that content hosted or published in any form does not violate any applicable laws. Depending on the nature of the contravention, the content providers may be subject to civil and criminal liabilities. However, electronic intermediaries such as ISPs, search engines and online marketplaces are eligible to benefit from the safe harbour provisions under the IT Act. To be eligible to take benefit of safe harbour laws, the intermediary is required to comply with certain conditions, for example:

- the intermediary's role must be limited to providing access to information made available by third parties;
- the intermediary must not initiate the transmission of data made available by third parties;
- the intermediary must not select the receiver of the transmission; and
- the intermediary must not select or modify the information contained in the transmission.

It also needs to be demonstrated that the intermediary has observed 'due diligence' in discharging its duties under the IT Act and the IT Intermediary Guidelines, which require that the intermediary should not conspire, abet, aid or induce the commission of the unlawful

act and should also expeditiously remove or disable access to objectionable content upon receiving knowledge.

## Content liability

### 23 When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

Under the Information Technology Act 2000 (the IT Act) and the Intermediary Guidelines, an intermediary is required to observe due diligence in discharging its duties that, inter alia, require publishing of the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person.

As per the Data Protection Bill 2019, where the website provider is an intermediary, it may be entitled to avail of safe harbour provisions, provided it meets the requirements under the IT Act and Intermediary Guidelines. However, where the website provider itself uploads contents on the website, it may be held liable if such content is not in accordance with the provisions of the IT Act, the relevant rules and the guidelines.

Further, as per the code of ethics provided under the Intermediary Guidelines, a publisher shall take into consideration the following factors, when deciding to feature or transmit or publish or exhibit any content, after duly considering the implications of any content as falling under the following categories, and shall exercise due caution and discretion in relation to the same, namely: (1) content that affects the sovereignty and integrity of India; (2) content that threatens, endangers or jeopardises the security of the state; (3) content that is detrimental to India's friendly relations with foreign countries; and (4) content that is likely to incite violence or disturb the maintenance of public order.

## Shutdown and takedown

### 24 Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

The earlier position has now been diluted by the above-mentioned judgment of the SC in the *Shreya Singhal* case. Previously, if an ISP had knowledge, either by itself or through being informed by an affected person, that content stored, hosted or published on the web page contains unlawful material, including defamatory content, it was under an obligation to disable, remove access to or take down such information expeditiously within 36 hours. However, in view of the aforesaid judgment, the ISP is not now obligated to remove or disable access to offending material unless there is a court order or a notification from a government agency in this regard. Once an ISP has received such a court order, it has 36 hours to remove or disable such content. Having said that, if the ISP still wants to block a web page containing defamatory material, a prior court order is not required under law.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

If a database on a website constitutes a copyrightable work in terms of the Copyright Act 1957 (the Copyright Act) and the website provider is the owner of such copyrightable work, it can prevent or restrict other people from using or reproducing data from the database.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Any hyperlinking of a domain name of a third-party website without the express permission of the third-party trademark owner may be construed as infringement under the trademark law and copyright law.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

No. Use of any third-party content on the website without the consent of the third-party content provider constitutes copyright infringement, unless such use is recognised as fair use under the Copyright Act. In terms of the Copyright Act, the potential consequences for copyright infringement could be civil as well as criminal in nature. For instance, in the case of copyright infringement, the owner of the copyright may be entitled to civil remedies such as an injunction and compensation or direct damages; or there may be criminal remedies in the form of imprisonment or fines in cases where a person knowingly infringes or abets the infringement of copyright.

### Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Due to the complex nature of operations in the metaverse, it may be difficult to identify the infringers and the infringements. Artificial intelligence and automated systems may be deployed for ensuring that infringement of copyright, trademark or patent in the metaverse is identified and addressed.

Further, there is no dedicated law dealing with infringement of copyright, trademark or patent in the metaverse, and therefore the intellectual property protection laws that are currently adopted in the physical, or real, world may also apply to the metaverse.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

### Exhaustion of rights – trademarks

Section 30(3) of the Trade Marks Act 1999 (Trade Marks Act) recognises exhaustion of rights of the proprietor of a trademark after the first sale of goods, provided that:

> *Where the goods bearing a registered trade mark are lawfully acquired by a person, the sale of the goods in the market or otherwise dealing in those goods by that person or by a person claiming under or through him is not infringement of a trade mark by reason only of: (a) the registered trade mark having been assigned by the registered proprietor to some other person, after the acquisition of those goods; or (b) the goods having been put on the market under the registered trade mark by the proprietor or with his consent.*

The aforesaid provision recognises the principle of international exhaustion. Further, the Trade Marks Act provides that the aforesaid provision does not apply where the owner has legitimate reasons to oppose dealings in the goods, particularly if the goods are changed or impaired after they have been made available in the market.

### Exhaustion of rights – copyrights

Copyright covers a wide variety of works in its contours. These include artistic, dramatic, literary, cinematic and academic works. The owner of a copyright has a bundle of rights in respect of the work. This bundle of rights can be traced in the Indian Copyright Act 1957 under section 14(1), which makes it clear that, irrespective of the kind of work in question, it is the exclusive right of the owner to issue copies of the work to the public or communicate it to the public. The Doctrine of First Sale in relation to copyright is work-specific and is not uniform, and varies in its application due to the classification of works into different kinds.

### Exhaustion of rights – patents

India recognises the principle of international exhaustion under section 107-A(b) of the Indian Patents Act 1970, which provides that 'importation of patented products by any person from a person who is duly authorised under the law to produce and sell or distribute the product, shall not be considered as an infringement of patent rights'.

There is no specific law dealing with exhaustion of rights or the first sale doctrine in relation to the metaverse.

### Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Yes. For instance, the Copyright Act empowers police authorities in India to seize infringing copies if the officer concerned is satisfied that an offence in respect of the infringement of copyright in any work has been committed. There have also been a few occasions where courts have passed orders in the nature of Mareva injunctions in India to restrain the defendants from disposal of their assets until conclusion of the trial or pending judgment in infringement actions instituted by IP owners.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Ordinarily the relief sought by IP owners includes:

- permanent injunction restraining defendants from infringing the owner's IP rights;
- permanent injunction restraining the defendant from selling the infringing product;
- destruction of goods infringing the IP rights;
- submission or seizure of books of accounts of the defendant;
- compensation in the nature of damages; and
- in a few cases, punitive damages.

Indian courts do not ordinarily grant punitive damages, but there have been a few instances where they have been awarded in matters involving IP infringement.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

While 'personal data' has not been defined under the Information Technology Act 2000 (the IT Act), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the SPDI Rules) framed thereunder define personal information as any information that relates to a natural person and that, directly or indirectly, is capable of identifying such person.

Further, the Data Protection Bill also defines personal data as data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

Further, the SPDI Rules define 'sensitive personal data or information' as personal information that consists of information relating to:

- passwords;
- financial information, such as bank accounts, credit cards, debit cards or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation;
- medical records and history;
- biometric information; and
- any details relating to the above as provided to body corporates for providing services.

A body corporate that collects, receives, stores, deals or handles personal information is required to frame a privacy policy. Such privacy policy is required to be published on the body corporate's website and shall include information pertaining to:

- statement of practice and policies;
- type of sensitive information being collected;
- purpose and usage of such information;
- circumstances in which such information may be disclosed; and
- security practices and procedures for securing against unauthorised access or disclosure of such information.

The SPDI Rules prescribe that prior to collecting 'sensitive personal data or information', a body corporate is required to obtain written consent from the provider of information (ie, the data subject) regarding the purpose of usage of such information. Accordingly, while collecting such information, the body corporate is required to ensure that the data subject is made aware that the information is being collected, the purpose for which the information is being collected, the intended recipients, and the name and address of the agency responsible for collecting and retaining such information. The SPDI Rules further stipulate that sensitive personal data can be collected only for a lawful purpose connected with the function of the body corporate and when the collection of such data is considered necessary for such purpose. Once such a purpose is fulfilled, the body corporate can no longer retain such information.

Prior to the collection of such data, the body corporate is required to provide an option to the data subjects not to provide the information sought to be collected. If the data subject does not provide consent or subsequently withdraws his or her consent, the body corporate has the option not to provide any services or goods for which the said information was sought.

The SPDI Rules also stipulate that the data subject should be given an opportunity to review the information provided and ensure that any inaccuracy or deficiency in the information provided is corrected. While the SPDI Rules do not provide a specific mechanism to be put in place, such opportunity should be available to data subjects as and when requested by them.

Under the SPDI Rules, the central government has prescribed the ISO/IEC 27001 standard for Information technology – Security techniques – Information security management system – Requirements, issued by the International Organization for Standardization and

International Electrotechnical Commission (ISO 27001), as one of the standards that a body corporate dealing with sensitive personal information may implement.

Indian law does not contemplate the conversion of personal data into anonymous data to overcome the applicability of the SPDI Rules. However, if the information is collected on an anonymous basis without it referring to a particular natural person, it is possible to take the view that the SPDI Rules are not applicable with respect to such information.

## Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

No. There is no requirement for parties involved in the processing of personal data to either register with any regulator or appoint an in-house data protection officer.

Further, certain entities involved in collection and processing of personal data or information are mandated to appoint a grievance officer to address the discrepancies and grievances of the providers of such information in a timely manner and also to publish the name and contact details of such grievance officer on their website.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The IT Act has extraterritorial jurisdiction to the extent that it is applicable to any contravention committed outside India by any person, irrespective of his or her nationality, if it involves a computer or a computer system or a computer network in India. In other words, applicability of the IT Act is agnostic to the physical presence of servers in India, and to the extent that users in India can access services by using a computer, computer system or computer network in India, the provisions of the IT Act would be applicable.

With respect to the transfer of sensitive personal information, the SPDI Rules allow a body corporate to transfer such data to any other body corporate or a person in India, or located in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, such transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the data subject or where such person has consented to the data transfer. In other words, sensitive personal data can only be transferred to another person with the consent of the data subject.

Further, the Data Protection Bill proposes to regulate the processing of personal data of individuals that is processed by the government, companies registered in India and foreign companies. The applicability of the Data Protection Bill extends to the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is: (1) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or (2)

in connection with any activity which involves profiling of data principals within the territory of India.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

In India, the IT Act, read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules), defines 'personal information' (PI) and 'sensitive personal data or information' (SPDI) and prescribes the standards for the collection, processing, retention and transfer of PI (including SPDI). PI can be processed for any lawful purpose connected with a function or activity of the body corporate collecting such PI – for example, service providers, intermediaries and employers. Such information can only be transferred to another entity in India or any other country that maintains the same level of data protection as required under the Privacy Rules, and should be done only if this is necessary for the performance of a contract between the transferor and the data principal, or with the consent of the provider of the information.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

There are no specific rules concerning the export or transfer of personal data to another jurisdiction.

Section 75 of the IT Act provides for the extra-territorial applicability of the Act. It provides that the provisions of the Act shall apply to any offence committed by any person irrespective of their nationality, provided such act or conduct constituting the offence involves a computer, computer system or computer network located in India.

Sections 43A and 72A of the IT Act provide for the payment of compensation and punishment in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

Therefore, when sensitive personal data is taken outside the territories of India and involves a computer, computer system or computer network located in India, sections 43A and 72A of the IT Act may be applicable.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

While the SPDI Rules do not expressly contemplate sale of personal data, transfer of personal information is permitted provided the data subject has consented to such transfer. Hence, by implication, the sale or licence of sensitive personal information may be permissible subject to disclosure of such conditions under the privacy policy and a valid contract with the data subject. In terms of Rule 6 of the SPDI Rules, a body corporate must seek prior permission of the information provider before disclosing such information to a third party.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

A person aggrieved of impermissible processing of sensitive personal data is entitled to claim damages by way of compensation under the IT Act. Any person (including a foreign national) may claim such damages by way of compensation under the IT Act.

Further, the Data Protection Bill 2019 also stipulates punishment for obtaining, disclosing, transferring or selling personal or sensitive personal data, knowingly or intentionally or recklessly, to another person resulting in significant harm to the data principal (ie, the natural person to whom the data belongs).

## Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

At present, India does not regulate the use of non-personal data. However, this may change soon as per the recommendations given by the Committee of Experts on Non-Personal Data Governance Framework formulated by the Ministry of Electronics and Information Technology (MEITY), which submitted its report in July 2020.

The Committee has defined three categories of non-personal data: (1) public non-personal data; (2) community non-personal data; and (3) private non-personal data.

The Committee has also defined a new concept of 'sensitivity of non-personal data', as even non-personal data could be sensitive in that (1) it may relate to national security or strategic interests, (2) it may be business sensitive or confidential information, or (3) it may be anonymous data that bears a risk of re-identification.

The Committee observed that non-personal data should be regulated.

Further, in May 2022, MEITY released its draft National Data Governance Framework Policy (Policy) which provides guidance on the procedures and security standards to be

implemented by the government for all non-personal data handled and collected by it. The policy aims to standardise and improve the government's data collection and management.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

There are no rules that require any document or record to be kept in original paper form and not instead be converted to a digital medium. In addition, this position has been reinforced under the Information Technology Act 2000 (IT Act), which states that in the event any law requires a document to be maintained in printed or written form, such requirement is considered to be satisfied even if such information or matter is made or rendered available in electronic format and is accessible as usable for subsequent reference.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Sector-specific regulations have prescribed storage requirements for certain kinds of documents and records. For instance:

- the IT Act, read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, provides that sensitive personal data or information (SPDI) can only be retained until such time the purpose for which such SPDI was collected is achieved, or unless otherwise required by applicable law;
- the Companies Act 2013 prescribes that any books of accounts and related vouchers, documents, etc should be retained for a period of not less than eight financial years;
- the Insurance Regulatory and Development Authority of India has issued the Insurance Cyber Guidelines, which require all registered insurance companies to maintain security logs of different systems and devices, to be retained for a minimum period of six months; and
- in accordance with the Securities Exchange Board of India Guidelines (Cyber Security & Cyber Resilience Framework for Stock Brokers/Depository Participants), stockbrokers and depository participants are required to ensure that records of user access to critical systems are identified and logged for audit and review purposes, and the logs should be maintained and stored in a secure location for a period of not less than two years.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

Pursuant to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules), any body corporate that possesses, deals with, or handles any sensitive personal data or information in a computer resource is required to implement prescribed security standards (ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements). Sector-specific cybersecurity measures have been made mandatory by regulators for some regulated businesses. For instance, in the banking sector, the Reserve Bank of India (RBI) requires banks to undertake certain security measures including, inter alia, logical access controls to data, systems, application software, utilities, telecommunication lines, libraries and system software; using the proxy server type of firewall; using secured socket layer (SSL) for server authentication; and encrypting sensitive data, such as passwords, in transit within the enterprise itself. The RBI specifically mandates that connectivity between the gateway of the bank and the computer system of the member bank should be achieved using a leased line network (and not through the internet) with an appropriate data encryption standard and that 128-bit SSL encryption must be used as a minimum level of security.

Additionally, in the telecommunications sector, the licence conditions imposed by the Department of Telecommunication (DOT) require every licensee to:

- ensure protection of privacy of communication so that unauthorised interception of messages does not take place;
- have an organisational policy on security and security management of its network, including network forensics, network hardening, network penetration tests and risk assessment; and
- induct only those network elements into its telecom network that have been tested as per relevant contemporary Indian or international security standards (eg, the IT and ITES elements) against the ISO/IEC 15408 standards (eg, the ISO 27000 series standards for information security management systems and the 3GPP and 3GPP2 security standards for telecoms and telecoms-related elements).

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

There is no specific requirement under the IT Act to inform the data subject of a cybersecurity incident. However, under the Intermediary Guidelines, the intermediary is required

to inform the Computer Emergency Response Team (CERT-In) of cybersecurity breaches as soon as possible. Further, specific types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, etc) must be mandatorily reported to CERT-In by service providers, intermediaries, data centres and body corporates within a reasonable time of the occurrence or noticing the incident to aid timely action.

The CERT Rules permit cybersecurity incidents to be reported by any person to CERT-In. However, specified types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, etc) need to be mandatorily reported to CERT-In by service providers, intermediaries, data centres and body corporates within a reasonable time of the incident occurring or being noticed to aid timely action. The Intermediary Guidelines require the intermediaries, as part of their due diligence obligations, to notify CERT-In of security breaches. CERT-In publishes the formats for reporting cybersecurity incidents on its website from time to time, which requires mentioning the time of occurrence of the incident, the type of incident, information regarding the affected systems or network, the symptoms observed, the relevant technical systems deployed and the actions taken, among others.

In addition, sector-specific regulators have their own reporting requirements. For instance, the Reserve Bank of India (RBI) requires banks to comply with the Cybersecurity Framework for Banks, which, inter alia, requires banks to report cybersecurity incidents to the RBI within six hours.

## Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

In a recent judgment in the case of *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* (Writ Petition (Civil) No. 494 of 2012), the Supreme Court of India held the right to privacy to be a fundamental right that is an intrinsic component of the right to life and personal liberty under article 21 of the Constitution of India and therefore a basic right of all individuals. Although there are precedents where the courts have held private communications between individuals to be covered within the purview of 'right to privacy', there are also precedents where Indian courts have admitted recordings obtained without consent as valid evidence. Given that this issue is unsettled, permissibility of recordings will need to be determined on a case-by-case basis. In any case, the SPDI Rules require body corporates to disclose personal data or sensitive personal information subject to prior consent of the data subject. However, this condition can be waived if the disclosure is to government agencies mandated under the IT Act for the purpose of verification of identity, or for the prevention or investigation of any offences, including cybercrimes.

Certain laws, such as the Indian Telegraph Act 1885 (the Telegraph Act) and the Information Technology Act 2000 (the IT Act), permit governmental and regulatory authorities to access private communications and personally identifiable data in specific circumstances. The Telegraph Act empowers the government to intercept messages in the interest of public safety, national security or the prevention of crime, subject to certain prescribed safeguards.

In that scenario, the telecoms licensee that has been granted a licence by the DOT is mandated to provide necessary facilities to the designated authorities of the central government or the relevant state government for interception of the messages passing through its network.

The IT Act also grants similar authority to the government and its authorised agencies. Any person or officer authorised by the government (central or state) can, inter alia, direct any of its agencies to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted, any information that is generated, transmitted, received or stored in any computer resource, in the event it is satisfied that it is necessary or expedient to do so in the interest of sovereignty and the integrity of India, the defence of India, the security of the state, friendly relations with foreign states, public order or preventing incitement to the commission of any cognisable offence relating to the above, or for the investigation of any offence. In our view, the instances described in the IT Act can be relied on by the government agencies to intercept data for cybersecurity incidents if they relate to contravention or investigation of any crime.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

The Public Gambling Act 1867 (the Gambling Act) prohibits and punishes public gambling and gaming activities in common gaming houses in India. While the Gambling Act prohibits a pure 'game of chance', it specifically excludes (from its ambit) any game of 'mere skill'.

The Punjab and Haryana High Court in *Shri Varun Gumber v Union Territory of Chandigarh and Others* analysed the legal sanctity of fantasy league games in India in view of the Gambling Act. The court held that the playing of fantasy games by a user involves various skill-based activities that require considerable skill, judgement and discretion, for instance, preparing the right team combination, studying the rules and the sportspersons' strengths and weaknesses, statistics, etc. In view of these factors, the court held that such fantasy games predominantly amount to a 'game of skill' with only an incidental element of chance, and accordingly are outside the ambit of the Gambling Act.

While various states in India have adopted the Gambling Act, certain states have also enacted their own state-specific laws to regulate gaming and gambling activities within their respective territory. Online gaming is specifically regulated in the state of: (1) Sikkim, where the Sikkim Online Gaming (Regulation) Act 2008 regulates online gaming and betting via electronic or non-electronic formats; and (2) Nagaland, where the Nagaland Prohibition of Gambling and Promotion and Regulation of Online Games of Skill Act 2016 regulates online games of skill.

Further, the Intermediary Rules were amended on 6 April 2023 to include provisions that govern online gaming, including online real money games. By doing so, it has also distinguished online real money games from gambling – a prohibited activity.

The following definitions have been added to the Intermediary Rules by way of the aforesaid amendment:

- online gaming: a game that is offered on the internet and is accessible by a user through a computer resource or an intermediary;
- online gaming intermediary: any intermediary that enables the users of its computer resource to access one or more online games;
- online gaming self-regulatory body: an entity designated under the Intermediary Guidelines for the purposes of verifying an online real money game as a permissible online real money game under the Intermediary Rules;
- online real money game: an online game where a user makes a deposit in cash or kind with the expectation of earning winnings on that deposit;
- permissible online game: a permissible online real money game or any other online game that is not an online real money game; and
- permissible online real money game: an online real money game verified by an online gaming self-regulatory body.

Further, the amendment states that the Ministry of Electronics and Information Technology may designate a few online gaming self-regulatory bodies in order to verify whether an online real money game is a permissible online real money game under the Intermediary Rules.

Further, the Intermediary Rules require intermediaries (including social media intermediaries, significant social media intermediaries and online gaming intermediaries) to, inter alia, observe necessary due diligence and publish rules and regulations and user agreements for access or usage of their website. Such rules and regulations and user agreements are required to include terms that, inter alia, inform the users not to host, display, upload, modify, publish, transmit, update or share any information that relates to or encourages gambling. Hence, hosting websites that operate online betting or gaming businesses are not permissible under the Rules, and any such activity can be shut down or taken down by an intermediary or government authorities in accordance with the Rules.

## Cross-border gaming

### 46 Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

In India, advertisements are permitted to the extent that they do not promote any activity that is prohibited by statute or law. Betting and gambling are illegal in most parts of India, and accordingly, advertisement of online betting platforms is restricted. In this regard, the Ministry of Information and Broadcasting issued an Advisory, dated 13 June 2022, advising print and electronic media to refrain from displaying advertisements of online betting platforms in India or targeting such advertisements towards the Indian audience. The Advisory is in continuance of an Advisory issued on 4 December 2020, wherein broadcasters were advised to comply with Advertising Standards Council of India (ASCI) Guidelines on Online Gaming (effective from 15 December 2020).

Read this article on Lexology

Advertisements pertaining to gaming businesses are permitted, to the extent such advertisements are related to those games that involve an element of skill and follow the ASCI Guidelines on Online Gaming for static/print and audio-visual advertisements.

There are no separate rules for advertisements in the metaverse, and these are permitted so long as such advertisements do not promote any activity that is prohibited by statute or law.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

An outsourcing contract would ordinarily result in an end product, the ownership of which will be at the heart of the contractual arrangement. This will necessarily involve issues with respect to ownership of intellectual property, particularly copyright. Since copyright created in the course of a contract for service is commissioned and owned by the contractor to begin with, the outsourcing contract should contain unambiguous provisions regarding the ownership and assignment of copyright. Provisions with respect to indemnity and limitation on liability are generally highly negotiated. In a cross-border scenario, the non-resident party has to bear in mind that prior Reserve Bank of India approval may be required before any amount can be remitted on account of damages. There is substantial emphasis on meeting service-level agreements and failure may have significant business continuity issues. Dispute resolution provisions, particularly regarding the ability to obtain interim relief, may also be equally important from the perspective of the service recipient.

Receipt of consideration for provision of services by a service provider may be subject to taxation in India, including good and services tax (GST), depending on factors such as the specific nature or character of such services, presence of permanent establishment, availability of treaty benefits and the like. In the event such consideration is taxable in India, the service provider may be required to undertake compliances such as obtaining relevant GST and income tax registration, discharge of the applicable taxes, issuance of relevant documents such as invoices and filing of relevant tax returns in India. Additionally, the service recipient may also be required to withhold applicable taxes and undertake requisite compliances. Accordingly, this would require a detailed examination based on specific facts.

In this regard, it may further be noted that typically, the compliances related to GST including obtaining GST registration, depositing the applicable GST on a taxable supply of service, issuance of invoice and filing of returns is on the supplier or provider of such service. However, for certain specified services, including on import of services, such compliances are required to be undertaken by the recipient of such service under the reverse charge mechanism.

## Sector-specific issues

### 48 Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

Based on the nature of business, certain regulators have issued specific outsourcing guidelines and regulations in relation to the regulated entities, such as:

- Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs – issued by the Reserve Bank of India (RBI);
- Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators – issued by the RBI;
- IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017 – issued by the Insurance Regulatory and Development Authority of India (IRDAI); and
- Guidelines on Outsourcing of Activities by Intermediaries – issued by the Securities and Exchange Board of India (SEBI).

Some of these sectoral regulations impose restrictions on the nature of activities that can be outsourced. For instance, the NBFC Outsourcing Guidelines provide that non-banking financial companies (NBFCs) should not outsource core management functions, including internal audit, strategic and compliance functions, and decision-making functions, such as determining compliance with know-your-customer norms for opening deposit accounts, sanction of loans (including retail loans) and management of investment portfolios.

## Contractual terms

### 49 Does the law require any particular terms to be included in outsourcing contracts?

While there is no overarching outsourcing law in India, as stated above there are multiple sector-specific guidelines and regulations that govern the outsourcing arrangements for regulated entities in India, and that provide for certain standard clauses to be included under such outsourcing arrangements. For example:

- as per the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017, the outsourcing arrangements entered into by an insurer with an outsourcing service provider located in India or outside India require clauses in relation to information and asset ownership rights, information technology, data security, guarantee or indemnity from the outsourcing service provider, contingency planning, etc;
- as per the Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators, the outsourcing arrangements that payment system operators enter into with third-party service providers should include provisions for scope of services, charges for services and maintaining confidentiality of customers' data, etc; and
- as per the Guidelines on Outsourcing of Activities by Intermediaries, the outsourcing agreements for intermediaries registered with SEBI should include provisions for the activities to be outsourced, appropriate service and performance levels, mutual rights, obligations and responsibilities of the intermediary and the third party, indemnity, continuous monitoring and assessment by the intermediary, etc.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

Under Indian law, employees have no rights when services performed by them are outsourced to a service provider (including consultation or compensation rights).

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

The Ministry of Commerce and Industry set up an Artificial Intelligence Task Force in August 2017 with a view to 'embed AI in Economic, Political and Legal thought processes so that there is systemic capability to support the goal of India becoming one of the leaders of AI-rich economies'.

To prepare a roadmap for a national AI programme, and to study AI in the context of four important perspectives, the Ministry of Electronics and Information Technology set up four committees to look at the following: citizen-centric services; data platforms; skilling, reskilling and R&D; and legal, regulatory and cybersecurity. These committees have published their reports, which are available on the Ministry's website.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Currently, there is no explicit law in India pertaining to AI and its legal status. However, there could be certain changes in the laws to cope with situations when AI and machine learning will be more advanced, especially with respect to intellectual property.

With respect to ownership rights, the approach of the legislature has been to include in the legislation only legal and natural persons for consideration as the owners of copyrights, intellectual property rights and patents in India.

In July 2021, the Standing Committee set up by Parliament published a report titled Review of Intellectual Property Rights Regime in India, wherein it recommended, inter alia, that a

separate category of rights for AI and AI-related inventions and solutions should be created. It further recommended that the Department Related Parliamentary Standing Committee on Commerce should make efforts in reviewing the existing legislation (the Patents Act 1970 and Copyright Act 1957) to incorporate the emerging technologies of AI and AI-related inventions in their ambit.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Presently, India does not have a law that regulates artificial intelligence (AI) and machine learning.

In February 2018, MEITY created four committees to promote AI initiatives and prepare a policy framework for AI. These four committees have released their reports on various aspects of AI such as:

- development of an enriched National Artificial Intelligence (AI) Resource Platform (NAIRP) of India;
- upskilling manpower for conducting research and development of AI;
- leveraging AI for identifying national missions in key sectors; and
- cyber security, safety, legal and ethical issues of the use of AI.

The National Institution for Transforming India (NITI) Aayog, a government think tank that advises the government on public policy and ensures inter-state coordination, published a report titled 'Responsible AI, #AIFORALL, Approach Document for India' in February 2021. The report proposes principles for the responsible management of AI systems that may be leveraged by relevant stakeholders in India. Case studies of AI systems in India and around the world were studied and the principles for responsible AI were derived in the said report from the Constitution of India and other laws, such as the IT Act. The report also derived principles from the laws and policies of other jurisdictions.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Indian indirect tax laws have undergone a complete overhaul with the introduction of the Goods and Services Tax (GST) with effect from 1 July 2017. As per the Indian GST laws, the supply of all goods and services within India, which, inter alia, includes sale (whether online or offline), barter, exchange and lease, etc, is subject to GST, unless specifically exempted. The import of goods is separately liable to customs duties, a component of which includes GST distinct from the GST payable on supply of goods or services. The rate of such taxes varies depending upon the classification of such goods and their nature.

Separately, in terms of the current GST framework, an e-commerce operator (who owns, operates or manages an e-commerce platform) is required to collect tax at source (TCS), at a rate of 1 per cent on the net value of taxable supplies of goods and services made by the vendors through the e-commerce platform, where the consideration for such supply is to be collected by the e-commerce operator. Further, TCS is to be collected once supply has been made through the e-commerce operator and the business model is such that the consideration is to be collected by the e-commerce operator, irrespective of the actual collection of consideration. The provisions related to TCS under the Indian GST laws were made applicable with effect from 1 October 2018.

## Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Placing of servers within India by an offshore entity could be subject to GST in India, depending on the specifics of how such server is used in providing services within India or carrying on business in India. Accordingly, the taxability of placing servers within India by an offshore entity needs to be examined in light of specific facts and circumstances.

## Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The e-invoicing system under the goods and services tax (GST) regime was implemented with effect from 1 October 2020 for taxpayers with an aggregate turnover exceeding 5 billion rupees. Subsequently, the e-invoicing requirement was extended to businesses with an aggregate turnover exceeding 1 billion rupees. Thereafter, the Central Board of Indirect Taxes and Customs (CBIC) notified the applicability of the e-invoicing requirement to businesses with an aggregate turnover ranging between 500 million rupees and 1 billion rupees, with effect from 1 April 2021. The government recently extended the applicability of the e-invoicing requirement to businesses having turnover of more than 200 million rupees, with effect from 1 April 2022.

The e-invoicing requirement shall not be applicable to the following categories of registered persons, irrespective of turnover, as notified in the CBIC's Notification No. 13/2020:

- an insurer or a banking company or a financial institution, including a non-financial banking company;
- a goods transport agency;
- a registered person supplying passenger transportation services;
- a registered person supplying services by way of admission to the showing of cinematographic films in multiplex services;
- a Special Economic Zone unit (excluded via CBIC Notification No. 61/2020); and

- a government department and local authority (excluded via CBIC Notification No. 23/2021).

There is no requirement to issue invoice copies in triplicate or duplicate, if e-invoicing is applicable to the taxpayer.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

Under the Information Technology Act 2000 (the IT Act), an adjudicating officer, appointed by the central government, is empowered to adjudicate the offences pertaining to contravention of any of the provisions of the IT Act or of any rule or regulation, made thereunder. The IT Act also stipulates that the Telecom Disputes Settlement and Appellate Tribunal established under the Telecom Regulatory Authority of India Act 1997 will be the Appellate Tribunal for the purposes of the IT Act.

Separately, the Reserve Bank of India has established offices of 'ombudsman' across various locations in India in respect of customer complaints including arising from prepaid instruments, e-wallets and other payment service providers.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

There are no specific ADR methods available under Indian law in respect of online and digital disputes, however, the regular ADR methods available under Indian law may be used for online and digital disputes as well.

Given the rise in online and digital disputes in India, the use of ADR methods available under Indian law has also increased.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

Given the increasing growth of the digital economy, it has been the government's endeavour to take active steps towards ensuring protection of the personal data of citizens. The law, in this regard and in light of a Supreme Court of India judgment affirming the right to privacy to be a fundamental right under the decision reached in *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* is proposed to be overhauled. The Ministry of Electronics and Information Technology constituted a committee of experts under Justice B N Srikrishna, Former Judge of the Supreme Court (Committee) to deliberate on a framework for data protection, to identify key data protection issues and recommend methods of addressing such issues under the draft Data Protection Bill 2018, which was later on substituted by the Data Protection Bill 2019.

The Data Protection Bill seeks to protect the autonomy of individuals with respect to their personal data, specify norms of data processing by entities using personal data, and set up a regulatory body to oversee data processing activities. However, the Data Protection Bill is yet to be introduced in the legislature.

In addition, in February 2019, the Department for Promotion of Industry and Internal Trade (DPIIT) created the Draft National e-Commerce Policy (NCP). The NCP aims to create a framework for regulating the e-commerce sector in the country along with the existing policies of Make in India and Digital India. The NCP also lays down strategies to address issues pertaining to, inter alia, consumer protection, data privacy and the e-commerce marketplace. However, the NCP is yet to be introduced in the legislature.

Separately, the Consumer Protection Act 2019 (CPA 2019) has been passed, wherein the term 'electronic service provider' has been introduced and is defined to include online marketplaces. The CPA 2019 also implicitly recognises that product liability claims in respect of a product should be made against the seller and not the electronic service provider. The recognition of an electronic service provider under the consumer protection law is a notable development since an express recognition of the distinction in liabilities of the seller and an e-commerce marketplace does not exist under the consumer protection laws of India, despite having been acknowledged in some decisions of consumer protection forums. Further, The Department of Consumer Affairs in the Ministry of Consumer Affairs, Food and Public Distribution issued the Consumer Protection (E-Commerce) Rules 2020, which came into force on 23 July 2020. Thereafter, the Ministry of Consumer Affairs, Food and Public Distribution notified the Consumer Protection (E-Commerce) (Amendment) Rules 2021 on 17 May 2021 to amend the E-Commerce Rules. These rules are proposed to be further modified, and a draft of the proposed modifications has been released for public comments. The proposed modifications include registration requirements for e-commerce entities and a requirement that they implement grievance redressal mechanisms, and impose other stringent requirements.

The Information Technology Act 2000 (the IT Act) provides exemption from certain liabilities to social media platforms, such as Twitter and Facebook, in respect of content posted by any third party on such forums. It was observed that several contents and comments posted through fake accounts amounting to issues like sedition, defamation, threats, etc, were being committed through such social media platforms.

In a petition filed before the Madras High Court in 2018, by Janani Krishnamurthy and Antony Clement Rubin, seeking, inter alia, mandatory linking of citizen's unique identity numbers (Aadhaar) with users of social media platforms like Twitter, Facebook and YouTube, the Madras High Court, considering the judgment passed in the case of *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors*, held that it shall not be mandatory to link Aadhaar with social media accounts. However, the issue of tracing the originator of a message on social media platforms that have end-to-end encryption by default is yet to be decided.

Thereafter, the Supreme Court, in a *suo moto* writ petition (*Prajjawala* case, see order dated 11 December 2018) observed that the Indian government may frame necessary guidelines to eliminate offences such as child pornography, imageries, videos and sites in content hosting platforms and other applications. The Supreme Court, in an order dated 24 September 2019, directed the Ministry of Electronics and Information Technology to apprise the timeline in respect of completing the process of notifying the new rules. The Ad-hoc committee of the Rajya Sabha presented its report on 3 February 2020 after studying the alarming issue of pornography on social media and its effect on children and society as a whole and recommended enabling identification of the first originator of such contents. In this regard, in supersession of the Information Technology (Intermediaries Guidelines) Rules 2011, the Intermediary Guidelines were notified in February 2021 and came into force on 25 May 2021.

Some of the key features of the Intermediary Guidelines are as follows:

- The Intermediary Guidelines prescribe due diligence that must be followed by intermediaries, including social media intermediaries. If due diligence is not followed by the intermediary, safe harbour provisions will not apply to them.
- The Rules seek to empower users by mandating intermediaries, including social media intermediaries, to establish a grievance redressal mechanism for receiving and resolving complaints from the users or victims. Intermediaries must appoint a grievance officer to deal with such complaints and share the name and contact details of such officer. The grievance officer must acknowledge the complaint within 24 hours and resolve it within 15 days of receipt.
- Intermediaries shall remove or disable access within 24 hours of the receipt of a complaint of content that exposes the private areas of individuals, shows such individuals in full or partial nudity or in sexual acts or in the nature of impersonation including morphed images, etc. Such a complaint can be filed either by the individual or by any other person on his or her behalf.
- To encourage innovation and enable growth of new social media intermediaries without subjecting smaller platforms to significant compliance requirements, the Rules make a distinction between 'social media intermediaries' and 'significant social media intermediaries'. This distinction is based on the number of users on the social media platform. The government is empowered to notify the threshold of the user base that will distinguish between social media intermediaries and significant social media intermediaries.

The Rules require significant social media intermediaries to conduct certain additional due diligence.

Further, the Ministry of Consumer Affairs, Food and Public Distribution has proposed revisions to the draft Consumer Protection (E-Commerce) Rules 2020. It is, inter alia, proposed to define 'cross selling', 'fall-back liability', 'flash-sale' and 'mis-selling', in order to avoid misrepresentation. It is further proposed to make registration with the DPIIT mandatory for all e-commerce entities. The proposed rules also seek to regulate the manner in which consent will be obtained from consumers for the sharing of their data with other persons.

AZB & PARTNERS
ADVOCATES & SOLICITORS

Hardeep Sachdeva hardeep.sachdeva@azbpartners.com
Priyamvada Shenoy priyamvada.shenoy@azbpartners.com
Shagun Badhwar shagun.badhwar@azbpartners.com

Unit No 4B 4th Floor Hansalya Building, Barakhamba Road, New Delhi 110 001, India
Tel: +91 114 022 1500
www.azbpartners.com

# Indonesia

Naufal Fileindi, Eliza Anggasari and Benedict Giankana
Guido Hidayanto & Partners

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The government adopts a relatively welcome but protective approach towards digital businesses in Indonesia – certain local nuances must be taken into consideration by local and foreign players. For instance, foreign electronic systems providers are required to register their electronic system with the Ministry of Communications and Informatics. This requirement has received widespread criticism due to its impracticality, but reflects the government's protective approach towards acting in the national interest. Regulations on cryptocurrency, private electronic system providers, payment services, and financial services have already been established in recent years.

The initial step in regulating digital businesses was conducted through the enactment of Law No. 11 of 2008 on Electronic Information and Transactions (as amended by Law No. 19 of 2016) (the ITE Law). Further regulations were later enacted, such as the obligation to obtain a licence for conducting online trading. Sector-specific regulations have also been established, including regulations on peer-to-peer lending, payment system providers, and regulatory sandboxes for digital financial innovations providers.

Furthermore, the Indonesian government has recently acknowledged the importance of personal data protection through the enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law). Its relevancy is reflected in the use of personal data for digital business, such as the financial information of customers in the financial services sector, or the addresses of customers for expedition purposes in an e-commerce platform.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

- The PDP Law;
- the ITE Law;
- Law No. 8 of 1999 on Consumer Protection (the Consumer Protection Law);
- Government Regulation No. 80 of 2019 on Trade through Electronic Systems;
- Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions;
- Minister of Trade Regulation No. 50 of 2020 on Provisions on Business Licensing, Advertising, Guidance, and Supervision of Business in Trade through Electronic Systems;
- Minister of Communications and Informatics Regulation No. 5 of 2020 on Electronic Systems Providers in the Private Sector (as amended by Minister of Communications and Informatics Regulation No. 10 of 2021);
- Minister of Communications and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems;
- Financial Services Authority Regulation No. 6/POJK.07/2022 of 2022 on Consumer and Public Protection in the Financial Services Sector; and

- Bank of Indonesia Regulation No. 23/6/PBI/2021 of 2021 on Payment Service Providers.

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

- Bank of Indonesia;
- Financial Services Authority;
- Ministry of Communications and Informatics;
- Ministry of Trade;
- Ministry of Transportation; and
- Commodity Futures Trading Regulatory Agency.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Certain rules and regulations, such as the ITE Law, the PDP Law, the Consumer Protection Law and Law No. 28 of 2014 on Copyrights (the Copyright Law), are applicable depending on the type of legal act and its consequences towards the Indonesian jurisdiction, as follows:

- The ITE Law stipulates that its provisions apply extraterritorially; in other words, to all legal acts conducted inside or outside the Indonesian jurisdiction, if said acts have legal consequences inside or outside the Indonesian jurisdiction that harm Indonesian interests.
- The PDP Law states that its provisions apply not only to the Indonesian jurisdiction but outside of it as well, in the event that the legal act has legal consequences within the Indonesian jurisdiction or for Indonesian citizens as data subjects located outside of the Indonesian jurisdiction.
- The Consumer Protection Law stipulates that business actors encompass not only those incorporated and domiciled in Indonesia, but also those who conduct business activities inside the Indonesian jurisdiction.
- The Copyright Law is applicable to all creations of Indonesian citizens, residents, and legal entities.

Provisions in the ITE Law shall apply to general digital business issues, but a specific legal act relevant to a specific law shall be subject to such respective laws. Foreign entities shall also be subjected to the respective laws if so stipulated.

### Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

Most business licensing is now processed through the Online Single Submission (OSS) System established by the Ministry of Investment (previously known as Investment Coordinating Board) in 2018. The procedures and requirements for business licensing, including submission of documents and further verification from the relevant government authorities, are all facilitated by the OSS System. The OSS System facilitates both digital businesses and brick-and-mortar businesses, with no distinct differences in the requirements and procedures aside from sector-specific or business line-specific requirements and business size/scale and risk classification.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Pursuant to Law No. 11 of 2008 on Electronic Information and Transactions (as amended by Law No. 19 of 2016) (the ITE Law), electronic contracts are legally binding on parties. Certain criteria as stipulated in the Indonesian Civil Code and Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions (GR 71/2019) for electronic contracts shall also apply, as follows:

- there must be agreement by the parties;
- the parties must have legal capacity to conclude an agreement;
- the object of the agreement must relate to a specific matter; and
- the object of the agreement must comply with relevant and applicable laws.

Furthermore, an electronic contract must consist of at least the following clauses:

- data of the parties;
- object and specification;
- requirements for electronic transactions;
- price and costs;
- procedures in the event that there is a cancellation by the parties;
- provisions that grant a right to the injured party to return the goods or request a replacement product if there is a latent defect (or both); and
- choice of law for the settlement of electronic transactions.

Though the ITE Law and GR 71/2019 acknowledge the validity of electronic contracts, the prevailing laws and regulations do not establish the validity of 'click-wrap' agreements.

Should the click-wrap agreement fulfil the necessary requirements for validity of an electronic contract, then it may be conducted.

The parties to an electronic contract may also execute such contracts through a digital signature. However, certain contracts are required by law to be entered into by a physical/wet signature and be kept in physical/paper form.

## Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Pursuant to the ITE Law, parties retain the right to determine the choice of law and forum of dispute resolution of a contract. If the parties do not, the choice of law and forum of dispute will be determined in accordance with private international law principles. Furthermore, Law No. 24 of 2009 on National Flag, Language, Coat of Arms and National Anthem and Presidential Regulation No. 63 of 2019 on the Use of Indonesian Language dictate that any agreement executed by an Indonesian party must include an Indonesian version of the agreement. In practice, a bilingual format is preferred.

## Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Digital or e-signatures are recognised as valid signatures in Indonesia. GR 71/2019 stipulates that e-signatures are categorised into certified and non-certified e-signatures. A certified e-signature is obtained by engaging an electronic certification provider and receiving an electronic certificate, while a non-certified e-signature does not undertake the above actions. The main difference between the two is their respective burdens of proof in court proceedings.

An e-signature shall have valid legal force and legal implications if it fulfils the requirements as follows:

- the data used is only related to the signatory party;
- the data used is under the control of the signatory party;
- any changes to the e-signature that occur after the signing are discoverable;
- there are certain methods that can be used to identify the signatory; and
- there are certain methods to indicate that the signatory has provided approval for the relevant electronic information.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

There are no specific dispute resolution forums for breach of digital contracts. Disputes arising out of, and remedies related to, the breach of a digital contract are subject to the laws and regulations applicable to physical contracts.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

There are no specific regulations on the advertising or selling of financial services digitally that have been established. However, general provisions on advertising online are established by the Ministry of Trade.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Electronic money is regulated through Bank of Indonesia Regulation No. 23/6/PBI/2021 of 2021 on Payment Service Providers (BI Reg 23/2021), which stipulates the use of the Indonesian rupiah as the value and currency used in electronic money. E-money is categorised based on its scope of operation as closed loop or open loop. Furthermore, BI Reg 23/2021 also limits the transactional value of electronic money to 20 million Indonesian rupiahs per month.

Indonesia also acknowledges cryptocurrencies, albeit as an asset in the form of an exchangeable futures commodity rather than a currency for payment.

### Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

BI Reg 23/2021 stipulates the obligation of payment transactions to be processed domestically for transactions using access to a source of fund in the form of instruments or services provided by a payment service provider. Additionally, BI Reg 23/2021 stipulates the use of the Indonesian rupiah as the value and currency in digital wallets.

Crypto wallets are yet to be regulated under specific laws, although they are recognised for crypto transactions.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Electronic payment providers are required to comply with the applicable laws and regulations on certain matters, including:

- business competition;
- electronic information and transactions;
- anti-money laundering and prevention of terrorism financing;
- consumer protection;
- implementation of the obligation to use Indonesian rupiahs; and
- personal data protection.

Payment system providers, which includes both banks and non-bank institutions, may cooperate with supporting providers. However, supporting providers are prohibited from accessing or administering a source of fund.

## Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Financial Services Authority Regulation No. 8 of 2023 on the Implementation of Anti-Money Laundering, Prevention of Terrorism Financing, and Prevention of Proliferation of Weapons of Mass Destruction Financing Programs in the Financial Services Sector allows financial service providers to use third parties to conduct KYC and AML identification requirements. However, it must be noted that the obligations and responsibilities of the KYC and AML identification remain with the financial services provider. Additionally, if the third party originates from a country potentially used as a location to conduct money laundering, terrorism financing, and proliferation of weapons of mass destruction financing, the financial services provider may only cooperate with the third party if:

- the financial services provider and the third party are members of the same financial conglomerate;
- the financial conglomerate has implemented AML, prevention of terrorism financing, and prevention of proliferation of weapons of mass destruction financing programmes effectively in accordance with recommendations from the Financial Action Task Force; and
- the financial conglomerate is supervised by a competent authority.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

Domain name registration in Indonesia is conducted on a first-come, first-serve basis. The application is submitted by the applicant to the domain name registry and registrar. There are no specific provisions establishing that non-residents are prohibited from registering a country-specific domain name in Indonesia.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Holders of international trademarks that have been registered in Indonesia are entitled to the registration, usage, and benefit of the domain name in Indonesia. However, it should be noted that domain name registration by such trademark holders must be conducted by a legal entity located in Indonesia.

Trademark holders are not required to present evidence of trademark registration prior to domain registration, however, evidencing trademark registration and ownership can benefit the applicant in any potential dispute.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

Online advertising is governed under Minister of Trade Regulation No. 50 of 2020 on Provisions on Business Licensing, Advertising, Guidance, and Supervision of Business in Trade through Electronic Systems. Its provisions apply universally to every electronic advertisement, regardless of the industry.

## Targeted advertising and online behavioural advertising

### 18 What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Targeted advertising and online behavioural advertising collected based on personal data must receive prior consent from the subject data, as it may be interpreted as processing personal data.

A separate consent for targeted advertising is typically produced on top of the usual consent for data collection and processing.

## Misleading advertising

### 19 Are there rules against misleading online advertising?

Electronic advertising must contain materials adherent to ethics and the prevailing laws and regulations. Further, electronic advertisements must:

- not deceive consumers as to the quality, quantity, materials, uses and prices of goods or service rates, or the timeliness of receipt of goods or services;
- not deceive customers as to the guarantee of the goods or services;
- not contain erroneous, wrong or inaccurate information regarding the goods or services;
- contain information regarding the risks of using the goods or services; and
- not exploit events or people without prior authorised permission or consent.

Electronic advertisements that display a customer's testimony or review of a product or service they have purchased must contain correct information and be conducted responsibly.

Additionally, Law No. 8 of 1999 on Consumer Protection stipulates that misleading advertisement is subject to imprisonment for a maximum of five years or a fine of up to 1 billion rupiah.

## Restrictions

### 20 Are there any digital products or services that may not be advertised online?

Law No. 11 of 2008 on Electronic Information and Transactions (as amended by Law No. 19 of 2016) prohibits the display or availability of electronic content containing obscenity, gambling, slander or defamation, and extortion or threats.

Additionally, according to Minister of Communications and Informatics Regulation No. 5 of 2020 on Electronic Systems Providers in the Private Sector (as amended by Minister of Communications and Informatics Regulation No. 10 of 2021), private electronic system providers must not provide or facilitate:

- the distribution of prohibited electronic information or electronic documents in conducting their services, such as matters that violate Indonesian laws and regulations or that disturb the public and public order; or

- information on how to access or provide access to prohibited electronic information or documents.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

There are no applicable regulations on direct marketing in general. Financial services players are prohibited from conducting marketing and offering products or services to prospective customers through private communication facilities without obtaining the prospective customer's consent.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

A user-generated content platform is exempted from liability. The exemption is granted only if the following actions have been fulfilled:

- the provider has ensured that their electronic system does not contain the prohibited content and does not facilitate the spread of said content;
- the provider has provided subscriber information for the purposes of supervision or law enforcement (or both); and
- the provider has conducted a takedown of the prohibited content.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

Liability will depend on the type of digital platform and its terms of use. User-generated content platforms place the burden of liability against the content maker or provider as the owner of the content, although the digital platform may be prone to liability to a certain extent. If the digital platform runs the platform independently, then the liability will be theirs solely.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Minister of Communications and Informatics Circular Letter No. 5 of 2016 on Limitations and Liabilities of Platform Providers and Merchants in conducting Electronic Commerce in the Form of User-Generated-Content (MOCI CL 5/2016) stipulates the obligation for user-generated content platform providers to remove or block (or both) prohibited content, subject to a complaint or report. Prohibited content pursuant to MOCI CL 5/2016 includes hate content, including harassment and degradation towards an individual on the basis of religion, sex, sexual orientation, race, ethnicity, age or disability, or content intended to incite or promote hatred towards an individual.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

Anonymised, encrypted, or stand-alone data is not protected by IP rights. However, a compilation of works or data, whether in a readable format by computer program or by other media, is classified as protected works.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Certain aspects of a website may be protected by intellectual property rights. By linking to a third-party website, a content provider may be subject to intellectual property rights owned by the third-party website's developer or owner, or both. Though there are no specific regulations prohibiting providing a link to a third-party website, obtaining prior consent from the link owner is good practice.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

As a rule of thumb, a digital platform cannot use third-party content without the owner's consent if there is indication of IP rights infringement. In practice, using third-party content is not uncommon. In that case, any violation of the usage or the content material itself will be subject to the relevant civil or criminal sanctions.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

As at the time of writing, due to the absence of regulations relevant to the metaverse in Indonesia, specific metaverse-related provisions on the establishment and enforcement of IP have not been enforced. Current applicable laws and regulations on IP enforcement in Indonesia will be applicable.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Though not explicitly stated, certain provisions under Law No. 28 of 2014 on Copyrights (the Copyright Law) reflect a similar concept to that of exhaustion of rights or the first-sale doctrine. The Copyright Law stipulates that the economic right to conduct distribution of a creation does not apply to creations already sold or to which the ownership of the creation has been assigned to another party. Additionally, Indonesian regulations on IP generally recognise the exhaustion of rights over IP when the relevant IP has been assigned to another party. However, it should be noted that these regulations do not stipulate specific provisions on digital products placed on a metaverse or other platform in another territory, and their subsequent exhaustion of rights.

## Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Authorities in Indonesia are granted the power to conduct dawn raids in relation to the infringement of IP if a complaint is filed by the IP owner. The investigation can be carried out by law enforcement investigators and civil servant investigators appointed by the Indonesian Directorate General of Intellectual Property.

## Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Civil remedies to IP owners are granted through a civil lawsuit, which grants the IP owner compensation or cease of infringement by the IP infringer, or both. Additionally, a search order may be issued based on a complaint by the IP owner, and an investigation conducted by the authorities. Freezing injunctions are also stipulated under Indonesian IP regulations but can only be conducted when a lawsuit has already reached the trial phase.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Law No. 27 of 2022 on Personal Data Protection (the PDP Law) defines personal data as data regarding individuals who are identified or can be identified separately or in combination with other information, whether directly or indirectly through an electronic or non-electronic system. Furthermore, article 4 of the PDP Law separates personal data into two categories, namely, specific personal data and general personal data, as follows:

**Specific personal data**

- health data and information;
- biometric data;
- genetic data;
- criminal records;
- child data;
- personal financial data; and
- other data in accordance with provisions of laws and regulations.

**General personal data**

- full name;
- gender;
- citizenship;
- religion;
- marital status; and
- combined personal data to identify a person.

However, the PDP Law does not stipulate further provisions on the processing of personal data based on these separated categories, nor does it stipulate a difference in treatment when processing these categorised personal data types.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

The appointment of a data protection officer is only obligatory under the following conditions:

- the personal data is used for public services;
- the core activities of the data controller are of a nature, scope or purpose that requires regular and systematic monitoring of personal data on a large scale; and
- the core activities of the data controller consist of personal data processing on a large scale for specific personal data or personal data related to crimes.

Additionally, Minister of Manpower Decree No. 103 of 2023 on the Establishment of National Indonesian Occupational Competency Standards for the Information and Communication Category of Main Classifications of Programming Activities, Computer Consultations, and Related Activities within the Personal Data Protection Expertise Sector (MOM Decree 103/2023) establishes that data protection officers may obtain certification to ascertain their competency in the personal data protection sector.

Additional regulations and procedures for data protection officers are to be further regulated under a forthcoming implementing regulation.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The PDP Law implies the extraterritorial application of its provisions to every person, public agency and international organisation conducting legal acts stipulated therein. Its extraterritoriality applies if said acts create legal consequences within the Indonesian jurisdiction, or for the personal data of Indonesian citizens outside the Indonesian jurisdiction, or both. However, the PDP Law does not stipulate the obligation of said organisation or individual to appoint a representative in the Indonesian jurisdiction.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

As stipulated under the PDP Law, the bases for personal data processing are as follows:

- an explicit valid consent from the data subject for one or several specific purposes that have been submitted by the data controller to the data subject;
- fulfilment of agreement obligations, in the event that a data subject is a party to, or to fulfil the request of the data subject when entering into, an agreement;
- fulfilment of legal obligations of the data controller in accordance with provisions of laws and regulations;
- fulfilment of the protection of vital interests of the data subject;
- conducting of duties in the context of public interest or public services, or exercising the authority of the data controller based on laws and regulations; and
- fulfilment of other legitimate interests, while noting the purposes, needs, and balance of interests of the data controller and the rights of the data subject.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Pursuant to the PDP Law, the jurisdiction receiving the data transfer is required to, at the least, have personal data protection levels equal to the provisions on data protections reflected in the PDP Law, or even higher. If the receiving jurisdiction does not, the data controller is then obliged to ensure that there is adequate and binding personal data protection in the receiving jurisdiction.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

The PDP Law does not recognise or regulate the sale of personal data. However, the general practice in processing data primarily relies on the consent of the data subject. Therefore, if the sale or transfer of personal data is consented to by the data subject, such sale or transfer may be deemed lawful.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

The rights of personal data subjects under the PDP Law are as follows:

- the right to obtain information on the identity clarity, legal interest basis/grounds, purpose of requesting and using personal data, and accountability of parties that request personal data;
- the right to complete, update or correct errors or inaccuracies in their personal data in accordance with the purpose of the personal data processing;
- the right to access and obtain a copy of their processed personal data in accordance with provisions of the laws and regulations;
- the right to end processing, or delete or destroy personal data regarding themselves in accordance with provisions of laws and regulations;
- the right to withdraw consent given to a personal data controller for the processing of their personal data;
- the right to object to a decision-making action based solely on automated processing, including profiling, that has legal consequences or a significant impact on the personal data subject;
- the right to delay or limit the personal data processing proportionally with the purpose of the personal data processing;
- the right to sue and receive compensation for violations of the laws and regulations in respect of the processing of their personal data;

- the right to obtain and use personal data regarding themselves from a personal data controller in a form that is in accordance with the structure and format commonly used or readable by an electronic system; and
- the right to use and send personal data regarding themselves to other personal data controllers, provided the systems used can communicate with each other securely in accordance with the PDP Law.

Furthermore, a data subject reserves the right to file a lawsuit if there is an abuse of power by the government, or to dispute the disclosure of their personal data by an electronic system provider.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

The PDP Law neither stipulates provisions on the use of non-personal data, nor defines what is considered non-personal data.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Notarial deeds may not be executed through a digital signature; they require a physical/wet signature and must be kept in paper form. The documents that serve as the basis for the notary to issue the notarial deeds are also required to be wet signed. Examples of documents requiring a physical notarial deed include deeds of restatement of shareholders' resolutions and transfers/assignments of rights over land agreements.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Minister of Communications and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems requires a minimum retention period of five years for personal data held in electronic systems. Additionally, Law No. 8 of 1997 on Company Documents stipulates that certain company documents, such as financial documents, are required to have a minimum retention period of ten years after the end of the accounting year of the relevant financial document.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

Pursuant to National Cyber and Crypto Agency Regulation No. 8 of 2020 on System Security in the Organization of Electronic Systems, electronic system providers are obliged to obtain an Information Security Management System Certification (ISMS Certification). ISMS Certification is issued by the ISMS Certificating Body to organisers of electronic systems. One of the main requirements in obtaining the certification is the implementation of International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 (ISO/IEC 27001).

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Data breaches are regulated under Law No. 27 of 2022 on Personal Data Protection (the PDP Law) and Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions (GR 71/2019). Failure to carry out personal data protection, such as a data breach event, requires the data controller to notify the data subject and the personal data protection agency (PDPA) in written form no later than 72 hours after the occurrence of such data breach. However, as the PDPA has not yet been established, the obligation on the notification of data breach occurrences is still subject to the provisions of GR 71/2019.

GR 71/2019 stipulates that in the event of a data breach, the electronic system provider is obligated to notify the data subject in written form. Furthermore, in the event of third-party action resulting in adverse effect to the electronic system of a platform, the platform must submit a report to the police and the Ministry of Communications and Informatics.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

The PDP Law stipulates that the rights of data subjects under the PDP Law are exempted for the interests of:

- national defence and security;
- law enforcement process;
- public interest in the context of state administration;

- supervision of the financial services, monetary, and payment system sectors, and financial system stability carried out in the context of state administration; and
- statistics and scientific research.

Pursuant to Minister of Communications and Informatics Regulation No. 5 of 2020 on Electronic Systems Providers in the Private Sector (as amended by Minister of Communications and Informatics Regulation No. 10 of 2021), the government – in this case, ministries, state agencies, and law enforcement officers – may request access to the electronic system or electronic data of a private electronic system provider. Government authorities may request access for the purpose of conducting a supervisory function or for law enforcement, subject to the relevant laws and regulations.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

It is not permissible to operate an online betting or gaming business in Indonesia. Pursuant to the applicable laws and regulations, betting and gambling are strictly prohibited in Indonesia.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

It is not permissible to advertise or provide access to an online betting or gaming business located outside the Indonesian jurisdiction. Any display or transmission of gambling through online means is a direct violation of Law No. 11 of 2008 on Electronic Information and Transactions (as amended by Law No. 19 of 2016).

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

The enactment of Law No. 6 of 2023 on Enactment ofGovernment Regulation in Lieu of Law No. 2 of 2022 on Job Creation into Law (the Job Creation Law) removes the previously established limitation that core business activities cannot be outsourced. However, caution needs to be exercised when engaging an outsourcing service provider to ensure that it possesses the requisite licences to provide such services.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

The Financial Services Authority prohibits co-funding services organisers to outsource the functions of assessment of funding feasibility and information technology.

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

Subject to Law No. 13 of 2003 on Manpower (as amended by the Job Creation Law), outsourcing provider companies are obliged to provide terms of transfer of protection of rights to workers in the event that there is a change in the outsourcing company and provided the object of the employment or work still exists.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

If employees are terminated and replaced through outsourcing for services previously conducted by the employees, then they are entitled to compensation in the form of severance pay or tenure awards and compensation in respect of rights that are supposed to be received. These compensations are applicable to both fixed-term employees and permanent employees.

Upon the enactment of the Job Creation Law and its implementing regulations, compensation money must be given to the fixed-term employees at the end of their contract period.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions stipulates that an 'electronic agent' is defined as an electronic system device created for the purposes of conducting actions automatically on certain electronic information conducted by a person (either individual person or legal entity). Therefore, artificial intelligence (AI) would theoretically be included in the regulation's definition of an electronic agent. Specific regulations regarding the use or development of AI are yet to be issued.

**Read this article on Lexology**

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions stipulates that an 'electronic agent' is defined as an electronic system device created for the purposes of conducting actions automatically on certain electronic information conducted by a person (either individual person or legal entity). Therefore, artificial intelligence (AI) would theoretically be included in the regulation's definition of an electronic agent. Specific regulations regarding the use or development of AI are yet to be issued.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

No specific rules or guidance regarding ethical AI and machine learning have been issued in Indonesia.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Online transactions are subject to tax mechanisms and provisions in accordance with applicable laws and regulations. Pursuant to Law No. 2 of 2020 on State Financial Policy and Financial System Stability for Handling the Corona Virus Disease 2019 (Covid-19) Pandemic, business actors conducting trade through electronic systems are subject to value-added tax obligations.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Law No. 7 of 1983 on Income Tax (as most recently amended by Law No. 6 of 2023 on Enactment of Government Regulation in Lieu of Law No. 2 of 2022 on Job Creation into Law) (the Income Tax Law) stipulates that a permanent establishment, used by an individual located outside of Indonesia or an entity not established and domiciled in Indonesia, is subject

to local taxations. Computers, electronic agents, or automated equipment that are owned, leased, or used by electronic transaction organisers to conduct business activities through the internet are categorised as permanent establishments under the Income Tax Law.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

There are no specific regulations on the formatting and use of e-invoicing in Indonesia.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

Currently there no specialised courts or other venues for the digital/online disputes.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

Online/digital disputes can be settled through arbitration, although uncommon. Disputes in the financial services sector are facilitated by the Financial Services Authority, while disputes relating to consumer protection may be conducted through the consumer dispute settlement agency.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

There are plans to amend Law No. 11 of 2008 on Electronic Information and Transactions (as amended by Law No. 19 of 2016). The amendment will focus on the implementation of electronic transaction systems and cybercrime provisions.

Additionally, the Artificial Intelligence National Strategy 2020–2045 elaborates on certain key issues relevant to the implementation and regulation of artificial intelligence in

Indonesia. The document also states the priority sectors of artificial intelligence, namely the health, bureaucracy reformation, research and education, food security, mobility and smart city sectors.

Blockchain technology is also receiving further attention from the government, with the aim of implementing land deed certificates as tokens. In the music industry, more and more artists are launching their music as non-fungible tokens with unique and personal utilisations.

Naufal Fileindi naufal.fileindi@lawghp.com
Eliza Anggasari eliza.anggasari@lawghp.com
Benedict Giankana benedict.giankana@lawghp.com

World Trade Center 3 Level 27, Jl Jend Sudirman
Kav 29-31, Jakarta 12920, Indonesia
Tel: +62 21 5011 0199
www.lawghp.com

# Israel

Eyal Roy Sage and Lior Talmud

AYR - Amar Reiter Jeanne Shochatovitch & Co

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

A 2013 government decision launched a digitalisation initiative, which resulted in a national ICT policy for the public sector. Among other things, the government is embracing cloud technologies, making data accessible, and enhancing digital services to citizens and companies. Changes to the e-signature legislation eased online commerce. Online content remains mostly unregulated, in stark contrast with broadcast media.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

Consumer Protection Law; Protection of Privacy Law; Communications Law (Telecommunications and Broadcasts); Standard Contracts Law; Electronic Signature Law; and their respective regulations and guidelines.

### Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The Ministry of Communications, the Privacy Protection Authority and the Consumer Protection and Fair-Trade Authority.

No specific regulator handles artificial intelligence issues yet. However, the Ministry of Innovation, Science, and Technology has drafted principles on this subject. Also, some sectoral regulators, like the Ministry of Health, have addressed the issue.

### Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Supreme Court case law has significantly limited prior jurisprudence that allowed foreign digital businesses to determine the law of the contract in standard terms contracts unless it was shown that the choice of law was depriving consumers' rights. A choice of foreign venue in standard terms contracts was already generally considered to be depriving consumers of their rights pursuant to the Standard Contracts Law 1982, as were provisions forcing arbitration, which were designed to prevent consumers from pursuing a class action.

Current Supreme Law case law guides that the greater the intention of the non-resident digital business to conduct business in Israel (for example, by advertising locally, accepting local currency, offering a Hebrew language website), the more likely it is that courts would apply local laws and insist local courts have jurisdiction, irrespective of any contractual terms to the contrary in a standard terms contract.

Where the contract is not a standard terms contract, the parties are free to determine the choice of law and venue, and agree on arbitration if they so wish.

### Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There are no special requirements regarding the establishment of a digital business and sale of digital content and services. The provision of certain telecommunications services requires registration or licensing at the Ministry of Communications, which requires foreign providers to register as a foreign company (or set up a local entity).

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Yes. Contracts may be formed and concluded digitally.

There are no special requirements for digital contracts. A contract is concluded when an offer is accepted, and acceptance can be by conduct.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Yes, the Standard Contracts Law voids contract terms that are unduly disadvantageous. There is a rebuttable presumption that provisions in a standard terms contract that unilaterally impose a venue, choice of law and arbitration and its terms are unconscionable.

The Standard Contracts Law applies to business-to-consumer and business-to-business contracts, but the bargaining power of the parties is taken into account. Small businesses

dealing with large online businesses are likely to be entitled to protection pursuant to the Standard Contracts Law.

Standard contract terms requiring disputes to be arbitrated designed to block consumers from pursuing class actions are void.

## Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

The law recognises electronic signatures, which cannot be denied admissibility merely for being electronic.

The Electronic Signature Law defines several types of e-signatures, which have different legal force:

- simple electronic signature – defined as electronic data or an electronic sign that is attached to or associated with an electronic message;
- secure electronic signature – defined as an electronic signature that is:
    - unique to the owner of the signing device;
    - enables apparent identification of the owner of the signing device;
    - created using a signing device that is under the sole control of its owner and enables detection of any change to the electronic message subsequent to signing; and
- certified electronic signature – defined as a secure electronic signature for which a certification authority has issued an electronic certificate.

A party who sets up a system that accepts simple electronic signatures (for example, an online business) and wishes to rely on another party's simple electronic signature bears the burden of proof that the other party signed.

An electronic message signed with a secure electronic signature is admissible as such in any legal proceedings and constitutes prima facie evidence that the message was not changed after it was signed, and that it was signed with the secure device identified in the certificate, if any.

A message signed with a certified electronic signature is also prima facie evidence that it was signed by the owner of the device. While any type of digital information can be signed with a simple electronic signature, when the law requires a signature, the requirement is often interpreted as meaning a certified electronic signature.

Certification authorities are licensed and supervised.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

No.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The Supervision of Financial Services (Regulated Financial Services) Law 2016 establishes a mandatory licensing requirement for financial service providers. Pursuant to the Regulation of Investment Advice, Investment Marketing and Investment Portfolio Management Law 1995, investment marketing, investment advice or portfolio management services require a licence.

Different regulators exist for various financial sectors, including the Capital Market, Insurance, and Savings Authority, the Supervisor of Banks, and the Israel Securities Authorities. Each regulator issues rules on advertising and selling financial services.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

The Supervision of Financial Services (Regulated Financial Services) Law 2016 prohibits the offering of regulated financial services without first holding a regulatory licence from the Israeli Capital Markets Authority. Section 11A of the said law defines 'financial asset' to include a cryptocurrency, and also any item upon which value can be stored (eg, a wallet). The definition of 'financial service' in section 11A includes the management or custody of a financial asset. In addition, based on certain criteria, a digital currency may be defined as a 'security' under the Securities Law 1968, and under this law, the offer and sale in Israel to the public of an instrument that qualifies as a security is subject to significant regulatory supervision, and in particular, the requirement to publish a prospectus, under the Securities Law.

There are no regulatory restrictions on the mere possession and use of digital currencies, but banks in Israel are reluctant to allow their clients to deposit to their bank accounts fiat money that originates from the sale of digital currencies. This is due to the zero-risk appetite policy applied by the banks in terms of AML compliance.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

The Supervision of Financial Services (Regulated Financial Services) Law 2016 prohibits the offering of regulated financial services without a licence from the Israeli Capital Markets Authority. Section 11A of the said law defines 'financial asset' to include a cryptocurrency, and also any item upon which value can be stored (eg, a wallet). The definition of 'financial service' in section 11A includes the management or custody of a financial asset. In addition, based on certain criteria, a digital currency may be defined as a 'security' under the Securities Law 1968, and under this law, the offer and sale in Israel to the public of an instrument that qualifies as a security is subject to significant regulatory supervision, and in particular, the requirement to publish a prospectus, under the Securities Law.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

The Payment Services Law 2019 regulates electronic payment systems. It aims to guarantee transparency of terms, certainty of execution time and similar protections for payment services users. This statute is largely based on the EU's Payment Services Directive.

Third-party access to digital information in bank accounts is regulated by the Financial Information Service Law 2021. This law governs the collection, transfer or use of financial information by various financial entities and the relationship between financial service providers (credit clearinghouses, investment portfolio managers, fintech companies, etc) and the sources of information, such as banks and credit card issuers.

Entities licensed by the Israel Securities Authority to provide financial information services may receive financial information about their clients (with their consent) from different information sources and supply additional information about the client to such sources.

## Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

No.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

Registration of an Israeli country-specific domain (.il) is made by accredited registrars of the Israeli Internet Association. It is possible to register a country-specific domain name without being resident in the country.

Registering domain names designed to hinder access to a competitor's site can amount to an unfair business practice.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Although domain names are not directly protected as trademarks, it is possible to register trademarks that consist of domain names. Ownership of a trademark or copyright can assist in challenging a competitive use or registration of a similar domain name or URL, as the use or registration of a similar domain can infringe a trademark and also give rise to claims of unfair trade practices such as passing off and hindering access to another business.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

There are laws against unsolicited commercial emails. Although advertising tobacco and related products is permitted in the printed press (subject to many restrictions), it is prohibited online. Other restrictions on advertising (such as on gambling) apply equally on and offline.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

The Protection of Privacy Law (sections 17C-17I); and 2/2017 Databases Registrar Guidelines.

Personal data may be used for targeted marketing if the data was lawfully collected by the advertiser, that is, the data subject gave his or her express or implied informed consent.

Transferring personal information for targeted advertising by third parties (eg, direct mail services) requires specific opt-in consent, and is generally seen as recommended if the linkage between the purpose for which the personal information was originally given and the advertising in question is weak.

Targeted advertising based on profiling must be identified as such and must identify the name of the advertiser. Data subjects have a right to have their information deleted from databases used for direct marketing. If a database is used for both operational and direct marketing purposes, then only the information not used for operational purposes needs to be deleted.

No law specifically addresses the use of cookies and similar technology as such, but to the extent the information is personal information, privacy laws apply.

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

There are no specific rules on online advertising. Section 2 of the Consumer Protection Law prohibits any act or omission likely to mislead consumers of any material aspect of a transaction, including the quality, nature, quantity and type of the service, maintenance service, conditions of warranty and more. This rule applies to advertising.

The Consumer Protection Regulations (advertising and marketing methods targeted at minors) list special provisions concerning advertising to minors, and also restrict using information collected from minors.

The rules of the Second Authority for Television and Radio, which apply to advertising on commercial broadcast TV and radio explicitly require substantiation for health-related advertising, although the rules make broadcasters liable for negligently allowing false or misleading advertising, so substation is often required.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

Advertising restrictions generally apply both offline and online, although the advertising of tobacco and smoking paraphernalia (including e-cigarettes) is completely prohibited online, but permitted with many restrictions in the printed press.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

Unsolicited emails, SMS, faxes and automated calls require opt-in consent, which can be withdrawn at any time. Opt-out consent applies in the case of prior contact, provided that the addressee was informed of the use of his or her contact details for advertising, that he or she was given an opportunity to refuse and did not, and that the advertisement in question relates to a similar product or services. All such advertising must be clearly marked, and opting out or withdrawing consent should be simple. In October 2022, a do-not-call database was established, as part of an amendment to the Consumer Protection Law, which prohibits marketing calls to numbers registered in the registry. Distance marketing by any means is subject to the disclosure and cooling-off provisions of the Consumer Protection Law.

Some lower courts have found the prohibition on unsolicited SMS to apply to modern messaging networks such as WhatsApp.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Theoretically, liability for contributory copyright infringement might arise against a party who merely hosts third-party infringing content if it has actual knowledge of the infringement and has materially contributed to it. Generally, however, right holders should seek a court order to remove infringing content or to block access to it pursuant to a 2019 amendment to the copyright law. Such an order can be given against ISPs and hosting providers.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

The general tort law principles that govern negligent misrepresentations apply to online content, namely duty of care, violation of the duty and resulting damage, and courts take a cautious approach to imposing a duty of care on the providers of content. A disclaimer of liability is customary and advisable in any case.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

An online content provider can shut down a website containing defamatory material without court authorisation if there is sufficient evidence for the defamatory nature of the material. This has not been laid down in statute but would seem to be a reasonable application of the general legal principles governing this question. ISPs, however, are committed to neutrality and would generally refrain from blocking access to a website without a court order.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

Some databases are protected by IP rights (under 'literary work'). According to section 4(b)of the Israeli Copyright Act 2007, 'originality' in the selection and arrangement of the items or data is required. Therefore, a database that collects data automatically may not be protected by IP rights. Data representing mere facts is not protected.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Yes.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Not if the content in question is protected by IP laws (specifically, copyright) or consists of personal information (and subject to purpose limitation), or the scraping circumvents technical measures (which may amount to an offence pursuant to the Computer Law). Liability under the Unjust Enrichment Law might also arise.

### Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

No.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

The concept of exhaustion is recognised, and rights can be exhausted only upon the legal first sale within the territory where rights were granted (local exhaustion). In the case of digital products, the doctrine would apply to the physical copy. Restrictions on virtual goods or online-only services can, however, be enforced contractually, for example by requiring geo-fencing.

## Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Yes, in the case of IP infringements that are also criminal offences.

## Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

The normal civil law remedies are available, which include injunctions, the appointment of receivers with the right to search and seize property, and disposition of infringing goods without compensation, recall from the channels of commerce, etc. Specifically for copyright infringements, remedies also include statutory damages.

A 2019 amendment to the Israeli Copyright Act, 2007 empowers courts to order third parties such as ISPs to provide the court with identifying details (such as an IP address) of alleged infringers who anonymously made available to the public infringing content. Such information can be used to sue anonymous infringers. The court may also appoint experts to assist in identifying the infringer.

The 2019 amendment also empowered courts to order ISPs and hosting providers to block access to infringing content or to sites with significant infringing content.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

'Personal data' ('information', as it is defined in the Protection of Privacy Law) means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

Although the statutory provisions specify only a limited number of attributes as personal data, the regulator and courts have expanded the definition significantly. The regulator's current approach, as reflected in the amendment to the Protection of Privacy Law, includes any data relating to an identified or an identifiable person, directly or indirectly, by reasonable means, including biometric identifier, ID number, telephone numbers, names of friends, email suffix and more.

'Sensitive information' is defined in the Protection of Privacy Law as: 'information on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person'.

The Privacy Protection Regulations (Privacy Protection Regulations (Instructions for Data that was transferred to Israel from the European Economic Area) 2023 add ethnic origin and trade union membership to the list of sensitive information. Databases that contain 'sensitive data' are subject to stricter registration requirements and a higher information security standard.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

A database should be registered if it meets certain low registration thresholds, such as data on more than 10,000 data subjects or there is sensitive data, irrespective of the number of data subjects.

There is no legal obligation under Israeli law to appoint a data protection officer (DPO). However, controllers must appoint a database manager, who is responsible for ensuring that the database is used for the purposes for which it was established, for taking security measures, and generally for compliance with the law. Moreover, the Protection of Privacy Authority recommends appointing a DPO to take on responsibilities not with the database manager. The DPO may be the database manager or a different function.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The Protection of Privacy Law 1980 does not contain explicit extraterritorial provisions, although powers would extend to local branches and subsidiaries. However, in a pending court case it is alleged that foreign companies must register their databases in Israel, thereby making them subject to the Protection of Privacy Law.

There is no requirement to appoint a local representative unless the database is registered in Israel.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

Strictly speaking, Israeli law acknowledges two legal bases for data processing – consent, and legal empowerment.

However, consent in Israeli data protection law is quite a flexible concept. While it needs to be informed, it can be implied. Processing for direct mailing services (ie, profiled personal data used for marketing by third parties) requires opt-in consent. There is requirement that consent be 'freely given', unless forcing it is depriving consumers under the Standard Terms Contract Law or is excessive in the context of employment. Some statutes also require opt-in consent, for example for the sharing of financial information as part of open banking.

In addition to the legal bases, there are defences that may apply to such cases where personal data is used where there is a 'legal, moral, social or professional obligation', 'legitimate personal interest' or 'public interest' to do so.

The Privacy Protection (Transfer of Data to Databases Abroad) Regulations determine that personal data can be transferred outside of Israel either to adequate jurisdictions, or pursuant to several export routes. Generally, jurisdictions complying with the GDPR are considered as affording an adequate level of protection under Israeli law. There are other possible export routes such as with the data subject's (express or implied) consent, data transfer to a signatory country of Treaty 108 or when the data importer was bound by an agreement to apply the same requirements as required under the Israeli law to the personal data that is transferred. Exports to jurisdictions deemed adequate by the EU are also allowed, subject to the same terms.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

The Privacy Protection (Transfer of Data to Databases Abroad) Regulations determine that personal data can be transferred outside of Israel either to adequate jurisdictions, or pursuant to several export routes. Generally, jurisdictions complying with the GDPR are considered as affording an adequate level of protection under Israeli law. There are other possible export routes such as with the data subject's (express or implied) consent, data transfer to a signatory country of Treaty 108 or when the data importer was bound by an agreement to apply the same requirements as required under the Israeli law to the personal data that is transferred. Exports to jurisdictions deemed adequate by the EU are also allowed, subject to the same terms.

Data importers abroad must contractually undertake to implement adequate measures to ensure the privacy of the data subjects and to not transfer the data to third parties (commonly interpreted as without the data exporter authorisation).

The Privacy Protection Regulations (Instructions for Data Transferred to Israel from the European Economic Area) 2023 determine four obligations on Israeli database owners with regard to personal data that was transferred from the EEA (excluding data that a data subject provided directly about himself): deletion of data after the receipt of a written deletion request from the data subject; data minimisation; data accuracy; and disclosure obligation.

Government guidelines requires government agencies to maintain certain types of sensitive data and operations to be kept in-country, but there are exceptions.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

Transferring personal data to third parties for their own purposes requires data subjects' consent. If the purpose of the transfer (sale) is direct marketing (eg, data brokerage), explicit opt-in consent is required. Transferring of personal data to third parties acting as processors (or that have an obvious need for the data, such as for fulfilment or payment) can generally be done with implied consent.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Data subjects have a right to access and rectify personal information concerning them. Data subjects have a to seek erasure of inaccurate data if the controller refuses to correct the

data, and a right to have data used only for direct (profiled) marketing to be deleted. These rights are not limited to citizens, but also apply to foreign data subjects' personal data that is being collected or processed in Israel or by or for an Israeli controller.

With respect to data that was transferred to Israel from the EEA, individuals also have a right to request data erasure, if the data is processed unlawfully, or if it is no longer necessary for the original purposes. Exceptions such as anonymisation and justifications like fraud prevention, legal proceedings, debt collection, and scientific and statistical research apply.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

No.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Yes, original documents scanned electronically and used in income tax accounting should be kept for three years from the date on which any report based on them was submitted.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Accounting records should generally be kept for seven years.

According to Bar Association Rules (Retention of Archival Material) it is required to keep legal documents for at least five years from the date of completion of the treatment of the matter.

There are banking and insurance sectorial requirements regarding a period for which documents or other record types should be kept.

Other laws also determine minimum (and sometimes, maximum) period governmental authorities should keep documents.

The Protection of Privacy Regulations (Information Security) contains two provisions on data retention: databases should not contain excess personal information (that it, personal information no longer needed for the purpose for which it was collected); and security logs should be kept for 24 months.

The Privacy Protection Regulations (Instructions for Data Transferred to Israel from the European Economic Area) 2023 impose enhanced data minimisation obligations to personal data that was transferred from the EEA, buy requiring the implementation of organisational, technological or other mechanisms to ensure that the database does not contain data that is no longer required for the purpose for which it was collected or held, or for another legal purpose. Data minimisation will not be required in cases where measures to prevent the reasonable identification of a data subject were taken.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

The Protection of Privacy Regulations (Information Security) list the requirements for security of databases. Databases that contain sensitive data are subject to higher security measures. Sectoral requirements apply to regulated industries, including the financial sector, transportation, telecommunications, critical infrastructure, and other key industries.

The Protection of Privacy Regulations (Information Security) require organisations who process personal information to take specific security measures. Sectoral requirements apply to regulated industries, including the financial sector, transportation, telecommunications, critical infrastructure, and other key industries. Certain organisations are subject to specific, detailed, and confidential instructions by the Internal Security Service or the Israel National Cyber Directorate.

ISO 27001 and PCI-DSS certifications are common.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Yes. The Protection of Privacy Regulations (Information Security), require both controllers and processors to notify the Protection of Privacy Authority immediately of any 'serious security incident'. There is no automatic requirement to inform affected individuals (although it may well be advisable to do so for damage mitigation purposes), but the Registrar of Databases can, in consultation with the head of the National Cyber Defence Authority, require that data subjects be notified.

The above applies to databases that are subject to the high and medium security levels in the regulation.

In addition to the general law, there are specific obligations of sectoral regulators that require the supervised body to notify the incident (eg, the Bank of Israel, Capital Market Authority, Insurance and Savings Authority, and Israel Securities Authority).

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Licensed or registered telecommunications operators must give certain agencies access to communications data (not content) pursuant to the Criminal Procedures (Enforcement Powers – Data Communications) Law 2007. A court order is required, except in exigent circumstances in relation to serious crimes (punishable by more than three years imprisonment) or risk to life, in which case a subpoena by certain police officers suffices. Subscriber information is generally available without a court order.

Under the Criminal Procedures Ordinance (Arrest and Search) (New Version) 1969, which applies where crimes are investigated, courts may issue orders against anyone to produce documents and information, including stored content (but not live communications).

The General Security Service Law 2002 empowers the service to obtain communications data (not content) from licensed telecommunications operators.

The Communications Law (Telecommunications and Broadcasting) 1982 compels licensed or registered telecommunications operators to cooperate with certain enforcement and security agencies, who may then access information autonomously, within their legal mandates. This statute does not itself compel the disclosure of information, therefore, no warrant or subpoena is required.

Finally, courts can issue intercept orders in cases involving serious crimes, and ministers can permit short-term intercepts in cases involving national security.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

No. Betting in sports is regulated in a specific statute that grants a monopoly to a public council. Public offerings of prize-bearing games of chance (no matter how trivial the prize) require a licence from the Ministry of Finance, but only the national lottery has received such a licence. There are some allowances for marketing campaigns involving raffles, and some exemptions for charitable and similar activities.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

No. Advertising or providing access to online betting or gaming that would be illegal had it taken place in Israel is prohibited, even if such activity takes place where it is legal.

To bolster the prohibition, the Powers for the Prevention of Crimes Committed Through an Internet Site Law 2017 empowers district courts to issue orders to ISPs to restrict access fully or partially to any internet site based on a determination that the restriction is necessary to prevent continued commission of certain offences, including prohibited games.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Outsourcing of personal data processing is subject to the security and data protection measures required by Regulation 15 of the Protection of Privacy Regulations (Information Security), which include a prior assessment and the conclusion of a contract that must contain certain provisions designed to ensure security and privacy. Similar provisions apply in the financial and other sectors.

Certain types of outsourced work, especially for services such as cleaning, are subject to strict employee protection laws. Employees assigned by temp agencies (other than in the IT sector) to the same workplace for nine months have a right to become employed by the workplace to which they are assigned. This right does not apply to companies providing services (such as cleaning) rather than employee placement.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

Outsourcing in the financial sector is subject to specific rules, but other than functions such as duties of the board of directors and senior management, particularly in determining strategies and policies, determining risk appetite, and control and supervision of risk management processes, and decisions such as on the opening or closing customer accounts, outsourcing is allowed.

Outsourcing in regulated industries will generally require a risk assessment and written contracts covering key aspects of the outsourced service.

## Contractual terms

### 49 Does the law require any particular terms to be included in outsourcing contracts?

Yes. Regulation 15 of the Protection of Privacy Regulations (Information Security) details the provisions that must be included in a contract with a provider. Outsourcing contracts should regulate:

- the data the external service provider may process and the permitted purposes of its use;
- the systems that the external service provider may access;
- the type of processing or activities the external service provider may perform;
- the agreement duration, the manner of returning the data to its controller at the end of the agreement, its destruction at the disposal of the external service provider and of reporting accordingly to the database controller;
- the manner in which data security obligations that apply to the processor of the database according to the regulations are implemented, and additional data security instructions set by the database controller, if any;
- the obligation of the external service provider to have its authorised users undertake to protect the information confidentiality, use the data only according to the agreement and implement the data security measures prescribed in the agreement;
- where a database controller permits the external service provider to provide the service through another entity, the duty of the former to include in the agreement with the other entity all the matters detailed in the regulation; and
- the obligation of the external service provider to report at least annually the manner in which it abides by the obligations of the regulations and the agreement, and any security incidents.

## Employee rights

### 50 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

A hearing prior to dismissal must be offered to all employees, in addition to compensation for termination (subject to a minimum term of employment). Unionised employees may have additional protection agreed between the employer and the union. Employees that are offered to keep their position and the same (or better) employment terms with the outsource provider would generally not be entitled to severance pay. However, in most cases employees are entitled to a severance package even if they quit.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

The Protection of Privacy Authority guidance is that data subjects be informed of automatic decision making, especially based on artificial intelligence. The Ministry of Innovation, Science, and Technology has drafted principles on this subject, including a recommendation to promote transparency and provide relevant information to individuals who come into contact with artificial intelligence (AI) or are impacted by its use.

The Protection of Privacy Authority also recommends (although this is not a legal requirement as such) to conduct a data protection impact assessment prior to engaging in processing that involves AI, machine learning, automated decision making or profiling. The Ministry of Innovation, Science, and Technology has drafted principles containing a recommendation to document the design and development process of AI, among other measures, to effectively manage safety risks.

Sectoral regulators in the banking and insurance industries have started surveys into the uses of AI in the industries they supervise.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

There are no rules. However, in December 2022 the Ministry of Justice published an opinion in which the Ministry concluded that in most circumstances the use of copyrighted materials for machine learning is permitted under the fair use doctrine or under the doctrine that permits incidental use of copyrighted materials. Some uses might also be permitted as a transient use.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

There are no rules, but according to principles published by the Ministry of Innovation, Science, and Technology, several ethics principles should be taken in consideration:

- respect for basic rights and public interest;

Read this article on Lexology

- fairness (equality and non-discrimination);
- transparency and explainability;
- reliability, durability, security and safety; and
- accountability.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

For tax purposes, a digital asset is considered as any other asset, and the gain from its sale is subject to ordinary income or capital gain tax, based on the person making the sale (for example, if the person making the sale is a day trader of the digital asset or a long-term investor). Online services are no different from offline services. In both cases income derived from the provision of services in connection with digital asset is taxable income under the general rules of taxation. However, the government approach, in the last few years, is to approve a complete reform in the matter, and to impose tax on such activities. Such reform, however, has yet to be approved.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

The placing of servers in Israel can constitute a permanent establishment, which would make income attributed to the permanent establishment taxable in Israel. However, the mere location of servers as such is not likely to be enough to create a permanent establishment, and the answer would depend on additional factors.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

Israeli businesses are required to issue 'tax invoices', which are a specific type of invoice often issued when payment is received along with a receipt. Tax invoices can be digital. They must contain the same information as paper tax invoices but must be electronically signed with a secure or certified e-signature. There is no specific requirement to provide copies of e-invoices to tax authorities; rather, the same tax inspection rules apply to both paper and electronic tax invoices.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

No.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

There are no formal ADR methods for online or digital disputes in Israel. ADR is common where the parties think specialist knowledge is needed and where discretion and speed are sought.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The government is aiming to modernise Israel's antiquated data protection rules, both by introducing significant changes to statutes and by issuing constant guidance.

Parliament is expected to resume hearings on Amendment 14 of the Privacy Protection Law. If adopted, the Amendment would, among other things, expand the enforcement powers of the Privacy Protection Authority, replace key definitions in the law in line with the EU General Data Protection Regulation, and scale back the obligation to register databases.

Israel is currently recognised as providing an adequate level of data protection, thereby allowing free data flows from the EU to Israel. As a part of the re-evaluation process carried out by the European Union Commission regarding the renewal of the adequacy status, the Minister of Justice has promulgated the Privacy Protection Regulations (Provisions Concerning Information Transferred to Israel from the European Economic Area) 2023. The Regulations impose four key obligations on Israeli controllers regarding personal data that was transferred from the EEA (other than data provided directly by the data subject): the right to request erasure; data minimisation; data accuracy; and enhanced transparency obligations.


Amar Reiter Jeanne Shochatovitch & Co

Eyal Roy Sage eyals@ayr.co.il
Lior Talmud liort@ayr.co.il

Champion Tower 39-40 Floor, 30 Sheshet Hayamin Road, Bnei Brak 5120261, Israel
Tel: +972 3 601 9601
www.ayr.co.il

# Italy

Paolo Balboni, Luca Bolognini, Raffaella Cesareo, Luciana Di Vito, Camilla Serraiotto and Claudio Partesotti

ICT Legal Consulting

RETURN TO CONTENTS

## Summary

**Read this article on Lexology**

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The government has adopted a cognisant approach to internet issues. The complexity and potential of the internet and the challenges it poses must be balanced with the rights and freedom of individuals. With this in mind, Italy's digital transformation strategy highlights the legislature's comprehensive approach from the private sector to public administration. In this context, the government is aware of the need to:

- strengthen the digital culture of citizens and enterprises; and
- improve the online provision of goods and services, which is considered a priority.

Therefore, to implement the beneficial effects of Industry 4.0, enterprises must be provided with digital knowledge-based technology to foster competitiveness. Moreover, the National Recovery and Resilience Plan (PNRR) adopted by Italy is dedicated to the digital transition. The Strategy for Digital Italy develops along two axes: the digitisation of the PA and ultra-fast networks.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

There are two main e-commerce models in Italy: business to business (B2B) and business to consumer (B2C), while new models such as consumer to business and consumer to consumer are developing. The legislature has adopted different legal instruments to regulate e-commerce in a comprehensive manner and has provided for the application of special legislation, including:

- Legislative Decree 70/2003, which implements EU Directive 31/2000/EC with the aim of developing an e-commerce framework;
- Legislative Decree 206/2005 (the Consumer Code) on consumer rights. The Consumer Code has recently undergone important legislative changes, aimed at transposing European standards for greater consumer protection, including some aspects of the sale of goods and the supply of digital content and digital services, respectively contained in EU Directive 2019/771 and EU Directive 2019/770, as further indicated below;
- Legislative Decree 26/2023, implementing EU Directive 2161/2019, which amends the Consumer Code and increases consumer protection;
- Legislative Decree 28/2023, implementing EU Directive 2020/1828, on actions for collective interests.
- EU Directive 2161/2019, implemented through article 4 of the European Delegation Bill, approved by the Italian Senate (AS 2481) on 30 June 2022;
- Legislative Decree 170 of 4 November 2021, implementing EU Directive 2019/771, which amends the Consumer Code as of 1 January 2022; and

- Legislative Decree 173/2021, implementing EU Directive 2019/770, whose provisions (set out in the new Chapter I-bis of Title II of Part IV of the Consumer Code) apply to the supply of digital content or digital services from 1 January 2022, with the exception of the right of redress and the rules on the modification of the digital content or service, which only apply to contracts concluded from that date.

Further, the following laws apply:

- the regulation of contracts set out in the Civil Code and the Digital Administration Code regarding the online signature of contracts;
- the Personal Data Protection Code;
- EU Regulation 2016/679 (General Data Protection Regulation);
- Legislative Decree 45/2012 on electronic currency;
- the national provisions of online payment services and intellectual property; and
- sector-specific legislation (codes of conduct, medical products).

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The main authorities in this regard are:

- the Competition and Market Authority;
- the Communications Regulatory Authority;
- the Data Protection Authority; and
- the Agency for Digital Italy.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

For international electronic contracts in the European Union, the nature of the parties to a contract determines the application of specific provisions. The general principle for B2B contracts is that parties have a free choice over the applicable jurisdiction of a contract. As a general rule under the recast EU Brussels Regulation (1215/2012), where the parties have no choice regarding the jurisdiction of a contract, the defendant's jurisdiction will apply. Where a defendant is not domiciled in an EU member state, the competent jurisdiction is determined by applicable national law (eg, Law 128/1995 in an Italian context).

If the defendant is a consumer, the applicable jurisdiction is the courts of the EU member state in which the consumer is domiciled, unless otherwise agreed, which must follow the EU Brussels Regulation if the parties reside in different countries, or the Consumer Code if they reside in Italy.

In the field of telecommunications, the United Sections of the Court of Cassation, in judgments No. 8240 and No. 8241 of 28 April 2020, states that the failure to carry out the compulsory attempt at conciliation renders the application inadmissible.

There is currently no specific jurisdictional legislation covering the metaverse. However, jurists are reflecting on the extent to which the rules in force in the real world can be applied to the metaverse, and whether an ad hoc codification should be considered instead. It should be noted that the development of the metaverse is taking place when new EU regulations have been adopted in the digital sphere. Certainly, the metaverse poses problems concerning the choice of applicable law, if one considers that the digital space will reside on privately owned hardware, software and telecommunications systems, often not clearly defined and in different countries. This poses problems in the application of the applicable law.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

The regulatory and procedural requirements to establish a digital business in Italy are almost the same as those to establish 'regular' businesses. Operators can choose from different types of business, the most common being limited liability companies and partnerships. There is also a new simplified limited liability company, which was introduced in 2012.

Incorporation must take place before a public notary. Other general requirements to set up businesses include:

- registration with the Register of Companies;
- obtaining a value added tax number;
- obtaining an Economic and Administrative Index number (indicating the category of the activity carried out); and
- certification of the start of the activities and other incumbencies.

Additional requirements for digital businesses include:

- making some corporate and non-corporate information easily accessible (article 7 of Legislative Decree 70/2003); other information instead – according to the rules of the Civil Code – must be included in deeds and correspondence (VAT, registered office, paid-in share capital);
- prior authorisation, if applicable;
- publication of the company's terms and conditions; and
- providing details of modalities of payments and other kinds of information to provide transparency regarding the services or products offered.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

The law allows contracts to be signed electronically as part of the 'distance contract' category. The general principles provided by the Civil Code apply to e-contracts. A contract is therefore concluded when one party acknowledges the other party's acceptance of the contract's terms and conditions. An e-contract can be concluded by an exchange of emails. The moment of conclusion in this case is considered to be when an email, containing acceptance of a contract, is delivered to a recipient or inbox of an email service provider. In some cases, the conclusion takes place with the start of the execution of the contract, as e-commerce can often be structured as an offer to the public. E-contracts can be also concluded by a click, which is equal to the signing of a traditional contract (section 1326 of the Civil Code). While 'click-wrap' contracts are valid, on specific unfair clauses jurisprudence has been contradictory on acceptance by the parties with an additional and specific handwritten or strong electronic signature.

Legislative Decree 70/2003 provides that in order for a 'click-wrap' contract to be valid, providers must send confirmation including:

- a summary of the general and specific conditions applicable to the contract;
- details of the main features of the goods or services provided; and
- detailed information regarding the price, payment methods, delivery costs, taxes and the right of the consumer to repent and withdraw, including the terms and conditions to exercise those rights.

As EU Directive 2161/2019 has been implemented, providers are also obliged to be more transparent with respect to the parameters for classification of online offers.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Legislative Decree 70/2003 is the main framework for contracting on the internet. The distinction between business-to-business (B2B) and business-to-consumer (B2C) contracts lies in the level of protection guaranteed by the applicable law. Stricter requirements apply in B2C contracts owing to special consumer law provisions (the Consumer Code), under which providers have additional pre-contractual obligations to provide clear and comprehensible information to consumers (sections 1341, 1342, 1325, 1326 and 2702 of the Civil Code).

Legislative Decree 26/2023, implementing EU Directive 2161/2019, has introduced relevant amendments, such as:

- new rules on consumers' right to withdraw;
- criteria for identifying the 'previous price' for price reduction notices;
- a requirement for clear information to be provided to consumers in the case of price reductions (any announcement of a price reduction must indicate the lowest price the professional has charged for the sale of the product during the 30 days preceding the application of the reduction);
- the extension of the consumer rights framework to contracts in which the consumer, in exchange for the supply of a digital content or service, provides or undertakes to provide personal data to the professional; and
- individual remedies for consumers (compensation, price reduction, termination of contract, etc) if they are harmed by unfair trade practices.

Legislative Decree 170/2021, implementing EU Directive 2019/771, makes changes to the Consumer Code regarding online sales contracts between consumers and sellers (B2C relationships).

Below are the contents of some of the main provisions, as amended or introduced (sections 128–135 septies of the Consumer Code):

- conformity of the good must be assessed in light of both subjective and objective requirements;
- the seller is liable for any lack of conformity existing at the time of delivery that becomes evident within two years; and
- complaints for product defects can be made within 26 months of delivery of the good.

The regulation of the supply of digital content and services has been reformed through Legislative Decree 173/2021, which will implement EU Directive 2019/770; the new and amended provisions (set forth in the new Chapter I-bis of Part IV, Title II of the Consumer Code) apply to the supply of digital content and services that takes place on or after 1 January 2022.

The rules of the new Chapter I-bis of the Consumer Code apply to contracts in which the consumer pays a price as well as to those in which the consumer provides or agrees to provide their personal data in exchange for the provision of the digital content or service and such data is not processed for the sole purpose of rendering the service.

## Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

E-signatures are regulated by the Digital Administration Code (CAD). The different types of e-signatures recognised by law are simple, advanced, qualified and digital.

While simple electronic signatures (eg, electronic file signed by insertion of username and password, clicking on a tickbox) are considered to satisfy the requirement of written form – although freely assessable in court by a judge – the document signed with an advanced,

qualified and digital electronic signature has the evidentiary effectiveness provided for by section 2702 of the Civil Code.

The Agency for Digital Italy's (AgID) Guidelines have been published, which allow for the online signature of documents through the SPID, a public system of digital identification, in compliance with article 20 of the CAD.

It should be noted that the law (article 21 CAD) states that the private deeds referred to in article 1350 of Italian Civil Code, Nos. 1 to 12, if provided as a digital document, shall be signed, on penalty of invalidity, with a qualified e-signature or digital signature.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

For B2C e-contracts, consumer legislation provides that consumers will not suffer in the case of a breach of pre-contractual obligations regarding additional expenses. For example, in the case of a lack of conformity of the goods sold, the consumer has the right to have the goods brought into conformity, without cost, by repair or replacement. Remedies on pre-contractual liability under the Civil Code apply to other breaches of pre-contractual obligations. Other general remedies provided by the Civil Code (eg, termination for unfulfilment, nullity for lack of essential elements of a contract, provisions on contract performance and compensation for damages, reduction of price) will also apply.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The promotion and selling of financial services or products are subject to specific rules. Articles 30 to 32 of the Consolidated Law on Finance regulate the distance selling of financial services or products. The authority for the regulation of the financial markets (CONSOB) has also adopted a specific regulation on intermediaries, which provides that only duly authorised intermediaries can promote and sell financial services or products via distance selling. The Consumer Code provides special protection for consumers.

As of 2 February 2022, asset managers are obliged to comply with the interpretative guidelines issued by the European Securities and Markets Authority, namely, the Guidelines on Marketing Communications under the Regulation on Cross-Border Distribution of Funds, adopted on 27 May 2021.

## Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Electronic monetary institutions are mainly regulated by Legislative Decree 218 of December 2017, which transposed EU Directive 2015/2366 and came into effect on 13 January 2018. In Italy, entities other than banks that exclusively carry out the activity of issuing electronic money are called Electronic Money Institutions (IMELs), empowered to perform this function by EU directives and subject to the supervision of central banks. In Italy, IMELs are counted among the credit institutions regulated in the Consolidated Banking Act and are subject to the supervision of the Bank of Italy, which has dictated specific rules of conduct to be followed – for example, the Bank of Italy's Provisions, dated 22 February 2022 and 2 November 2022, amending the Supervisory Provisions for Payment Institutions and Electronic Money Institutions of 17 May 2016 (22A01380).

So far, the Italian government has addressed virtual currencies as part of anti-money laundering matters, but has not adopted specific legislation regarding digital assets.

EU Regulation 2023/1114 (the Markets in Crypto-Assets Regulation (MiCA)), will be applicable from June 2024. The Regulation establishes uniform requirements for the public issuance of and admission to trading of various crypto-assets.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

MiCA shall apply to member states from 30 December 2024.

However, in Italy, the Decree of the Ministry of Economy and Finance dated January 2022 provides precise obligations for service providers in relation to the use of virtual currency and digital wallets, both to operate in the state and in terms of disclosure requirements.

According to article 3 of the Decree, providers of crypto currency services and e-wallets must apply for registration with the organisation responsible for management and supervision of financial advisor and credit broker lists (OAM). Such registration is considered a necessary requirement to lawfully carry out the aforementioned activity.

Information to be provided in the application form differs depending on whether the applicant is a natural person or a legal entity. Following the communication, OAM verifies the validity and completeness of the information and the attached documentation and, within 15 days of receipt, allows or denies registration. If there is incomplete documentation, OAM has the right to suspend the procedure to acquire additional information.

Registration is in any case subject to the possession of the same requirements as for operators carrying out currency exchange activities pursuant to article 17-bis, c 2, Legislative Decree 141/2010.

The Legislative Decree establishes that to obtain registration by OAM, providers must communicate their operations in Italy and continue to exercise their activity according to specific deadlines provided.

Moreover, article 5 of the Decree of the Ministry of Economy and Finance requires crypto currency and e-wallet providers to transmit data on customers and transactions carried out in the national territory on a quarterly basis to OAM.

Law No. 197 of 29 December 2022 (Budget Law 2023, article 1, paragraphs 126 to 147) provides, for the first time in Italian legislation, for a unified tax regulation of cryptocurrencies, crypto-assets or virtual currencies. The provision thus introduces a unitary tax regulation for crypto-assets, which includes taxation of capital gains realised and other income received through transactions involving crypto-assets, however denominated, at 26 per cent if they exceed the €2,000 threshold in the tax period.

## Electronic payment systems

### 13 How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

The EU Payment Services Directive (2015/2366/EU) (PSD2) aims to improve existing EU standards for electronic payments. The PSD2 sets standards covering security, transparency and information requirements for electronic payments and the protection of consumers' financial data, together with the rights and obligations of users and payment service providers.

The PSD2 introduced the 'open banking' (or 'open data') system, in which financial information is shared, subject to customer consent, between banks and with external companies, as well as 'third parties' (TPPs), to develop innovative products and services.

Italy has implemented the PSD2 via Legislative Decree 218/2017 (also amended by Legislative Decree No. 36/2020). The main changes that the Decree has introduced concern:

- the extension of scope of certain exemptions thereto; and
- the introduction of new payment services to which service providers in this sector are subject.

The recent measures regarding the point of sale (POS) obligation and electronic invoicing contained in the National Plan of Resilience and Recovery 2 came into force in July 2022 – a further piece of a long-term plan by the Italian government to favour the use of electronic payments. Specifically, an administrative penalty will be linked to the POS obligation, and electronic invoicing will be extended to the flat-rate schemes.

In 2018, the Agency for Digital Italy's (AgID) Guidelines on electronic payments for public administrations and public service providers that adopt AgID's platform were issued. The Guidelines define rules, standards and technical specifications.

## Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Decree-Law 76/2020, converted into Law 120/2020 establishes that if the customer has a digital identity with 'at least a significant level of security', the identification obligation is met, even if there is no physical presence of the customer. The digital identity must, however, have been issued under the Public System for the Management of Digital Identities (SPID) or under an electronic identification scheme included in the list published by the European Commission pursuant to article 9 of EU Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).

The eIDAS Regulation, while not explicitly addressing KYC or AML, establishes a framework for trust in electronic transactions, which can have a direct impact on KYC and AML procedures. These procedures often necessitate stringent proof of identity, which electronic identification compliant with eIDAS can facilitate. Coupled with the eIDAS Regulation, the Simplifications Decree highlights the utility of digital identity in meeting KYC requirements, providing this digital identity has a significant level of security.

However, these identifications also align with the mandates of the European Central Bank and EU Directive 843/2018 (5th Anti-Money Laundering Directive (AMLD5)). These mandates require financial institutions within the EU to perform rigorous KYC checks on their customers to prevent money laundering and the financing of terrorism. Understanding the nature of the customer's activities, verifying their identity, and assessing their associated money laundering risks are essential parts of these checks.

Moreover, the AMLD5 encourages a risk-based approach. This approach suggests that the measures employed to mitigate money laundering should match the risks posed by the customer. Therefore, institutions may need to apply more comprehensive identification processes for customers representing a higher risk, potentially going beyond just the username and password and multi-factor authentication (MFA) procedures.

The secure nature of these digital authentication processes also comes to the forefront. Financial institutions must ensure their digital authentication processes – which involve practices like secure coding, penetration testing, timely software updates and the use of secure communication channels – are robust and secure. The AMLD5 also has provisions for third-party reliance, allowing entities obligated to perform KYC checks to depend on third parties to conduct these checks. However, the ultimate responsibility remains with the entity relying on the third party; the former must therefore ensure that the third party is compliant with AML and KYC regulations.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

The '.it' domain is assigned by the Italian Registration Authority (RA) under the Regulation on Assignment and Management of Domain Names (the Regulations). Applications to register a '.it' domain name must be filed with the RA through a registrar and in accordance with the Regulations. Other restrictions include the prohibition of registering domain names identical or similar to third-party distinctive signs so as to profit from their goodwill or reselling them to such third-party owners (cybersquatting, typosquatting).

The main principles for domain names are 'first come, first served' and the domain name's uniqueness. According to applicable law, only business entities or adult individuals that are resident or have a registered office in a European Economic Area country, the Vatican State, San Marino or Switzerland may register a domain name in Italy.

The licensing of domain names is not a common business practice in Italy but is legally feasible (usually within the broader scope of trademark licence agreements). Registrars' terms of service might nevertheless require that the domain name owner assumes liability for damages caused by unlawful use of the domain if the owner fails to provide the licensee's contact details to a third party giving reasonable evidence of actionable harm.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Domain names are subject to the principle of unity of distinctive signs (Intellectual Property Code, section 22). It is therefore prohibited to adopt a domain name that is identical or similar to a trademark used in a business activity if the similarity between the signs or business activity and the products or services will cause a likelihood of confusion. The owner of a pre-existing trademark may invoke protection based on trademark or unfair competition rules. Likewise, registration of a domain name does not per se imply that that a distinctive sign also fulfils all the requirements for trademark protection.

Ownership of a registered trademark is usually fundamental to support the claimant's rights against a competitive use or registration of a similar domain name. Indeed, to challenge a '.it' domain name registration, claimants must provide evidence of:

- ownership of a distinctive sign (ie, a trademark or a service mark, a company name, a name) with which the disputed domain name is identical or confusingly similar;

- the absence of legal rights or a legitimate interest of the registrant in the disputed domain name; and
- the domain name having been registered and used in bad faith.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

The relevant rules governing advertising on the internet include Legislative Decree 206/2005 (the Consumer Code), as amended by:

- Legislative Decree 146/2007 on unfair business practices;
- Legislative Decree 145/2007 on misleading advertising;
- the Self-Regulatory Code of Commercial Communication of the Institute of Self-Regulation for Advertising (IAP), accepted by the near totality of advertising operators in Italy through subscription to the IAP or standard clauses included in contracts; and
- Legislative Decree 70/2003 on e-commerce.

Other specific rules on targeted advertising are included within Regulation (EU) 2022/2065 (the Digital Services Act (DSA)).

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

As a general rule, consent is required to profile a customer base for targeted advertising, according to article 122 of the Personal Data Protection Code (implementing the EU e-Privacy Directive 2002/58/EC). With regard to cookies, in June 2021 the Italian Data Protection Authority adopted new Guidelines on the Use of Cookies and Other Tracking Tools, which replace the previous guidelines provided by the Authority in 2014. Most importantly, the new guidelines confirm that the prior informed consent of the user referred to in article 122 of the Personal Data Protection Code needs to fulfil the validity requirements set forth in articles 4(11) and 7 of the General Data Protection Regulation, namely, consent must be expressed by means of a clear affirmative action, such as by clicking on a button or ticking a box. Therefore, actions such as scrolling or swiping through a webpage, or similar user activity, do not satisfy the requirement of a clear and affirmative action (as indicated by the European Data Protection Board in its Guidelines 05/2020 on Consent under Regulation 2016/679).

Specific rules on targeted advertising are included in the DSA. In particular, providers of online platforms that present advertisements on their online interfaces are required to ensure that the recipient of their service can easily identify the following:

- that the information is an advertisement, including through prominent markings;
- the natural or legal person on whose behalf the advertisement is presented;

- the natural or legal person who paid for the advertisement, if that person is different from the natural or legal person on whose behalf the advertisement is presented; and
- meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters.

Providers of online platforms are also required to avoid presenting advertisements:

- to all recipients of the service when the advertisement is based on profiling, as defined by article 4(4) of the GDPR, using special categories of personal data, as defined by article 9(1) of the GDPR; and
- to minors when the advertisement is based on profiling, as defined by article 4(4) of the GDPR, when they are aware with reasonable certainty that the recipient of the service is a minor.

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

As a general rule, the provisions on misleading and illegal comparative advertising apply to online advertising. In addition to the legal sources on misleading advertising, Decisions 17589/2007 and 17590/2007 of the Competition and Market Authority (AGCM) on misleading and illegal comparative advertising apply. Individuals or organisations may report advertising as misleading to the AGCM.

In the event of a violation of or non-compliance with the IAP's Self-Regulatory Code of Commercial Communication, including its provisions on misleading advertising, the interested parties can file a report and a monitoring committee will then commence an investigation. The report must include details of the alleged violation and relevant documentation should also be provided.

Specific sector regulations issued by the relevant authorities may provide additional provisions (eg, advertising relating to financial services).

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

The advertising of pharmaceuticals is authorised only for over-the-counter products. Under Legislative Decree 219/2006, the advertising of pharmaceuticals must be authorised by the Ministry of Health and advertising on the Internet must include details of such authorisation in addition to other requirements (National System Guidelines of the Ministry of Health).

For games and betting, the Competition and Market Authority approved Guidelines concerning the prohibition of advertising games with cash winnings applicable to entities operating in the gambling sector.

There are special rules providing restrictions for certain types of services and products such as alcohol, tobacco, financial services, cosmetics products, food and food supplements.

The Regulatory Code of Commercial Communication provides special provisions for the advertising of pharmaceutical products, food supplements, beauty treatments, toys, travel and gaming.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

The use of automated means (eg, automated calling or communications systems without human intervention or email, fax or text) for marketing purposes is allowed only with the prior consent of the consumer (ie, the 'opt-in'). Unsolicited marketing is not allowed.

In 2013, the Data Protection Authority issued its Guidelines on Marketing and Against Spam and introduced the requirement for a unique indication of consent for marketing purposes, providing that selective opt-out has to be guaranteed. Consumers or data subjects can opt out at any time from one or more of the means of marketing communication used by data controllers. Other provisions have been introduced for telemarketing (Law 5/2018).

Exceptions to the above-mentioned general rule are as follows: section 130 of the Data Protection Code regulates 'soft spam', which is considered an exception to the opt-in rule regarding promotional emails. If data controllers obtain the electronic contact details of customers in the context of the sale of a product or service, they can use this data for direct marketing of similar products or services, provided that the customers are clearly and distinctly given the opportunity to object free of charge and in an easy manner to such use of their electronic contact details when collected and on receipt of each additional message when customers have initially agreed to such use.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

ISPs do not have a general obligation to monitor published contents in advance (article 17, Legislative Decree 70/2003) and, according to article 16 of Legislative Decree 70/2003, the ISP (in particular the hosting provider) is not liable for information stored by the recipient of the service, provided that:

- the ISP 'is not actually aware of the fact that the activity or information is illegal and, with regard to actions for damages, is not aware of facts or circumstances that make manifest the illegality of the activity or information'; and
- 'as soon as it becomes aware of such facts, upon communication from the competent authorities, it acts immediately to remove the information or to disable access to it'.

The Digital Services Act (DSA), applicable as of January 2024, specifies ISPs' duty of care obligations, integrating detailed rules for the various categories of ISP. With regard to hosting providers, user-friendly notification mechanisms for reporting illegal content are provided for.

On the ISP's liability, Italian jurisprudence (Decision 7708/19, Corte di Cassazione, Sez V – Court in Rome, Section XVII Civil, Decision 693/2019) confirms what is stated with regards to the ISP's liability, analyses the profiles of liability also with reference to the hypothesis of omissive liability and the active and passive roles of ISPs.

A more recent jurisprudence (Decision 39763/2021, Corte di Cassazione) clearly established the liability of the platform for copyright infringement. Specifically, the Court ruled that the general liability provisions apply to the active hosting provider (eg, that which carries out the activities of content selection and cataloguing). This would result in damages being recovered by the owner of the infringed copyrights.

## Content liability

### 23 When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

If the provider directly delivers the incorrect information or intervenes to modify the content of the information, direct liability profiles may apply. If, on the other hand, the content is uploaded by a third party, it is necessary to verify the effective power of control of the website provider, assessing the circumstances of the case. It is advisable (but not required by law) to post a notice about the origin of content containing a disclaimer regarding the accuracy or correctness thereof to exclude the website provider's liability for incorrect information and for any consequences resulting from reliance on said content. Furthermore, it is advisable to ensure that the terms and conditions relating to the use of the website include specific contractual provisions that release the provider from liability for incorrect information published on its website.

In the absence of specific regulations on the metaverse, metaverse providers would not be excluded from the above considerations.

With regard to the liability of ISPs, recent jurisprudence (Decision 7 7708/19, Corte di Cassazione Sez V) distinguishes between active and passive hosting providers. An active hosting provider performs certain operations on content (filtering, indexing, selection, etc), while passive hosting providers provide a mere technical service.

A passive hosting provider can be called to answer for damages suffered unless the conditions for the exemption of liability under article 16 of Legislative Decree 70/2003 are met.

An active hosting provider, on the other hand, is subject to the ordinary rules of civil liability, and could also be liable for an offence by means of omission in conjunction with the author of the violation, if it does not promptly remove the illegal content.

More recent jurisprudence (Decision 39763/2021, Corte di Cassazione) clearly establishes the liability of the platform for copyright infringement.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

As soon as an ISP becomes aware of such defamatory material, upon communication from the competent authorities, it shall act immediately to remove the information or to disable access to it.

In fact, according to the Civil Supreme Court, the obligation of removal does not require a formal warning from authorities, but a simple communication made by any ordinary means is sufficient to ensure that the ISP is aware of the infringement of the right of a third party.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

Databases can be protected either as creative (copyrightable) works or as assets created through the investment of resources (even where databases may not be qualified as creative). In the first case, the right holder may take action against unauthorised reproductions or other uses of its database (including, to an extent, the contents of that database). The second case is regulated by the sui generis rights afforded to database owners, who are entitled to prevent reproductions of their database (in whole or in part, to the extent that the arrangement and structure of the database is copied or used without permission), but this entitlement does not extend to the contents of the databases which, in themselves, may not be eligible for protection. Rights holders of databases can authorise the permanent or temporary reproduction of a database, in full or in part, by any means and in any form. The recent implementation of the new EU Directive on Copyright in the Digital Single Market provides some limitations and exceptions to the exclusive rights of the rights holders for reproductions and extractions of lawfully accessible works for the purposes of text and data mining.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Linking to third-party websites may trigger different legal issues and therefore a case-by-case analysis is recommended, even more so if new intellectual property (IP) realities (such as a metaverse) are involved. Simply linking to the homepage of another website is usually admissible. Deep linking (to a specific page within another website), including framing (ie, allowing users to access elements of another website on the original website thus giving

the impression that the framed element belongs to the original website), may constitute copyright infringement. Embedding third-party content may also constitute copyright infringement or unfair competition when users cannot identify the original source or are induced to believe that there is a commercial relationship between the two websites. Should a trademark be part of a link, trademark infringement may occur. To the extent that a linked website contains illegal content, the linking website may be considered liable for contributory infringement. Verifying the linked website's linking policy and seeking prior consent is always recommended.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

As a general rule, a copyrightable work belongs to its author or assignees. Rights holders can prevent third parties from using their work or any derivative work. A website owner's unauthorised use of third-party copyrighted content constitutes copyright infringement, unless such use is permitted in certain circumstances. Italian copyright law does not provide for a general defence based on fair use; rather, it allows specific permitted uses where, given the circumstances or intended use, the use of third-party copyrighted work (or a portion thereof) is permitted.

The above principles should likewise apply to the metaverse, in the current absence of a dedicated discipline (even following the implementation of the new EU Directive on Copyright in the Digital Single Market).

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

There is currently no dedicated legislation covering the protection of intellectual property rights in a metaverse. Hence, all intellectual property principles need be adapted by way of interpretation to this new technical and commercial scenario (eg, collecting evidence of an infringement, the scope of licensed rights, measure of damages). As a general suggestion, negotiations of new IP contracts should also explicitly address licence rights for metaverse-related usage.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Yes. Exhaustion of rights is a principle that embraces both intellectual and industrial property law and is expressly recognised by both the Italian Industrial Property Code and Italian Copyright Law.

Exhaustion occurs only where the first sale or other transfer of ownership is made by the rights holder or with their consent, in the territory of Italy or in the territory of a member state of the European Union or the European Economic Area.

The application of exhaustion of rights for digital products has also been strongly debated at the EU level; by way of example, a recent Court of Justice of the European Union decision ruled that the question of exhaustion does not arise in the case of online services (namely, e-books). Likewise, at this early stage of the legal analysis of the metaverse, there would be arguments to dispute that exhaustion applies to digital products placed on a metaverse.

## Administrative enforcement

### 30 Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

The Italian Collecting Society (SIAE) and the Communications Regulatory Authority (AGCOM) are granted surveillance powers to prevent and establish copyright infringement (eg, the authority to access premises and request the disclosure of documents). The SIAE also has investigative powers with regard to suspected value added tax avoidance.

AGCOM can adopt measures against the illicit publication of digital work online, including the power to request the removal of access to websites hosting infringing content or the removal of unlawful content. Administrative fines and criminal proceedings may apply in the case of non-compliance with AGCOM.

Pursuant to EU Regulation 608/2013 concerning the enforcement of IP rights, Customs can seize goods in the case of IP infringement.

Public prosecutors also have enforcement powers when an IP infringement constitutes a criminal offence.

## Civil remedies

### 31 What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

IP owners can rely on a significant variety of remedies in civil proceedings, either in the course of proceedings on the merits or in urgent actions (interim proceedings). Civil remedies include:

- permanent (and interim) injunctions against infringers;
- penalties for further infringements;
- damages;
- the seizure or destruction of infringing goods or production facilities;
- the publication of a court order;
- the removal of infringing goods from the market; and
- the issue of a disclosure order.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

The Personal Data Protection Code reflects the definition of 'personal data' provided by article 4(1) of the EU General Data Protection Regulation (GDPR):

> *Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Article 9(1) of the GDPR also introduce special categories of personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership. Genetic data and biometric data are also included as special categories. According to section 2-septies of the Personal Data Protection Code, the Data Protection Authority will adopt specific identification security measures with regard to the selective access to data to ensure that said information is made available to data subjects. The Data Protection Authority has provided specific provisions for the storage and security of genetic data as per Order No. 146/2019.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

There are no registration requirements at present. Data protection officers can be in-house or external and must follow the GDPR.

### Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

In this respect, Italian data protection legislation follows the rules set out in the GDPR.

### Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

In this respect, Italian data protection legislation follows the rules set out in the GDPR.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

In this respect, Italian data protection legislation follows the rules set out in the GDPR. In addition to this are the Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, which provide for a six-step methodology to address data transfers, and Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, which summarise the requirements set forth by EU law in order for public surveillance measures to be lawful.

In the criminal sector, Italy has adopted Legislative Decree 51/2018, implementing Directive (EU) 2016/680 and repealing Council Framework Decision 2008/977/GAI. Article 31 et seq of the Decree regulates in what cases the transfer of these types of data to a third country or international organisation can take place.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

Particular attention must be paid to cases in which:

- personal data is communicated to autonomous third-party data controllers; and
- lists from third parties are received from autonomous data controllers; it should be verified that personal data has been lawfully collected by the transferor.

In this regard, we refer to the Authority's Guidelines on Marketing and Against Spam (4 July 2013) that provide specific provisions for the transfer of personal data to third parties for marketing purposes. In particular, the Guidelines state that:

> *a data controller planning to collect personal data also with a view to communicate (or transfer) such data to third parties for the third parties' marketing purposes must first inform data subjects appropriately … and obtain specific consent.*

Further, the Italian authority requires that data controllers who intend to use personal data that has been collected or sold by data brokers or third parties verify the obligatory compliance requirements of at least 10 to 15 per cent of the transmitted data (eg, that the data subjects were dutifully informed and have explicitly consented).

There is currently no specific metaverse legislation in Italy differing from the applicable industry regulations.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Italian data protection legislation follows the rules set out in the GDPR. In addition, there is no difference between citizens and foreign individuals with regard to data protection law.

Regarding remedies, section 140 bis of the Personal Data Protection Code provides for alternative forms of protection: in situations where data subjects consider that their rights based on the applicable law have been violated, they may lodge a complaint with the Data Protection Authority or appeal before the Italian judicial authority. However, the Italian legislator has prescribed that there are two remedies, mutually exclusive to each other: filing a complaint with the Data Protection Authority or taking the matter to the judicial authority.

Section 141 of the Personal Data Protection Code provides that a data subject may lodge a complaint with the Data Protection Authority, according to article 77 of the GDPR.

The complaint to the Data Protection Authority must contain all the details set out in section 142 of the Personal Data Protection Code (eg, a detailed indication of the circumstances on which it is based and the provisions violated).

Section 144 of the Personal Data Protection Code provides that anyone may submit a report, which the Data Protection Authority may take into consideration.

The Data Protection Authority may take the measures referred to in articles 58 and 56 of the GDPR.

Italian legislation does not provide specific regulations for individuals of Italian citizenship, and the requirements of the GDPR will be applicable.

## Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

Data that is not included within the definition of personal data is regulated by EU Regulation 2018/1807 on a framework for the free flow of non-personal data in the EU.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

In January 2022, the new AgID Guidelines on the Formation, Management and Preservation of Electronic Documents came into effect. The Guidelines apply to all organisations, public and private, obliged to preserve electronic files that constitute the originals to be archived, according to civil, tax and digital administrative obligations.

Decree 58/2013 of the President of the Council of Ministers identifies the types of unique original analogue documents for which, due to public needs, the obligation to preserve the original documents in paper format remains. Such documents are, for example, and by way of non-exhaustive list: acts contained in the Official Compendium of Legislative Acts of the Republic of Italy; notary acts; judicial, procedural and judicial police acts for the next 20 years; state property and historical documents; and acts preserved in notary archives. The complete list is contained in the Annex to the aforementioned Decree.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Italian sector-specific laws provide for the retention period of certain documents.

In some cases, the retention period of documents is determined by the limitation period of legal action: article 2946 of the Civil Code provides that '[e]xcept where the law provides otherwise, rights are extinguished by prescription with the lapse of ten years'.

The following are some examples of such sector-specific provisions:

- accounting records must be kept for 10 years from the date of the last entry, pursuant to article 2220 of the Civil Code; and
- tax invoices must be kept for a period of 10 years after their creation.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

Article 32(1) of the EU General Data Protection Regulation (GDPR) is the starting point regarding the security measures that must be taken into account to ensure the cybersecurity of data and to limit the possibility of personal data breach. The principles and measures set out in this standard are then used as a reference and further implemented by regulations, standards and technical guidelines developed by bodies and organisations at the European and international level.

Each organisation can use European Network and Information Security Agency, International Organization for Standardization, and National Institute of Standards and Technology guidelines, as well as other guidelines, in order to determine its own framework and adapt it to its specific needs and context. Thus, there is no requirement to achieve a minimum level of cybersecurity common to all organisations, applying in this context the principle of accountability, through which organisations must be able to demonstrate the adequacy of the technical and organisational measures taken to protect the data they process. To this end, it will be crucial to verify that the processing has a low residual risk by assessing the risks in advance and adopting appropriate security measures.

Finally, additional references are represented by:

- Legislative Decree 65/2018 (implementing EU Directive 2016/1148/EU), which applies to e-commerce in the cases set out in Annex III of the same Decree; and
- the new EU Payment Services Directive (2015/2366/EU), which provides for important innovations in the world of digital payments.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Italy's data breach notification requirements reflect those set out in the GDPR. With regard to cybersecurity, Legislative Decree 65/2018 (implementing EU Directive 2016/1148/EU (the NIS Directive) on the security of network and information systems) also applies to e-commerce. Legislative Decree 65/2018 defines the technical and organisational measures that must be adopted to manage and minimise the risks of cyberattack. In this regard, Legislative Decree 65/2018 refers to EU Regulation 151/2018, which sets out factors that must be considered by digital service providers.

In the case of a security incident, Legislative Decree 65/2018 provides that digital service providers must notify Italy's Computer Incident Response Team without undue delay. The digital services providers indicated in Legislative Decree 65/2018 are those expressively included in Annex III of the NIS Directive (eg, search engines, cloud service providers and e-commerce platforms).

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

In Italy, investigating authorities have the right to access personal data in the course of a criminal investigation.

In particular, under articles 234 and 234 bis of the Code of Criminal Procedure, the judicial police or the Public Prosecutor may obtain copies of acts and documents containing personal data; in the event of a request for data or documents by the judicial authority, it is not permitted to refuse to produce them.

According to article 391 bis et seq of the Code of Criminal Procedure, the defendant's lawyer is allowed, when carrying out defensive investigations, to request personal data. There is no explicit provision for access to acts and documents; the same purpose is achieved by requesting information orally from the person who will be required to answer during the specific interrogation.

Moreover, pursuant to section 132, paragraph 3 of the Personal Data Protection Code, if there is sufficient evidence of crimes for which the law establishes the penalty of life imprisonment or imprisonment of not less than a maximum of three years, and of crimes of threatening and harassing or disturbing persons by means of a telephone, when they are serious, where they are relevant to the continuation of the investigation, the data is acquired from the supplier by reasoned decree of the judge, at the request of the public prosecutor or at the request of the defence counsel of the accused, the person under investigation, the injured party or other private parties. If the prosecutor's decree is not validated within 48 hours, the data acquired cannot be used.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Italy has adopted stringent legislation with regard to online betting and gaming. As a general rule, betting and gaming are governed by the state (through article 1 of Legislative Decree 496/1948), which can grant concessions to private operators. Secondary legislation concerning betting and gaming is found in the Civil Code and special laws and regulations

issued by the Customs and Monopolies Agency. Different products are regulated separately under the scope of specific laws and regulations (eg, online betting and online bingo). Concessions, authorisations and licences are required to lawfully perform online betting and gaming activities and provide products and services to persons located in Italy. The main type of licence is a concession, which is normally issued through a public tender. The general principle is that only authorised operators can offer online betting and gaming.

Residents can use only licensed online casinos and betting websites. Websites that provide gaming services must indicate that they are authorised to do so. Article 24 of Law 111/2011 prohibits minors (ie, residents aged under 18) from taking part in public games with cash prizes.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

According to Italian gambling advertising guidelines issued by the Authority for Communications Guarantees (AGCOM) in 2019, article 9 establishes that the general prohibition of paid game advertising applies to entities having their registered office, including branch offices, in Italy. The provision sets the fight against gambling as a general objective by introducing an absolute ban on the dissemination of 'any form of advertising, including indirect advertising' relating to games with cash prizes presented 'in any form and by any means, including sporting, cultural or artistic events, television or radio broadcasts, daily and periodical press, publications in general, posters and computer, digital and telematic channels, including social media'. The prohibition also applies to entities with registered offices abroad, if they have:

- received a concession for the provision of pay-per-click gaming in Italy from the Customs and Monopolies Agency; and
- been authorised to provide audio-visual media services in Italy.

Distinctive signs of legal gaming are not covered by the prohibition in article 9 only where they strictly identify the place where the relevant activity is carried out (by way of example, mere business signs or domains of online sites).

There is currently no specific metaverse legislation in Italy that differs from the applicable industry regulations.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

There is no overarching legislation on outsourcing, but sector-specific laws and guidelines apply at national level. In particular, the Civil Code's general provisions on contracts apply,

and its specific provisions on service and work contracts or supply contracts. Hence, the general rules provided in the Civil Code apply with specific regard to the general principles applicable to contracts (article 1321 et seq Civil Code), supply contracts (article 1559 et seq Civil Code) and works and services contracts (article 1655 et seq Civil Code).

## Sector-specific issues

### 48 Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

Provisions regarding specific sectors (eg, financial services or e-contracts) will be applicable. It is advisable to evaluate what kind of legal structure is used for outsourcing. Regarding personal data, specific provisions on transfers and databases must be considered.

## Contractual terms

### 49 Does the law require any particular terms to be included in outsourcing contracts?

Sector-specific laws and guidelines apply to outsourcing contracts. Among the sector-specific laws, reference is made in particular to:

- EU General Data Protection Regulation (GDPR) (eg, for IT and cloud services);
- CAD: Digital Administration Code;
- Public Contract Code (Legislative Decree 163/2006);
- the discipline of temporary employment agency work contracts;
- Sub-Supplier Contract Law (Law 192/1998);
- the Bank of Italy's guidelines; and
- circulars governing the outsourcing of services by banking institutions.

In light of the above, it is highly recommended to include some of the following remedies and mechanisms in outsourcing contracts, as appropriate:

- service levels (SLAs) are usually agreed upon to monitor contract performance and ensure a minimum satisfactory level of service. Other SLA-related remedies may include termination (eg, if a penalty cap is exceeded) and the right to claim compensation for additional damages;
- a detailed change request procedure is usually agreed upon;
- the parties can agree on periodic audits in order to monitor contracts;
- the appointment of joint committees to handle any service-related issues or any changes to the service;
- escalation procedures aimed at involving an adequate level of management to address and manage contractual disputes before a claim is brought to court;
- the adoption of benchmarking mechanisms to facilitate the measurement of service performance and agree on service changes or price adjustments (or both); and
- with specific regard to IT outsourcing, service specifications for data processing agreements should comply with requirements set out by article 28 of GDPR, that are binding on processors and sub-processors.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

As a general principle, in the case of a transfer of a business, employment relationships are transferred to transferees as a going concern – without the prior consent of employees – and continue seamlessly with transferees. Legislation and case law distinguish between transfers that include the transfer of all assets (ie, workforce, contracts and goods) from transfers that involve a change of supplier that provides services via outsourcing.

Employee rights in the transfer of a business are regulated by section 2112 of the Civil Code. As a general principle, transferred employees maintain the rights from their previous employment relationship. Further, under certain conditions (eg, the number of employees involved), the parties to a transfer must undertake a consultation procedure with trade unions. Where outsourcing is not qualified as a transfer of business, the transferee may decide to apply the Collective Labour Agreement as provided by law to the transfer of employees. The transferee would then commence negotiations with the trade unions.

In the case of outsourcing contracts under which the direct management and implementation of one or more services are carried out by third parties, Legislative Decree 276/2003 provides that third parties and companies requesting the services of a third party are jointly liable for the remuneration, social security and severance package of workers involved in the contract's execution.

The level of protection guaranteed in Italy depends on whether workers are employees, self-employed or freelance workers.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

In Italy there is no specific legislation for artificial intelligence or machine learning. However, Italy adopted the Strategic Programme on Artificial Intelligence 2022–2024 (Strategic Programme) in November 2021. Italian institutions and ministers had, prior to that, already tried to provide a basic legal framework for artificial intelligence.

There is no specific Italian legislation on automated decision-making and profiling different from the applicable European legislation. In Labour Law, Legislative Decree 104/2022 (the 'Transparency Decree'), amended by Legislative Decree no. 48/2023, introduced precise information and transparency obligations for employers with respect to the use in the workplace of fully automated decision-making or monitoring systems designed to provide

relevant information for the purposes of recruitment or appointment, management or termination of the employment relationship, assignment of tasks or duties, and information on the monitoring, evaluation, performance and fulfilment of employees' contractual obligations.

Other relevant measures include the Italian Supervisory Authority's Guidelines on the Processing of Personal Data for Online Profiling – 19 March 2015 and Guidelines on Marketing and against Spam – 4 July 2013. In the latter, the Data Protection Authority confirmed its consolidated approach that requires, as a rule, the data subject's consent for profiling purposes.

In this regard, mention should be made of two relevant decisions issued, respectively, by the Regional Administrative Court (TAR Lazio – Roma, decision No. 9230/2018) and the Council of State (Decision No. 8472/2019), which assessed the use of automated means in a public administrative procedure, identifying the limits of use of automated means.

The above-mentioned decisions highlight two fundamental conditions for algorithmic effectiveness: (1) the full knowability of the module used and the criteria applied by algorithm; (2) the imputability of the algorithm's decision to the public administration, which must be able to verify the logic used, the legitimacy of the decision and the outcomes generated by the algorithm.

With respect to automated decision-making processes and the transparency of related algorithms, the Supreme Court of Cassation in judgment No. 14381 of 25 May 2021, in the context of the development of reputational profiles, established that the consent of the data subject is validly given only if it is freely and specifically expressed with reference to a clearly identified processing operation; it follows that, in the case of a web platform (with annexed computer archive) designed to process the reputational profiles of individual natural or legal persons based on a calculation system with an algorithm aimed at establishing reliability scores, the requirement of awareness cannot be considered satisfied where the algorithm's executive scheme and the elements of which it is composed remain unknown or cannot be known by the data subjects.

## IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

After the proposal of the Artificial Intelligence Act, while waiting for a new legal framework for artificial intelligence-based works, some general guidelines can be identified to assess when intellectual property protection can be claimed for assets created by artificial intelligence.

Copyright protection can be claimed for artificial intelligence that consists of software, provided that protection is limited to those elements that express the (minimum) creativity

of the author (such as the source code, but not the algorithm). As to patents, while computer programmes and mathematical methods are not eligible as such for patent protection, computer-implemented inventions can be patentable. The European Patent Office specifically addressed artificial intelligence-related inventions when updating its Guidelines for Examination in the European Patent Office.

As to whether or not an artificial intelligence system might be considered as an 'author' to whom copyright or a registered patent (or both) can be assigned, this is not possible under the current legal scenario that limits ownership to human beings; yet, it is reasonable to foresee that this human-centred approach may be superseded due to the unrelenting evolution and spread of artificial intelligence systems.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

There is no specific legislation on artificial intelligence (AI) or machine learning in Italy. The main references to AI legislation are at the European level by way of the proposed Artificial Intelligence Act by the European Commission, which was approved in June 2023 by the European Parliament. Also, at international level, there are references such as the set of recommendations and guidelines on AI in medicine or OEDC's Recommendation of the Council on Artificial Intelligence.

Italy has, however, adopted the Strategic Programme for Artificial Intelligence – AI – 2022/2024. The programme aims to develop national strategies identifying targets and priority areas for investments, as well as specific areas of intervention in the sector. Also significant are the National Research Programme 2021–2027 of the Ministry of Universities and Research, which envisages a specific sphere of action dedicated to AI in coordination with other sectors, such as digital transformation, big data, robotics and cybersecurity, and the 'Proposals for an Italian Strategy for AI', drafted by a group of 20 high-level experts working at the Ministry of Economics.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Online sales are subject to regular taxation according to the principle of territoriality and the nationality of transferors and transferees. Treaties between some countries exist to avoid double taxation.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

In general, the principle of territoriality applies. This relates to the countries in which:

- a supplier's head office and a customer's head office are located or the countries in which their branch offices, if any, are located; or
- the countries in which they have identified themselves for tax purposes, regardless of the location of their servers.

The principle of territoriality is generally connected to the country in which the head office of a supplier and buyer are located. Local legislation cannot be excluded with regard to the location of servers in countries other than those in which the companies have their registered or secondary offices or where they are registered for tax purposes.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The obligation of electronic invoicing was introduced by the 2018 Budget Law (article 1, paragraphs 909, 916 and 917).

Initially, it was provided with reference only to gasoline and diesel supplies and services provided by subcontractors to the main contractor, in a contract with a public administration.

On 1 January 2019, the electronic invoicing requirement was extended to all supplies of goods and services between businesses and to final consumers.

From 1 July 2022, the electronic invoicing obligation is extended to taxpayers under the flat rate and advantage regime who received compensation exceeding €25,000 in 2021.

Electronic invoices are conveyed through the *Sistema di Interscambio* managed by the Internal Revenue Service, which keeps all invoice data.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no specialist courts for online or digital disputes.

**Read this article on Lexology**

## ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

There are several ADR methods provided by law:

- amicable settlements;
- judicial conciliation;
- arbitration as an alternative means of dispute resolution to a court decision, as provided for by section 806 of the Code of Civil Procedure; and
- mediation.

The telematic conciliation procedure of the Competition and Market Authority and the Communications Regulatory Authority is also worth mentioning.

The Consumer Code provides a voluntary out-of-court settlement procedure for domestic and cross-border disputes between consumers and professionals residing and established in the EU. Under this procedure, an ADR body provides a solution for the parties or brings the parties together to facilitate an amicable settlement.

In Italy, like in other EU member states, parties can use, according to the EU Online Dispute Resolution Regulation (524/2013), an online dispute resolution platform.

ADR methods are not widely used in Italy, but are becoming more common.

# UPDATE AND TRENDS

## Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The new Artificial Intelligence Act may well increase productivity in the digital world, as well as improve innovation and digital processes. One foreseeable impact is that many companies will adopt artificial intelligence to maintain a competitive edge in the digital marketplace.

The Digital Services Act provides better protection for consumers and their rights online and establish a transparency and accountability framework for online providers. The Act, in fact, aims to foster innovation, growth and competitiveness within the single market. There is, for example, new procedures for removing illegal online content. Essentially, online intermediary services fall under the scope of the Digital Services Act.

The Digital Markets Act bans a number of practices commonly used by large platforms that act as 'gatekeepers'. The Digital Markets Act, among other things:

- applies only to the major providers of the basic platform services most inclined to unfair practices, such as search engines, social networks or online brokerage services, that meet the objective legislative criteria to be designated as access controllers;
- sets quantitative thresholds as a basis for identifying presumptive access controllers; it will also have the power to designate firms to serve as access controllers, following a market survey;
- prohibits several clearly unfair practices, such as preventing users from uninstalling preinstalled software or applications; and
- requires access controllers to proactively put in place certain measures, such as targeted measures that enable third-party software to function properly and interoperate with their services.

The forthcoming EU ePrivacy Regulation could place restrictions on e-commerce operators.


| | |
|---|---|
| Paolo Balboni | paolo.balboni@ictlc.com |
| Luca Bolognini | luca.bolognini@ictlc.com |
| Raffaella Cesareo | raffaella.cesareo@ictlc.com |
| Luciana Di Vito | luciana.divito@ictlc.com |
| Camilla Serraiotto | camilla.serraiotto@ictlc.com |
| Claudio Partesotti | claudio.partesotti@ictlc.com |

Via Borgonuovo 12, Milan 20121, Italy
Tel: +39 02 8424 7194
www.ictlegalconsulting.com

**Read more from this firm on Lexology**

**Read this article on Lexology**

# Japan

[Takashi Nakazaki](#)

Anderson Mōri & Tomotsune

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The Japanese government continues to focus its attention on the internet and digitalisation more generally as potential growth factors for the Japanese economy and with the aim of facilitating entrepreneurship and development.

The government formulated the concept of 'e-Japan' in 2000, when it decided to encourage the country to become more focused on information technology (IT), and the IT Basic Act became effective in 2001.

The government's positive attitude towards the internet is evidenced by some of the measures that it has taken. For example, the government has favourably adopted e-government or 'e-application' approaches under which certain applications may be filed with the government through the internet. Also, immediately after the covid-19 lockdown, the government modified its position on e-signatures and clearly stated that contracts may be executed with e-signatures and without seal impressions.

In September 2021, the government established the Digital Agency as a command centre for digital administration.

In June 2022, the government gave the green light to a new policy that plans to develop and expand the Web3 environment in the country, including the use of crypto currencies, non-fungible tokens (NFTs) and decentralised autonomous organisations (DAOs).

During the 2023 G7 summit in Hiroshima, digital ministers discussed the human-centric approach to artificial intelligence (AI), which may cover regulatory or non-regulatory policy tools. As the host country, Japan's approach to AI regulation may have considerable influence on consensus-building among global leaders.

Japan has developed and revised AI-related regulations with the goal of maximising AI's positive impact on society, rather than suppressing it due to overestimated risks. The emphasis is on a risk-based, agile and multistakeholder process, rather than a one-size-fits-all obligation or prohibition. Japan's approach provides important insights into global trends in AI regulation.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

Japan has many laws and regulations governing business on the internet.

First, the IT Basic Act was the principal legislative instrument governing internet-related issues. Second, the Civil Code, the Consumer Contract Act, and the Act on Specified

Commercial Transactions are the main legislative instruments for dealing with e-commerce. Third, some intellectual property laws may be applied to internet-related issues. The Act on the Protection of Personal Information, the Premiums and Representations Act and the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers may also be applied.

The Ministry of Economy, Trade and Industry (METI) has published the Interpretative Guidelines on Electronic Commerce and Information Property Trading on its website. These guidelines explain, with examples, how internet-related laws may be applied in certain situations.

Also, the government will urge corporate managers to take the lead in making organisational changes and devising these plans, in addition to ensuring that equipment is secure. The government spelled out these steps by April 2022 as it made the first full revision of the country's key infrastructure action plan since 2017. The new rules, which focus on economic security, took effect in fiscal year 2022.

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The regulatory bodies are the Cabinet Office (CO), METI, the Ministry of Finance (MoF), the Ministry of Internal Affairs and Communications (MIC), the Personal Information Protection Commission (PPC) and the Consumer Affairs Agency (CAA). The CO is responsible for general regulation; the METI is mainly responsible for the regulation of e-commerce; the MoF is responsible for taxation; the MIC is mainly responsible for general communication for networks forming the internet; the PPC is responsible for data protection; and the CAA is responsible for consumer protection in the context of e-commerce.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

In Japan, under the Code of Civil Procedure, the courts may generally exercise jurisdiction over defendants residing or located in Japan, even if they provide goods or services from outside. This is the case even where the defendants are non-residents and located in foreign countries, if certain conditions are met; for example, if performance of the obligations under the agreement concluded between the parties is made in Japan, the courts can generally exercise jurisdiction. In addition, in a case where the agreement is concluded between a consumer and a business operator, if the address of the consumer at the time of filing a lawsuit is in Japan, the courts can generally exercise jurisdiction. The same can be said for internet-related transactions or disputes. However, where there is some extraordinary circumstance meaning that it would be unfair or against the principle of an expeditious trial, the courts may dismiss the action without prejudice in whole or in part.

There are no court cases where the courts have applied these tests or rules to transactions in the metaverse.

Also, the amendment to the Telecommunications Business Act came into effect on 1 April 2021, aiming to protect domestic users and secure fair competition by enhancing the enforcement of the Act against foreign entities, and the Japanese regulatory authority, the Ministry of Internal Affairs and Communications (MIC), published a set of guidelines (MIC Guidelines) which are aligned with the purpose of this amendment. Based on the MIC Guidelines, even foreign entities that have no telecommunications facilities in Japan are subject to regulation if they have certain nexuses with Japan.

Finally, consumers in Japan have recourse to local courts that have jurisdiction over their residence, even if the parties agreed about exclusive foreign court jurisdiction.

### Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There are no special regulatory or procedural requirements for the establishment of digital businesses. However, certain businesses, such as virtual (crypto) currency exchange services, are regulated under the law. Establishing such a business requires notification, reporting, permission and registration, etc, in accordance with the law.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

It is possible to form and conclude contracts electronically. While a normal contract between persons at a distance is formed upon the dispatch of a notice of acceptance, an electronic contract is formed at the time of receipt of the notice of acceptance by the other party.

Click-wrap contracts can be enforceable in Japan. Contracts can be formed by simply clicking the 'I agree' or 'I accept' button, which signals acceptance of the vendor's terms and conditions.

However, some requirements must be satisfied for click wrap contracts to be enforceable. For example, it is required that the vendor's terms and conditions be clearly shown on the screen during online transactions and the user agrees with the vendor's terms and conditions by clicking the 'I agree' or 'I accept' button as conditions to effect such transactions. When the vendor's terms and conditions are only posted on the website, and are not easy to notice, and users are not required to click the 'I agree' or 'I accept' button regarding the

vendor's terms and conditions for the use of the website, the click-wrap contract is not enforceable.

Working condition notices must be delivered in paper form unless the worker agrees otherwise.

## Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

The Civil Code, the Consumer Contract Act, the Act on Specified Commercial Transactions and the Electronic Contract Act are the main laws. The Consumer Contract Act, the Act on Specified Commercial Transactions and the Electronic Contract Act distinguish between business-to-consumer and business-to-business contracts.

There are provisions for protecting consumers in contracts between businesses and consumers.

Under provisions relating to internet transactions, treatment of consumers' erroneous transactions is important. Under the Civil Code, if there is gross negligence on the part of the consumer, a business entity may assert that a contract is valid even if a consumer has operated erroneously. However, under article 3 of the Electronic Contract Act, the business entity may assert that a contract is valid only when the entity has taken measures to confirm the consumer's intent (eg, if the company has presented an opportunity for the consumer to confirm the content of an offer before making his or her final acceptance, or if the consumer has expressly abandoned any need for confirmation).

## Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Under the Act on Electronic Signatures and Certification Business, the term 'electronic signature' is defined as a measure taken with respect to information that can be recorded as an electromagnetic record. A record that is made in order to express information is basically presumed to be established authentically if the electronic signature is performed by the principal with respect to information recorded in such electromagnetic record. E-signature providers can be accredited by the Ministry of Justice, and only 10 e-signature providers were accredited as of June 2022.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

There are no special forums for dispute resolution or remedies available for the breach of digital contracts, and the government continues to consult about establishing a new institution for dispute resolution in relation to the breach of digital contracts.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The Financial Instruments and Exchange Act requires a financial instruments business operator to indicate the following information in such advertising:

- the name or trade name of the financial instruments business operator;
- the fact that the financial instruments business operator is authorised as a financial instruments business operator, and its registration number; and
- particulars concerning the nature of the financial instruments business conducted by the financial instruments business operator.

These matters are specified by Cabinet order as important matters that may have an impact on customers' judgement.

There are also rules against making an indication that is significantly contradictory to facts, or seriously misleading with regard to the outlook of profits from conducting financial transactions, and other matters, specified by Cabinet Office ordinance.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

The issue of electronic money, such as prepaid payment instruments, is regulated under the Payment Services Act (PSA).

The prepaid payment instrument may only be used to purchase goods and services and cannot be redeemed except in cases of statutory exceptions.

An issuer of prepaid payment instruments, including e-money, is required to comply with applicable rules under the PSA. Where a prepaid payment instrument is only usable for payments to the issuer for its goods or services, such issuer will not be required under the PSA to undergo any registration, although they would still have to comply with certain notice requirements. On the other hand, issuers of prepaid payment instruments that are usable

not only for payments to the issuer for its goods or services, but also for payments to other parties designated by the issuer ('third-party businesses'), will be required to undergo registration as an 'issuer of prepaid payment instruments' under the PSA.

Also, 'crypto assets' corresponding to virtual currency and 'electronic payment instruments' corresponding to stable coins are defined, and issuers of stable coins and intermediaries of transactions regarding virtual currency and stable coins are regulated, under the PSA.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

There are no rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value, under Japanese law.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

The Banking Act and certain other laws, including the regulations on electronic payment intermediate service providers, regulate legal systems for electronic payment intermediate services. A person must be registered with the prime minister. In order to engage in electronic payment intermediate services, a person who obtains such registration and engages in electronic payment intermediate services is called an 'electronic payment intermediate service provider'.

Major regulations governing the business of electronic payment intermediate service providers are as follows:

1 An electronic payment intermediate service provider that intends to conduct services that constitute electronic payment intermediate services must, in principle, disclose certain matters in advance, as specified by the Cabinet Office Ordinance. Such matters include the trade name or address, authority, indemnity and the contact details of the office dealing with complaints.
2 With regard to electronic payment intermediate services, electronic payment intermediate service providers must provide information to prevent misunderstandings, ensure proper handling of user information, ensure safety management and take measures to manage outsourcing contractors, as specified by the Cabinet Office Ordinance.
3 Electronic payment intermediate service providers must conduct business in good faith.
4 Electronic payment intermediate service providers must conclude a contract regarding electronic payment intermediate services with a bank before performing acts that constitute electronic payment intermediate services. Furthermore, the electronic payment intermediate services provided must be in accordance with such contract.
5 If banks and electronic payment intermediate service providers conclude the contract described in (4) above, they must, without delay, publish matters regarding the allocation

of indemnity liability in cases where users suffer damage, the measures for proper handling of user information, and the measures for safety management.

In concluding a contract with electronic payment intermediate service providers, banks must prepare and publish the standards required for electronic payment intermediate service providers and must not treat the electronic payment intermediate service providers that meet such standards in an unjust or discriminatory manner.

## Online identity

### 14 Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

There has been strong demand from fintech companies to be able to use the results of identity verification performed by other specified business operators, for instance where there are multiple business operators with financial licences within one corporate group.

The proposal was tested at the Financial Service Agency's (FSA) FinTech Proof-of-Concept (PoC) Hub, where three Japanese megabanks and other financial institutions experimented with sharing the results of identity verification performed using blockchain. It was concluded that the results of identity verification performed by a specified business operator can be used by certain other specified business operators on the basis of entrustment of KYC.

However, it seems that subsequently there were differences of opinion between the FSA and the National Police Agency, which has administrative jurisdiction over the Act on Prevention of Transfer of Criminal Proceeds, with the final conclusions only announced in October 2019. The conclusions stated that identity verification results may be used even if all the procedures leading up to the execution of a contract are not entrusted to another specified business operator (outsourced party), provided that the outsourced party acts between the entrusting business operator and the customer, for example as an agent or intermediary – namely, situations such as where the outsourced party's name is displayed on the entrusting business operator's website at the time the customer is conducting the application procedures with the entrusting business operator, and the outsourced party is positioned between the entrusting business operator and the customer and it is the outsourced party that requests the customer to enter its login ID and password.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

The .jp domain names are registered and administered by the Japan Registry Service Co Ltd (JPRS), to which management and administration of .jp domain names were transferred from the Japan Network Information Centre (JPNIC). Applicants can apply for .jp domain names through parties designated by the JPRS. Domain names are granted without any examination on the principle of first to file, unless they are the same as already registered domain names. Notably, however, the illegal acquisition of a domain name is defined as unfair competition under the Unfair Competition Prevention Act: the act of acquiring or holding the right to use a domain name or using a domain name that is identical or similar to another party's specific trademark, service mark or the like for the purpose of obtaining illegal profit or causing damage to a party is defined as unfair competition.

It is not possible for non-residents of Japan to register domain names with categorised JP domains (.co.jp, .ne.jp). Of course, by being resident in Japan, foreign nationals as well as Japanese nationals can register them. It is also possible for any foreign national to register a general .jp domain name if he or she has a local contact in Japan.

Also, there are no restrictions around the use of URLs to direct users to websites, online resources or metaverses.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Yes. The owner of a trademark can challenge the registered 'pirate' domain name. Domain names are granted without any examination on the principle of first to file, so it is unavoidable that domain names similar to registered trademarks are actually registered.

This can cover not only the .jp domain names but also other generic top-level domain names (gTLDs), such as .com and .net.

In addition to the litigation process, it is possible to seek dispute resolution through the Japan Intellectual Property Arbitration Centre (JIPAC) (certified by the JPNIC) regarding .jp domain names, under the JP-Dispute Resolution Policy (JP-DRP). With respect to other gTLD domain names, of course, the dispute resolution procedure is internationally available, and is operated by dispute resolution service providers such as the World Intellectual Property Organization Arbitration and Mediation Center, as certified by the Internet Corporation for

Assigned Names and Numbers (ICANN) in accordance with the Uniform Domain Name Dispute Resolution Policy established by ICANN. The owner of the trademark can demand the cancellation of the registered domain name or its transfer to the owner in these dispute resolution procedures.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

First, there is the possibility that business-to-consumer e-commerce may mislead consumers. Misleading representations are therefore prohibited under the Act against Unjustifiable Premiums and Misleading Representations as well as the Unfair Competition Prevention Act.

Regarding this point, the Fair Trade Commission has issued guidelines with respect to representations in business-to- consumer e-commerce entitled 'Problems and Points of Concern under the Premiums and Representations Act Concerning Representations in Business-to-Consumer E-Commerce', which set out points of concern regarding representations by businesses. The Consumer Affairs Agency has also issued more recent guidelines entitled 'Problems and Points of Concern under the Premiums and Representations Act Concerning Advertising Representations in Internet Consumer Transactions'.

Second, under the Act on Specified Commercial Transactions, a business entity that sells products over the internet:

- must present certain matters stipulated in the Act;
- is prohibited from using false or misleading advertisements; and
- is prohibited from providing advertisements by electronic means to any targets who have indicated they do not wish to receive such advertisements.

Furthermore, certain acts or regulations that regulate specific areas such as pharmaceuticals, health foods and money-lending businesses govern advertising on the internet.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

A business entity handling personal information shall not handle personal information about a person without obtaining the prior consent of that person, beyond the scope necessary to achieve the purpose of utilisation. So, if the scope of utilisation in a certain business purpose, which is shown in advance to the person, does not include profiling to target advertising on its website, the business operator cannot do so without obtaining the prior consent of the person involved. No particular law or judgment on profiling to carry out targeted advertising exists so far.

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

Misleading representations are prohibited under the Act against Unjustifiable Premiums and Misleading Representations, which prohibits any representation:

- in which the quality, standard or any other content of goods or services is portrayed as being much better than the actual goods or services, or in which the goods or services are portrayed as being, contrary to fact, much better than those of competitors; or
- by which the price or any other trade terms of goods or services could be misunderstood by general consumers to be much more favourable than the actual goods or services, or than those of competitors, if the representation is likely to induce customers unjustly and to interfere with general consumers' voluntary and rational choice-making.

With regard to the first point above, advertisers should keep evidence to prove the quality, standard or other contents in question of the actual goods or services, such as the results of experiments or investigations, opinions of experts, or academic literature.

From 1 October 2023, Japan will regulate stealth marketing in which influencers or others are paid to promote products and services to their followers without disclosing a financial interest under the amendments of the Act against Unjustifiable Premiums and Misleading Representations.

These rules apply to all consumer advertising in all industries.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

From 2009 to 2013, only a few medicines could be sold over the internet based on the amended Ordinance of the Ministry of Health, Labour and Welfare.

However, after the Supreme Court rendered a judgment in January 2013 stating that this Ordinance was illegal and void, the Pharmaceutical Affairs Act and the Pharmacists Act were amended in December 2013.

By these amendments, only limited and specified high-risk non-prescription medicines are now prohibited from being sold over the internet.

In addition, after the amendment to the Act on Welfare and Management of Animals in August 2012 relating to the sale of pets over the internet, it is necessary to show the pets and provide relevant information about them to customers on a face-to-face basis.

Finally, goods or services that are generally in violation of rules or regulations are not permitted to be sold on the internet.

### Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

Under the Act on Regulation of Transmission of Specified Electronic Mail and the Act on Specified Commercial Transactions, an opt-in approach is being adopted. In principle, under these Acts, advertisements by email or SMS shall not be provided by electronic means to any target unless he or she has demonstrated his or her wish to receive such advertisements.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

A content provider that mistakenly provides information leading to a third party's loss or damage may actually be liable just for providing the information. A content provider that provides information owing to a third party's contribution may be liable only when the transmission of such information apparently infringes another person's rights and it is easy to delete, which is basically the same as the liability of ISPs. Under the Act against Unjustifiable Premiums and Misleading Representations, a party that makes misleading representations can be subject to an order for suspension and payment of a surcharge.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

An online content provider that mistakenly provides information leading to a third party's loss or damage may actually be liable just for providing the information. An online content provider that provides information owing to a third party's contribution, may be liable only when the transmission of such information apparently infringes another person's rights and it is easy to delete, which is basically the same as the liability of ISPs.

Notices in this regard may be effective if a notice comprises an agreement between the website provider and viewers.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

When ISPs fail to delete illegal information sent by users or other posted messages, they may be held liable.

To prevent exposure to such tort liability, ISPs may be able to shut down a web page containing defamatory material without any third party's authorisation if a shut-down is the only way to delete illegal information, provided that the ISPs follow the requirements under the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

No, data are not protected by IP rights.

In Japan, some databases are copyright-protected. So, if people use copyright-protected databases, a website provider may stop them from using or reproducing data for commercial purposes.

A website provider sometimes uses technological restriction measures for those databases to prevent other people from using or reproducing data. Making those technological restriction measures ineffective without permission may be prohibited under the Unfair Competition Prevention Act as well as the Copyright Act.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Links to third-party websites are generally possible without permission.

However, a website owner must assume any liability.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

A website, digital platform or other online content provider (including a metaverse) cannot use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider, unless the exemption arising from citation in the Copyright Act applies.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Generally speaking, the key to whether a work can be protected as a copyrighted work is whether the work is creative or not. As to the creativity of virtual objects in the metaverse, such as items and buildings, there is difficulty in that there are multiple methods of creating virtual objects, which may affect the existence or non-existence of creativity. In other words, some virtual objects are created to faithfully reproduce objects that exist in the real world, while others are created from scratch by 3D craftsmen. With regard to the former, an object that faithfully reproduces an object that exists in reality by 3D scanning is unlikely to be found to have copyrightability in the object itself, as the composition and angle cannot be conceived and creativity cannot be found in it. As for the latter, creativity is recognised as an ordinary work and there is a high possibility that copyrightability will be recognised, but it has been pointed out that the scope of protection may be narrower for objects in the form of practical objects, such as furniture in the metaverse.

Trademarks are registered by category, and some utilisation of trademarks on a metaverse would not be covered by existing registration categories. Also, it is difficult for an owner of an existing trademark to exploit trademark rights against someone who utilised that trademark on a metaverse.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

The exhaustion of a patent is a well-established concept in Japan, while no statutory provisions exist. The Supreme Court of Japan has made two notable decisions involving patent exhaustion: one related to the recycling of ink cartridges for ink-jet printers, and the other related to the parallel importation of high-end automobile wheels from Germany for which corresponding patents existed in Japan and Germany. The German company, BBS, originally made and sold patented products and wanted to stop the parallel importation of its products into Japan from Germany based on its Japanese patent.

Under the Japanese laws, the copyright protection is given to expressions as opposed to ideas. While technical ideas are protected by the Patent Act, expressions having a low threshold of creativity are protected by the Copyright Act. When it comes to items such as package inserts for drugs or medical devices, it is generally believed that the Copyright Act does not protect informational contents on facts, but it protects the documents to the extent that such documents show some creativity beyond the information that they convey. Most likely, reproducing information in the package inserts does not constitute a copyright infringement.

Rights would not, probably, be exhausted by placing the digital product on a metaverse or other platform in another territory.

**Read this article on Lexology**

### Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Dawn raids by police are possible if the case is under criminal investigation.

Although an injunction that prevents the infringer from using the intellectual property is possible, freezing injunctions as to the infringer's assets are not provided in relation to IP infringement. Provisional attachment under the Civil Preservation Act and attachment under the Civil Execution Act are available for monetary claims, including a claim for compensation for damages based on IP infringement, both of which may be similar to freezing injunctions.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Injunctions and compensation for damages are available. Civil remedies designed for intellectual property do not include search orders and freezing injunctions.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Regarding personal data, the Act on the Protection of Personal Information (APPI) defines 'personal information' as information about a living individual by which the specific individual may be identified by name, date of birth or other description (including information that will allow easy reference to other information, thereby enabling the identification of the specific individual). Under the APPI, a business entity handling personal information must specify as much as possible the purpose for which the information will be used, and expressly inform the person of this purpose when the information is obtained directly from the person in writing, including electronically and, where such personal information has been obtained in some other way, disclose or notify the person of the purpose.

There is a category of sensitive personal information. This includes information relating to race, creed, social status, medical history, criminal record, the fact of being a victim of crime and other descriptions that require special consideration in handling to avoid unjustifiable discrimination, prejudice and other disadvantages. Obtaining sensitive information without the consent of the person is not permitted. The opt-out method is not available for sensitive personal information.

Anonymisation and pseudonymisation in accordance with the law may be used to avoid some regulation. Customer consent is not required to provide anonymised information

(called 'anonymously processed information') to a third party, provided that the items of the information included in the anonymised information and how to provide it to a third party are made public. It is not allowed to provide pseudonymised information (called 'pseudonymously processed information') to a third party even where customer consent has been obtained.

The 2020 amendments introduced new obligations for business operators providing information that is not personal data for the providing party but which would be considered personal data when received by the recipient. The amendments require the providing party in this case to (1) confirm that the principal has given consent to the acquisition by the recipient of such information (and, if the receiving party is located in a foreign country, that the principal has been provided with information on the system for protecting personal information in such foreign country and the protective measures to be taken by the receiving party); and (2) maintain records of this confirmation. On this basis, the acquisition of such consent from the principal is also obligated under the amendments.

Examples of information that may be considered personal data when received by the recipient would be identifier information such as cookies, and information exchanged on data management platforms that contains identifier information. However, information subject to these new obligations would not be limited to the foregoing; rather, the obligations will generally apply to the provision of 'personally referable information' in a situation where the information would be considered personal data when received by the recipient, because the recipient could easily collate the information with other information (such as the name of the principal) to identify the principal.

## Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

No, under the APPI there are no requirements to register with any regulator to process personal data, or to appoint a data protection officer.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The APPI could apply to organisations outside Japan if the organisations have provided goods or services to persons in Japan and have acquired personal information relating to those persons and handle that personal information or anonymised information produced by that personal information in a foreign country. The 2020 amendments expand the scope of the provision on extraterritorial application to cover the entire amended APPI, and replace the stipulation on the cases to which the extraterritorial application provision applies in cases where a personal information-handling business operator handles personal information or personally referable information of a person in Japan, in relation to supplying goods or services to a person in Japan. Under the amendments, the requirement that personal

information must be acquired in relation to supplying goods or services to a person in Japan has been deleted and the new provision instead broadly covers situations where personal information is handled in relation to supplying goods or services to a person in Japan, regardless of the relevance to Japan at the time of acquisition.

Individuals residing outside Japan may be protected by the APPI if other requirements for protection are fulfilled.

There are no requirements to appoint a representative in relation to the application of the APPI.

## Bases for processing

### 35 What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

Under the APPI, there are no concepts corresponding to reasons or bases for processing personal data under the EU General Data Protection Regulation. Under the APPI, it is necessary to obtain data subjects' consent for third-party provision of personal data for exporting or transferring personal data to another jurisdiction.

## Data export and data sovereignty

### 36 Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

In principle, the APPI requires a transferor to obtain the prior consent of the principals to transfer their personal data to a third party located in a foreign country. The principals' consent to overseas data transfers is not necessary if either of the following conditions is met:

1 the foreign country is specified in the enforcement rules as a country having a data protection regime with a level of protection equivalent to that of Japan; or
2 the third-party recipient implements technological and organisational measures for data protection that comply with the obligations corresponding to the obligations of a business operator handling personal information (ie, data controller) under the APPI.

For item (1), as at the time of writing, the enforcement rules have listed only EEA countries and the UK as such foreign countries.

For item (2), under the enforcement rules, the standards of the data protection system that a third-party recipient outside Japan must meet are either of the following:

1 there is assurance, by appropriate and reasonable methodologies, that the recipient will treat the disclosed personal data in accordance with the principles of the requirements for handling personal data under the APPI; or
2 the recipient has been certified under an international arrangement, recognised by the Personal Information Protection Commission (PPC), regarding its system of handling

personal data (to date, the only PPC-recognised international arrangement is the APEC Cross-Border Privacy Rules System).

Under the cross-border transfer guidelines for the APPI, 'appropriate and reasonable methodologies' in item (a) above include agreements between the disclosing party and the recipient, and inter-group privacy policies, which ensure that the recipient will treat the disclosed personal information in accordance with the principles of the APPI.

In addition to the above requirements, the APPI will require:

- business operators that purport to provide personal data to a foreign third party upon the principal's consent to provide information on the system for protection of personal information in such foreign country, as well as information on protective measures to be taken by such third party, to the principal in advance; and
- business operators that have provided personal data to a foreign third party without the principal's consent (as permitted in the APPI) to take necessary measures to ensure that such third party will continuously implement protective measures for the provided personal data, and to provide the principal with the relevant information upon request.

Also, there are no data sovereignty or national security rules that require data, data servers or databases to remain in Japan.

## Sale of data to third parties

### 37 May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

This type of sale of personal data may be possible if the consent of the website users has been obtained. Alternatively, the anonymously processed information as defined in the Act on the Protection of Personal Information may be used, although some obligations under the law are still imposed when making and using anonymously processed information.

No particular liability for such a sale is provided under the law, but general civil liability should apply to the seller and buyer in the case of, for example, improper disclosure of personal data.

## Consumer redress

### 38 What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Under the APPI, an individual is entitled to the following rights against a business operator handling personal information:

- to demand disclosure of his or her personal data;
- to demand correction of his or her personal data if such data is incorrect; and

- to demand cessation of utilisation, or deletion, of his or her personal data if the personal data is used beyond the scope necessary to achieve the purpose of utilisation or it was obtained unjustifiably.

Additionally, a general civil remedy is available, for example, in the case of improper disclosure of personal data.

These rights are not limited to Japanese citizens and they extend to foreign individuals in Japan.

### Non-personal data

**39** | Does the law in your jurisdiction regulate the use of non-personal data?

There are no applicable laws or rules concerning collection and utilisation of non personal data. Several guidelines have been published for the protection and utilisation of personal data and non-personal data. To promote fair contracts for sharing and utilising personal data and non-personal data, the Ministry of Economy, Trades and Industry published the Contract Guidelines on Utilisation of AI and Data. Those guidelines explain the key legal issues when entering into contracts for data sharing and utilisation with actual model clauses.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** | Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

The 2021 Japan tax reform made certain fundamental revisions to the Act on Utilisation of Telecommunications Technology in Document Preservation, etc., including changes to the preservation of transaction information sent and received electronically.

Currently, preservation in hard-copy format for transaction information sent and received electronically is permitted as an alternative to preserving such data electronically. However, for transaction information that is sent and received electronically on or after 1 January 2022, the option for hard-copy preservation was abolished, and preservation is required in the form of electromagnetic records (ie, electronic data).

The Act on Specified Commercial Transactions requires provision of certain documents in paper form, and the government continues to consult about permitting provision of such documents in electronic form.

The Act on Utilisation of Telecommunications Technology in Document Preservation, etc Conducted by Private Business Operators, etc permits storage of various documents and records in electronic form. Also, the Act requires storage of electronic books in the electronic format when receiving them in an electronic format, and storage of electronic books in the scanned format when dispatching them in an electronic form.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

The tax laws require records related to tax to be kept for seven years. Also, various documents related to internal company administration should be kept for several years.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

There is nothing specific to this jurisdiction. The usual measures should be taken, such as:

- updates of the operating system and other software;
- use of anti-virus software;
- regular backups;
- use of passwords;
- access limitation;
- limitation of device to be used; and
- restriction of unsafe website viewing.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Under the Act on the Protection of Personal Information (APPI), a report to the data protection authority (the Personal Information Protection Commission (PPC)) and notification to affected data subjects are mandatory in specific cases, as outlined below.

A digital business entity or other business entity handling personal information needs to submit a report to the PPC if any of the following data breach incidents (including leakage, loss or destruction of personal information) occurs, or is likely to have occurred:

- data breach containing sensitive personal information;
- data breach that is likely to harm an individual's property;
- data breach that is caused by malicious actions (for example, in the case of ransomware attack); or
- data breach that involves over 1,000 data subjects.

Reports to the PPC must be submitted twice. An entity must, when it becomes aware of data-breach incidents, immediately (ideally within three to five days) report the incident to the PPC. Thereafter, in addition to the first report, the entity must file a second report within 30 days (or 60 days, depending on the type of data breach) of the day of recognition of the data breach.

In addition to the data breach report to the PPC, an entity must notify the incidents to each data subject promptly. If it is impossible to contact data subjects for any reason, then the entity must take alternative measures. Unlike the reports to the PPC, there is no specific time limit for notifying data subjects. The APPI requires the relevant entity to notify the personal data breach to data subjects immediately, according to the circumstances. Therefore, an entity needs to judge the timing of notification on a case-by-case basis. For example, the official APPI guidelines state that if the details of the personal data breach are still unclear and there is a risk that providing notification based on this insufficient information will confuse the data subjects, then the entity does not need to provide notification of that information to data subjects.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Where the authorities have a warrant issued by a court, or a business entity is obliged to disclose data to the authorities under Japanese laws and regulations, the authorities may request the business entity to disclose data to them.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Horse racing, boat racing, bicycle racing, motorcycle racing, lottery and toto (football lottery) are permitted for certain entities. There is no prohibition on or penalty against the online purchase of betting tickets for those activities. After the amendment to the Lottery Ticket Act in April 2012, lottery tickets may be purchased via the internet.

Online gaming businesses, including online poker and online casino games, are prohibited in Japan.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Online casinos and betting websites are currently not allowed. It might be punishable to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

One of the key legal issues relevant in outsourcing is the actual enforceability of the outsourcing agreement. If Japanese companies outsource the provision of services, those companies will commonly insert provisions into the outsourcing agreement limiting their liabilities and reserving their rights as much as possible.

However, if, for example, defects in products or leakage of information caused by the outsourced company leads to damage or injury to consumers in Japan, the outsourcing company may not be totally exempt from liability under the Civil Code or Product Liability Act even if its liabilities are limited in an agreement. In addition, outsourced companies outside the jurisdiction may be able to file an application in their own jurisdictions for IP rights that are almost the same as those licensed by the outsourcing companies or generated by the outsourced companies on the basis of the activities provided in the agreement.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

There are no particular digital business services (including digital financial services) that cannot be outsourced in Japan.

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

The Subcontract Act requires inclusion of certain items in outsourcing contracts, such as the amount of subcontract fee and when the subcontract fee is paid. The Act on the Protection of Personal Information does not require any particular terms to be included in outsourcing contracts.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

There is no direct rule or regulation regarding employees who previously carried out services that have been outsourced. However, under the Japanese Labour Contract Act, dismissal is strictly restricted for a company during normal economic conditions, and so usually cannot be justified on the grounds that services were outsourced. In such cases, the company may have to maintain employment by providing other jobs for employees by transferring them to a different position or location of work.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

Under Japanese law, there are no rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence (AI), machine learning, automated decision-making or profiling.

#### Regulation on AI

Japan has no regulations that generally constrain the use of AI. According to the AI Governance report version 1.1, published by the Ministry of Economy, Trade, and Industry (METI) in July 2021 and describing Japan's AI regulatory policy comprehensively, legally binding horizontal requirements for AI systems are unnecessary in Japan since regulations face difficulties in keeping up with the speed and complexity of AI innovation. A prescriptive, static, and detailed regulation in this context could stifle innovation. Therefore, the report concludes that the government should respect business sectors' voluntary efforts for AI governance while providing nonbinding guidance to support or lead such efforts. The guidance should be based on multistakeholders' discussions and be continuously updated in a timely manner. This approach is called 'agile governance', which is Japan's basic approach to digital governance.

Sector-specific regulations do not prohibit the use of AI, but rather require business sectors to take appropriate measures and disclose information about risks. For example, the Digital Platform Transparency Act imposes requirements on large online malls, app stores, and digital advertising businesses to ensure transparency and fairness in transactions with business users, including the disclosure of key factors determining their search rankings. Furthermore, the Financial Instruments and Exchange Act requires businesses engaging in algorithmic high-speed trading to register with the government, and establish a risk management system and maintain transaction records.

There are a few laws that do not directly legislate AI systems but that still remain relevant for AI development and use. The Act on the Protection of Personal Information (APPI) describes the key mandatory obligations for organisations that collect, use or transfer personal information. The amendments to the APPI in 2022 introduced the concept of pseudonymised personal information. This new concept is expected to encourage businesses to use more data for AI development.

### Regulation promoting the use of AI

While the abovementioned regulations on AI are often discussed, regulations promoting the use of AI are important to maximise AI's positive impact on society. Legislators in Japan have used regulatory reform to promote the use of AI in a variety of contexts.

Also, in 2020, the revised Road Traffic Act and Road Transport Vehicle Act came into force, allowing Level 3 automated driving on public roads. New amendments that allow Level 4 automated driving came into effect on 1 April 2023. In the financial sector, the Installment Sales Act was revised in 2020 to enable a 'certified comprehensive credit purchase intermediary' to determine credit amounts using data and AI. Previously, credit card companies had to use a statutory formula taking into account annual income, family structure and other factors when assessing credit amounts.

Furthermore, for plant safety, a 'super certified operator' system was established in 2017 under the High Pressure Gas Safety Act. Plant operators must stop their operations and conduct safety inspections once a year, but operators certified as having advanced safety technology utilising AI and drones are allowed to conduct safety inspections without interrupting operations for up to eight years.

Several guidelines have been published for data sharing and utilisation for AI development. The Guidebook on Corporate Governance for Privacy in Digital Transformation and the Guidebook for Utilisation of Camera Images, both jointly developed by METI and the Ministry of Internal Affairs and Communications, provide guidelines on how to handle privacy data in terms of not only complying with APPI but also taking appropriate measures based on communication with stakeholders.

## IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

The training data sets and other data associated with artificial intelligence and machine learning are not protected by intellectual property rights under Japanese law. The Copyright Act was amended in 2017 to promote the use of data in machine learning. The amendments clarified that downloading or processing data through the internet or other means to develop AI models does not infringe copyright of existing copyrighted works. In addition, the 2019 amendments to the Unfair Competition Prevention Act protect shared data with

limited access, which typically entails data sets sold for a fee. The unauthorised acquisition or misuse of such shared data is subject to claims for injunction or damages. These unique provisions will help AI developers use more data for AI learning while protecting the appropriate interests of the data holders. Also, there are no particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems. The government has started legal discussions on new limitations on using existing copyrighted works for AI learning, based on the emergence of generative AI.

There are no particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems, and the government has started legal discussions on this issue too.

## Ethics

### 53 Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

In 2019, the government published the Social Principles of Human-Centric AI (Social Principles) as principles for implementing AI in society. The Social Principles set forth three basic philosophies: human dignity, diversity and inclusion, and sustainability. It is important to note that the goal of the Social Principles is not to restrict the use of AI in order to protect these principles but rather to realise them through AI. This corresponds to the structure of the Organisation for Economic Cooperation and Development (OECD) AI Principles, whose first principle is to achieve 'inclusive growth, sustainable development and well-being' through AI.

To achieve these goals, the Social Principles set forth seven principles in relation to AI: (1) human-centric, (2) education and literacy, (3) privacy protection, (4) ensuring security, (5) fair competition, (6) fairness, accountability and transparency, and (7) innovation. It should be noted that the principles include not only the protective elements of privacy and security but also the principles that guide the active use of AI, such as education, fair competition and innovation.

As to guidance for private parties, the government provides various tools to help companies voluntarily implement appropriate AI governance measures. METI's Governance Guidelines for Implementation of AI Principles summarised the action targets for implementing the Social Principles and how to achieve them, with specific examples. It explains processes to establish and update AI governance structures in collaboration with stakeholders according to an agile governance framework.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Online products transmitted domestically are subject to consumption tax, and as such they are treated the same as non-online products traded domestically. However, online products transmitted from foreign countries are not subject to consumption tax, while non-online products imported from foreign countries are subject to consumption tax.

The Japanese government has maintained a policy of not imposing tariffs on the sale of online products and, as such, online products are treated differently from non-online products imported from foreign countries.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Tax liabilities generally arise in the jurisdiction in which income is obtained.

So, even if operators incorporated in Japan place their servers outside Japan, that placement does not generally have any effect on tax liabilities and those operators will generally be subject to tax liability in Japan. However, if operators incorporated outside Japan place their servers in Japan, they will not generally be subject to tax liability in Japan as long as the source of the income remains outside Japan.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The Act on Preservation of Electronic Books requires storage of an electronic invoice in the electronic format when receiving an electronic invoice, and storage of an electronic invoice in the scanned format when dispatching an electronic invoice. There are no requirements to provide copies of e-invoices to a tax authority or other agency under Japanese law.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

No. The Intellectual Property High Court specialises in IP disputes such as those arising from patents and copyrights, and therefore deals with online digital patent and copyright disputes, but that court is not necessarily a specialist court for online or digital disputes.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

Arbitration or mediation may be used to resolve online or digital disputes. Courts may also handle mediation proceedings for such disputes. The Software Information Centre provides ADR for software-related disputes. Most of those cases are related to system development transactions.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The government is continuing to integrate various guidelines for artificial intelligence (AI)-related businesses and intends to publish the new integrated guidelines later in 2023. The government presented draft action guidelines for the development and utilisation of generated AI at the AI Strategy Council in April 2023, with a focus on requiring businesses to disclose AI specifications and measures to prevent the utilisation of AI for criminal purposes. The draft was presented to the G7 countries, with the aim of reaching an agreement by the end of 2023 through coordination by a specialised team established in July 2023.

The responsibilities common to the development stage and the provision and use stage of generated AI are expected to be basic, such as complying with existing laws, not causing human rights violations and respecting democratic values. The content of the responsibilities to be fulfilled by businesses at each stage will be worked out in the future. There is a proposal to require developers above a certain size, such as Open AI and Google in the United States, to disclose what data and technologies were used to develop generative AI and how the input information leads to the output of generative AI.

# Anderson Mōri & Tomotsune

Takashi Nakazaki takashi.nakazaki@amt-law.com

1-1-1 Otemachi Otemachi Park Building, Chiyoda-ku, Tokyo 1008136, Japan
Tel: +81 3 6775 1000
www.amt-law.com

# Luxembourg

Anne-Marie Ka, Vincent Semideï and Pierre van der Woude
Brucher Thieltgen & Partners

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The Luxembourg government has taken a proactive attitude and approach towards digital business. In 2014, the government launched the Digital Luxembourg Action plan. It is still investing in enhancing the digital transformation change with its Electronic Governance 2021–2025 strategy. According to the European Commission, Luxembourg ranks third out of 35 countries in terms of maturity of digital public services within the 'eGovernment Benchmarks 2022'.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

The main legislation for digital content and services are:

- the law dated 14 August 2000 on e-commerce, as amended (E-commerce Law);
- the Civil Code;
- the Commercial Code (for business-to-business transactions);
- the Consumer Code (only for B2C transactions);
- the law dated 1 August 2018 concerning the organisation of the National Commission for Data Protection and the general system on data protection, as amended (Data Protection Law);
- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, as amended (eIDAS Regulation); and
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended (GDPR).

The secondary legislation consists in several punctual act for a specified sector or subject such as, for example:

- the law of 18 April 2001 on copyright, related rights and databases, as amended (Copyright Law);
- the law dated 30 May 2005 concerning the specific provisions for protection of the individual in respect of the processing of personal data in electronic communications sector, as amended (E-communication Law);
- the law dated 18 July 2014 on cybercrime, as amended (Cybercrime Law);
- the law dated 25 July 2015 on electronic archiving, as amended (Archiving Law);
- the law dated 23 December 2016 on end-of-season sales and sidewalk sales and misleading and comparative advertising, as amended (Advertising Law);

- the law dated 28 May 2019 implementing Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information system across the Union, as amended (NIS Law); and
- the law of 10 November 2009 on payment services, on the activity of electronic money institution and settlement finality in payment and securities settlement systems, as amended (Payment Services Law).

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

Irrespective of the area, the process for passing regulations in Luxembourg is the same and comprises different steps. Either the Chamber of Deputies or the government may propose a bill.

Depending on the particular subject, a bill of law is drafted by the competent ministry. Various Ministry could also act together such as the Ministry of Digitalisation, the Ministry of Economy or the Ministry of Communications and Media.

In order to come into force, a bill of law, after going through the process of opinions and discussions, must pass within the Chamber of Deputies, be enacted by the Grand Duke and published in the Official Journal of the Grand Duchy of Luxembourg.

Depending on the area, various authorities are responsible for the supervision and the regulations:

- Luxembourg Institute of Regulation for telecommunications, energy, postal services...
- Financial Sector Supervisory Commission for financial services;
- Insurance Commissariat for insurance services; and
- National Data Protection Commission for data protection.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Jurisdiction clauses are valid and recognise in Luxembourg as long as they are not contrary to any mandatory provision of national or international law.

The parties' freedom to choose a court is in some cases restricted by statute. For instance, the Consumer Code provides that clauses intended to deprive consumers of their right to bring actions in the ordinary courts are null and void.

In the absence of jurisdiction clause, claimants may bring an action either in the place where the defendant lives or, depending on the nature of the contract, the place where the goods are delivered or the services are performed.

### Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

In Luxembourg, access to online business is not subject to any prior authorisation. However, any commercial activity requires a licence to operate without distinction as to the nature of the content or services. This licence is granted by the Ministry of Economy, which requires a physical presence in Luxembourg (ie, a fixed place of business) and checks the professional integrity of the applicant.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Yes. Digital contract formation is subject to the general rules provided by the Civil Code (capacity, consent, lawful purpose and consideration).

Additional requirements are provided by the E-commerce Law and the Consumer Code, which are mainly linked with prior information obligations. The E-commerce Law excludes different types of contracts, such as contracts that create or transfer real estate ownership or contracts governing by family law or inheritance law.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Regulation (EC) No. 593/2008 on the law applicable to contractual obligations (Rome I) is applicable to digital contracts.

For business-to-business contract, the principle is that the parties can choose the law applicable to their contract. If no choice of law has been specified, the applicable law is determined pursuant to various rules provided in Rome I.

For business-to-consumer contract, the governing law is the law of the country where the consumer has his habitual residence, provided that the seller directed its activity to that country. The parties are free to choose a different governing law but the consumer will continue to benefit of the provisions of his national legislation if they are more favourable than the provisions of the chosen governing law.

The contract should be concluded in a language understood by the parties.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Pursuant to article 1322-1 of the Civil Code, any signature may be either handwritten or electronic and defines the latter as a set of data, inseparably associated with the deed, which guarantees its integrity, identifies the signatory and expresses their consent to the deed.

Pursuant to article 1317-1 of the Civil Code, authenticated deeds and titles, such as notarial deeds, can also be drawn up and signed electronically using a specific procedure.

Not all e-signatures will have the same probative value as handwritten signatures. The eIDAS Regulation distinguishes between the simple electronic signature, the advanced electronic signature and the qualified electronic signature.

Digital or e-signature providers do not have to be registered or licensed. However, the member states of the European Union and European Economic Area publish trusted lists of qualified trust service providers.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

There are no special forums for dispute resolution or remedies for the breach of digital contracts. The courts will apply the classical rules on the allocation of jurisdiction. However, any dispute concerning a contract concluded between a professional and a consumer can be settled out of court by referring the matter to a consumer mediator.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

Products and services are regulated by sectoral authorities responsible for ensuring compliance with specific provisions. The Financial Sector Supervisory Commission (CSSF)

regulates all matters concerning the marketing of financial instruments to consumers or professionals.

Pursuant to the Consumer Code, consumer credit agreements or property loan agreements are subject to additional information obligations.

## Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

The notion of digital assets presents a great diversity and if the majority of tokens are not subject to any specific legislation (ie, cryptocurrency), the CSSF considers that those that are to be considered as falling under the conditions of financial instruments or electronic currencies are subject to the relevant legislation for each of these matters.

Payments institutions, electronic money institutions and account information service providers are regulated by the CSSF.

Virtual assets are also governed by the Law of 12 November 2004 on the fight against money laundering and terrorist financing (AML Law) and the Payment Services Law.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Virtual currencies are not currencies and fundraising through public offerings in the form of so-called initial coin offerings are not regulated and do not enjoy the support of a central bank or deposit guarantee.

However, the use of Distributed Ledger Technology (DLT) in the financial market was introduced into Luxembourg law with the law of 1 March 2019, which amended and extended the scope of the law of 1 August 2001 on the circulation of securities, allowing account holders to hold securities accounts and register securities by means of secured electronic registration mechanisms, including distributed electronic registers or databases.

Similarly, the law of 22 January 2021 allows credit institutions and investment firms to operate a central account keeper to maintain issuer accounts through DLT.

Virtual asset service providers have to register with the CSSF, whose role will be limited solely to AML/CFT registration, monitoring and enforcement.

### Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Electronic payment systems are governed by the Payment Services Law. This law imposes a number of requirements, including compliance with a licensing procedure, central administration and infrastructure.

The law of 20 July 2018 has implemented the revised Payment Services Directive (EU) 2015/2366 by amending the Payment Services Law. It enables personal and business customers to share their data securely with banks and third parties, allowing them to compare products, initiate payments and request account information.

### Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

The AML Law provides that a professional may, under certain conditions, use a third party to meet their KYC and AML due diligence obligations. The final responsibility cannot be delegated, the professional will always be directly responsible for its subcontractor.

It should be noted that certain activities, which may also be related to customer due diligence for AML/CTF purposes, may only be carried out by licensed financial sector professionals, for example, activities related to customer records management or communication services.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** 4.1.1. What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

The infrastructure for registering domain names with the national extension '.lu' is managed by the Restena Foundation. The rules are mentioned into their domain name charter.

Domain names must be available and must not be identical or confusingly similar to a trademark to which another person has any rights.

There is no obligation to be a resident to apply for a Luxembourg domain.

There is no specific legislation regarding the use of URLs to direct users to websites, online resources or metaverses.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

A domain name is registered in the name of the holder on a 'first come, first served' basis. The holder becomes the owner of the domain name.

Under the Benelux trademark convention, a domain name can be registered as a trademark if it fulfils the requirements.

If a trademark holder considers that a recently filed trademark infringes their previously registered trademark, they can file a notice of opposition. The opposition must be based on an earlier trademark right afforded through a Benelux or EU trademark.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

Advertising Law prohibits misleading advertising and regulates comparatives advertising without distinguishing the medium used.

Pursuant to E-commerce Law, advertising must be made in a transparent way.

Criminal Code and Consumer Code also provide rules regarding advertising.

In addition, Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) prohibits gatekeepers from reusing a user's personal data for targeted advertising purposes without the explicit consent of the data subject.

Similarly, Regulation (EU) 2022/2065 of 19 October 2022 on a single market for digital services (Digital Services Act) imposes new obligations, in particular with regard to the transparency of profiling methods and tools, targeted advertising and content, and the prohibition of targeted advertising to minors on the basis of their personal data, or to any person on the basis of sensitive data (sex, political opinions or sexual orientation).

## Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

The E-commerce Law requests as a general rule, a clear, specific prior consent with the right to withdraw the consent at any time.

If the use of targeted advertising implies the processing of personal data, the General Data Protection Regulation will also apply. It provides additional rights for data subjects that form the subject of 'direct marketing', which includes targeted advertising and also in the case of profiling or automated decisions.

For consumers, specific rules are provided in the Consumer Code.

## Misleading advertising

**19** Are there rules against misleading online advertising?

The Advertising Law prohibits misleading and restricts comparative advertising (online and on premises advertising). The advertiser has to prove the respect of the different conditions provided by the Advertising Law.

Wrong consumer advice or recommendations can also be considered as misleading advertising.

## Restrictions

**20** Are there any digital products or services that may not be advertised online?

As a general rule, anything that is illegal or contrary to public policy (eg, the human body, drugs or weapons, signs and symbols that might provoke a rebellion or any public order problems) cannot be advertised.

Similarly, the sale and marketing of products or services subject to a specific authorisation regime (eg, alcohol, tobacco or medicines) is subject to limitations.

The Consumer Code also regulates advertising for a number of contracts (eg, credit agreements or mortgage agreements).

## Direct email marketing

**21** What regulations and guidance apply to email, SMS and other direct marketing?

Regarding unsolicited commercial communications, the E-commerce Law requests as a general rule, a clear, specific prior consent with a right to withdraw the consent at any time. Some exceptions are possible when for example, similar products or services are offered by the same seller, with a possible opt-out.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Pursuant to the E-commerce Law, any service provider through which information transits may be held liable. This law provides for several exemptions from liability depending on the type of storage of the information (simple transport, caching or hosting), as well as, in certain cases, monitoring measures to limit the risks of possible infringements.

The liability of any person who processes information for publication, regardless of the medium, is subject to a duty of accuracy and truthfulness in relation to the facts communicated, in accordance with the Law of 8 June 2004 on freedom of expression in the media (Freedom Law). This law has a broad scope, as it applies equally to content provider, broadcaster and publisher, whose definitions are equally broad.

The Digital Services Act adds a series of obligations to online platforms to limit the distribution of illegal content and products online (racist attacks, child pornography images, sales of drugs and counterfeit goods).

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

A digital platform or online content provider is liable for the content published. It can be exempted from liability if it:

- only hosts content at the users request and cannot amend the content; and
- is unaware that it hosts illegal content or activities.

Upon knowledge of the unlawful content, the service provider must remove it promptly or make it impossible to access.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Subject to the respect of the freedom of speech, an online content provider or ISP can remove or make inaccessible online content without court authorisation.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

According to the Copyright Law, the structure of the database (ie, its container) can be protected by copyright against unlawful copying when the choice or arrangement of the elements materialises an original intellectual creation. The author of the database then has copyright on the structure of the database but this does not allow them to prohibit certain types of acts, reproductions or uses.

The content of the database (among other data) can be protected by an exclusive right for the benefit of the person who initiated the creation of the database under certain conditions (substantial qualitative or quantitative investment).

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Luxembourg does not have any general national legislation that would prohibit reference to third-party sources as such. However, the creation or hosting of a hypertext link to a third-party site, without the authorisation of the operator may constitute an infringement of copyright or trademark.

The CJUE has ruled on the use of hyperlinks (C-160/15). In light of the CJUE case law, there is no apparent distinction between a hyperlink to a third-party site and a hyperlink to digital content within the website itself.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

It will be necessary to verify the nature of the rights that exist on these contents (eg, copyright, licences or IP rights) and determine if the authorisation from the author or holder of the rights was obtained, in order to be able to use or reproduce them.

### Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Trademark protection in the metaverse, in particular the comparison of the use of a trademark to be used for identical or similar goods and services in order to invoke a prohibition, raises difficulties of assessment.

The new version of the Nice Classification includes downloadable image files, downloadable music files and downloadable digital files authenticated by non-fungible tokens (NFT). In

this regard, the European Union Intellectual Property Office already recommends, when registering a virtual goods trademark, to specify which type of goods or service is concerned.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

The theory of exhaustion of rights or the first-sale doctrine is known in Luxembourg law by European law and applicable by virtue of the Benelux Convention on Intellectual Property of 25 February 2005, as amended, and the Copyright Law.

Its application follows European case law in this area and still raises many discussions in the digital field. In practice, the resale of second-hand software is possible, subject to certain conditions, in particular the removal of the original copy of the software from the first purchaser.

Its application in the metaverse will therefore vary according to the asset concerned and its qualification in the metaverse (eg, software, intangible copy of the physical asset), or its mode of transmission (eg, licence, sale).

In the current state of technology and law, intellectual property owners will have to be vigilant about the contractual framework and more specifically about the general conditions of use of the dematerialised asset.

In the context of the metaverse, the question of exhaustion of rights is not yet clear and, as of today, has not been discussed before the Luxembourg courts.

## Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

No specific national legislation provides the authorities with the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement.

For '.lu' domain names, there is a judicial procedure that allows to freeze temporarily the use of a '.lu' domain names if a valid court action has been brought against the domain name holder.

## Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

IP owners have several remedies under the Benelux Convention and the Copyright Law.

The actions aim either to repair the damage or to stop the infringement. These include compensation for the damage suffered, withdrawal of the products from the market, return of the infringing goods or means used to the owners, allocation of the benefits derived from the infringement and publication of the decision establishing the infringement. It does not include search orders and freezing injunctions unless it involves criminal behaviour.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Data Protection Law refers to the definition of personal data in the General Data Protection Regulation (GDPR) and sets out the measures for processing such data (eg, transfer outside the EU, specific security measures, etc).

Personal data is defined as any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data or an online identifier.

Additional rules apply to the processing of specific categories of personal data such as sensitive personal data which are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed solely to identify a human being, health-related data, data concerning a person's sex life or sexual orientation, which in principle may not be processed, apart from certain exceptions.

Although anonymous personal data does not fall under the scope of the GDPR, pseudonymous data are considered as personal data.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Parties involved in the processing of personal data does not have to register with any regulator to process personal data. However, it will have to appoint a data protection officer, whether it is a controller or a processor, if its core activities involve processing of sensitive data on a large scale or involve large-scale, regular and systematic monitoring of individuals. In that respect, monitoring the behaviour of individuals includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

Data Protection Law and the GDPR apply to:

- data controller and data processors located in Luxembourg or in another member state of the European Economic Area; and
- processing of personal data of data subjects based in the European Economic Area by a controller or a processor outside the European Union, where the processing activities relate to the offer of goods or services or the monitoring of data subjects' behaviour.

In the case of a cross-border processing, the Luxembourg authority could be designed as the lead supervisory authority.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

The lawful grounds for processing personal data are set out in article 6 of the GDPR.

These are:

- the consent of the individual;
- performance of a contract;
- compliance with a legal obligation;
- necessary to protect the vital interests of a person;
- necessary for the performance of a task carried out in the public interest; or
- in the legitimate interests of company or organisation (except where those interests are overridden by the interests or rights and freedoms of the data subject).

Exporting or transferring of personal data to another jurisdiction may be necessary among others for international trade and international cooperation, outsourcing of services to external providers, using online IT services, cloud-based services, remote access services or global HR databases.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Transfers of personal data to third countries or international organisations should be done in full compliance with the following rules:

- the recipient's country has received an adequacy decision from the European Commission;
- the sender and the recipient are within separate companies, and are bound by a contract containing standard data protection clauses;
- the sender and recipient are within different entities of a multinational corporation or corporate group within which binding corporate rules have been agreed; and
- the transfer is an exceptional event and the sender can rely on one of the GDPR's derogations.

## Sale of data to third parties

### 37 May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

The GDPR does not prohibit the sale or rental of personal data (eg, customer databases), subject that the data may only be used for the purposes for which it was collected. The data subject must be informed of the purposes of the collection, including the subsequent sale. As a result, data stored for other purposes (eg, administrative or accounting) cannot be transmitted.

In the case of opposition or refusal of consent, the data must be deleted and excluded from the scope of the sale.

The parties shall respect the GDPR's requirements and are jointly responsible for ensuring the lawfulness of the transfer and the implementation of appropriate safeguards to protect the data.

The purchaser would have to inform individuals of the sale of the file as soon as possible, verify the existence of consent from the data subject, and put in place measures to respect the rights of individuals offered by the GDPR (eg, the right to object and the right to be forgotten).

The Data Governance Regulation 2022/868 facilitates the sharing of data between different sectors and industries within the EU under strict conditions of appropriate safeguards to protect personal data.

No specific rules exist for the metaverse.

## Consumer redress

### 38 What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

The rights are as follows:

- right to information;
- right of access;
- right to rectification;

- right to erasure;
- right to restriction of processing;
- right to data portability;
- right to object; and
- right to not be subject to automated decision-making.

These rights applied to all data subjects based in the European Economic Area.

### Non-personal data

**39** | 8.8.1. Does the law in your jurisdiction regulate the use of non-personal data?

Regulation (EU) 2018/1807 of 14 November 2018, applicable in Luxembourg, provides a general framework to ensure the free movement of non-personal data within the European Union, as well as rules on the availability of data for competent authorities, the development of a cooperation procedure between member state authorities, and data porting.

In addition, the framework for requests for access by foreign authorities and for transfers of non-personal data is the subject of two proposed regulations, the Data Act and the Data Governance Act, which will provide protection models in line with those of the GDPR.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** | Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Pursuant to the E-commerce Law, the following documents must be formalised exclusively in original paper form:

- contracts that create or transfer rights over real estate, except for rental rights;
- contracts for which the law requires the intervention of courts, public authorities or professions exercising public authority;
- contracts of sureties and guarantees provided by persons acting for purposes that are not part of their professional or commercial activity; and
- contracts relating to family law or inheritance law.

The law of 7 July 2023 implements Directive 2019/1151 of 20 June 2019, which amends Directive 2017/1132 with regard to the use of digital tools and processes in company law. It sets up the digitalisation of the notarial profession.

Directive 2017/1132, as amended by Directive 2019/1151, requires that authentic instruments for the formation of companies falling within its scope can be drawn up in electronic format, and that they can be drawn up remotely.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

There are various retention periods applicable under Luxembourg law.

The following are some examples:

- contracts with customers must be kept for a period of 10 years from the end of the contractual relationship to which the documents relate; and
- accounting documents and supporting documentation must be kept for 10 years from the end of the accounting year to which the documents relate.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

The NIS Law provides requirements for security measures and notification of serious incidents.

From a data protection perspective, the General Data Protection Regulation (GDPR) requires companies acting as controller or processor to adopt technical and organisational measures necessary to ensure the security of personal data, such as pseudonymisation and encryption or measures ensuring the timely restoration of availability and access to personal data after an incident.

The integration of ISO standards, in particular the technical specification ISO/IEC TS 27110 and ISO/IEC TS 27100, into internal procedures can be an important asset in the field of digital security.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

No specific legislation applies to digital business in the case of data breach.

The GDPR requires the controller to notify the breach, as soon as possible and, if possible, no later than 72 hours after becoming aware of the breach.

**Read this article on Lexology**

The authority in Luxembourg is the National Data Protection Commission.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person, the controller shall notify the data subject of the personal data breach as soon as possible. The data subject shall be notified by a communication in clear and simple terms, setting out the nature of the personal data breach and containing at least: the name and contact details of the Data Protection Officer or other point of contact from whom further information can be obtained; a description of the likely consequences of the personal data breach and the measures taken or to be taken to remedy or mitigate the personal data breach.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

The interception of data and their retention by the authorities are governed by several laws and regulations in Luxembourg. Public authorities can intercept data and even require telecommunication service providers to give them access to certain data, in the context of a flagrant crime, the safeguarding of state security, defence, public safety and for the prevention, investigation, ascertainment and prosecution of criminal offences.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Luxembourg laws are not clear to the regime applicable to online gambling.

The licensing regime for online gambling is subject to the same rule as land-based gambling.

To date, the National Lottery is the only entity licensed to provide online gambling services in Luxembourg.

The legal gambling age in Luxembourg is 18.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Luxembourg does not currently intend to impede the activities of service providers established in other EU member states where they are authorised to provide their services.

The advertising of gambling is generally allowed but must not target minors. The advertising of land-based and online gambling is not otherwise subject to specific restrictions or regulations. However, the general regulations regarding faithful, trustworthy and honest commercial advertisements are applicable to gambling.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

The main issues around outsourcing are generally related to IT security and the transfer and confidentiality of data, in particular when it includes personal data.

Environmental, social and governance issues are also becoming increasingly important in the service provider relationships.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

CSSF circulars 22/806 and 22/811 provide a framework for the outsourcing of certain activities in Luxembourg, within the European Union or a third country, or both, for regulated actors in the financial sector (eg, banks, payment institutions, GFIA (in certain cases), PFS, etc).

These entities must assess all the activities they outsource and determine through formal documentation their level of criticality to determine those that will require special treatment, as well as the entity's outsourcing policy. This list of critical activities must be notified to the CSSF. Entities must also put in place an exit plan, regularly updated.

Not all services can be outsourced, for example, audit and internal control functions can only outsource operational tasks.

All outsourcing that implies a transfer of personal data must comply with the General Data Protection Regulation (GDPR).

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

CSSF circular 22/806 imposes a list of elements that must be contained in the outsourcing contract.

Pursuant to the GDPR, to the extent that the outsourcing results in the processing of personal data, a certain number of clauses are mandatory.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

In the case of termination of the employment contract, any employee can challenge the grounds of dismissal and obtain damages if the dismissal is considered as unfair.

Employee transfers or usage for outsourcing should comply with the rules on transfer of undertakings and the illegal lending of workers.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

To date, no specific rules and restrictions apply. However, Luxembourg announced a set of measures to be implemented with respect to ensure that legal and ethical guidelines are implemented to protect fundamental rights and freedoms.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Luxembourg does not have specific laws exclusively dedicated to intellectual property and AI or machine learning, these technologies are subject to the existing legal framework for intellectual property, data protection and contract law.

In terms of intellectual property, copyright ownership of AI-generated works remains unclear and depends on factors such as the involvement of human creators in creating the work.

In general, it is possible that data may be protected by intellectual property rights, such as copyright or database rights, if it meets the conditions for protection under the relevant laws.

The European Union has taken up these issues to advocate a standardised intellectual property regime, in particular the European Parliament Resolution of 20 October 2020 on intellectual property rights for the development of technologies related to artificial intelligence (2020/2015(INI)) or the European Parliament Resolution of 3 May 2022 on artificial intelligence in the digital age (2020/2266(INI)), but for the time being, Luxembourg does not have a specific rule on the subject.

### Ethics

**53** 13.3.1. Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

In an official statement, the government of Luxembourg indicated it is committed to promoting the Ethics Guidelines for Trustworthy AI published by the Expert Group on Artificial Intelligence set up by the European Commission. The guidelines list seven requirements that trustworthy AI should meet, including, but not limited to, transparency, diversity, non-discrimination, fairness and accountability.

The guidelines do not however constitute binding legislation. In this respect, the EU has announced its MEPs are aiming to reach an agreement on a set of rules relating to AI by the end of 2023.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

All business activities whether online or not are subject to the ordinary tax rules, including corporate income tax, municipal business tax, net wealth tax and VAT, if the activity is carried out by a Luxembourg company or a Luxembourg branch of a foreign entity.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Under Luxembourg tax law, any income generated by business activities in Luxembourg is taxable in Luxembourg, as soon as the activity is located in Luxembourg or through a permanent establishment, regardless of where the servers or other IT infrastructure is located.

If a company places its servers outside its home jurisdiction in Luxembourg, it may nevertheless be subject to tax in Luxembourg, in that a computer server may qualify as a permanent establishment, if the servers are used in the course of the company's business activities in Luxembourg.

**Read this article on Lexology**

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The law of 16 May 2019 on electronic invoicing in the context of public procurement and concession contracts makes electronic invoicing mandatory in the context of public procurement.

Authenticated electronic invoices must be kept in their original form and be accessible during the entire invoice retention period.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no specialist courts or other venues in Luxembourg that deal with online or digital issues and disputes.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

The consumer mediator can be contacted for any dispute arising from a sale or service contract, including online or digital, for B2C conflicts and for domains not assigned to the four specialised entities (CLLV for travels, the Financial Sector Supervisory Commission for financial issues, the Luxembourg Institute of Regulation for Telecom Issues and Insurances Mediation).

The EU provides a specific tool when a dispute arises over an online purchase. A complaint can be lodged via the online dispute resolution (ODR) platform with an ODR body in any language and in any country of the EU.

The Civil and Commercial Mediation Centre is also one of the operators able to conduct a mediation for national and cross-border commercial litigations, including online disputes.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

Luxembourg will be impacted by the pending European legislation in the area of technology.

The main developments are as follows:

- IT resilience with the Digital Operational Resiliency Act;
- the NIS 2 Directive;
- the Digital Markets Act and The Digital Services Act, which will impact the major digital platform relations and Bigtech regulation;
- the AI Act, which is to be monitored as it would be applicable within 36 months of its entry into force;
- the eIDAS 2 Regulation, which will inevitably lead to significant operational changes for trust service providers; and
- the Data Act and the Digital Governance Act.


Anne-Marie Ka anne-marie.ka@brucherlaw.lu
Vincent Semideï vincent.semidei@brucherlaw.lu
Pierre van der Woude pierre.van-der-woude@brucherlaw.lu

16-18, Bd. Emmanuel Servais, BP 507 · L-2015 Luxembourg
Tel: +352 26 02 71
www.brucherlaw.lu

**Read more from this firm on Lexology**

**Read this article on Lexology**

# Malaysia

Tong Lai Ling and Jed Tan Yeong Tat*
Raja, Darryl & Loh

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The Malaysian government is committed to being agile, sustainable and progressive towards a vibrant digital economy. The government generally acknowledges the need to address digital content and services, digital transformation and doing business online and has been taking active steps and measures to address the same, for example:

- developing initiatives (MyDIGITAL) aimed at transforming Malaysia into a digitally enabled and technology-driven high income nation, and a regional lead in digital economy;
- raising cyber security awareness and taking steps to ensure that Malaysians have the skills and knowledge to combat cyberattacks;
- encouraging the building of a trusted, secure and ethical digital environment; and
- expanding the coverage and quality of internet in Malaysia through its national broadband initiatives.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

The following legislation (non-exhaustive) has general application and may apply to digital content and services, digital transformation and the conduct of business online:

- Electronic Commerce Act 2006;
- Consumer Protection Act 1999;
- Computer Crimes Act 1997;
- Personal Data Protection Act 2010;
- Communications and Multimedia Act 1998;
- Copyright Act 1987;
- Registration of Business Act 1956;
- Strategic Trade Act 2010;
- Contracts Act 1950;
- Trade Descriptions Act 2011; and
- Sale of Goods Act 1957.

Each of the above governs different aspects of digital content and services, digital transformation and the conduct of business online, the applicability of which may depend on the nature of the matter or transaction.

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The regulatory bodies are:

- in respect of digital content and services, internet access and telecommunications, generally the Malaysian Communications and Multimedia Commission;
- in respect of e-commerce, primarily the Ministry of Domestic Trade and Consumer Affairs; and
- in respect of personal data protection, the Department of Personal Data Protection.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

In determining the jurisdiction, Malaysian courts may consider the following:

- the choice of law in the terms governing the transaction (having regard to the doctrine of freedom of contract);
- the physical presence and business location of the seller;
- the place of performance of the contract;
- the location in which the services are being provided or the goods are being manufactured or supplied;
- whether the laws governing the transactions or disputes have extra territorial effect; and
- other factors in determining the forum for which the transaction has the closest and most real connection.

## Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

The main regulations that govern the conduct of online business owners and online marketplace operators in Malaysia are the Consumer Protection (Electronic Trade Transactions) Regulations 2012 (the Regulations). The Regulations are issued pursuant to the Consumer Protection Act 1999 (CPA) and impose obligations on online business owners and online marketplace operators to take certain steps to protect the interests of consumers, including the disclosure of certain information on their respective websites.

The legislation and regulations that apply to such business or activities (in their non-digital form) must be adhered to, notwithstanding the fact that the business or activities will be carried out digitally.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Yes, a contract is formed and concluded digitally when the contracting party affixes an 'electronic signature' on the digital contract, which may consist of any letter, character, number, sound or any other symbol or any combination thereof.

Contracts that cannot be concluded digitally include powers of attorney, wills and codicils, creation of trusts, and negotiable instruments.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

No, parties have the freedom to determine the choice of governing law, contract language or forum for disputes. Such freedom applies to business-to-consumer and business-to-business contracts.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

A digital signature is a transformation of a message (defined as a digital representation of information) using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine:

- whether the transformation was created using the private key that corresponds to the signer's public key; and
- whether the message has been altered since the transformation was made.

Signing takes place by way of the affixing of a digital signature by the signer with the intention of signing a message.

An e-signature can be in the form of any letter, character, number, sound or other symbol or any combination thereof created in an electronic form adopted by a person as a signature. E-signatures may generally be used to sign documents, however they may not be used to sign powers of attorney, wills and codicils, documents relating to the creation of trusts and negotiable instruments. Signing takes place by way of affixing the said letter, character, number, sound or other symbol or any combination thereof in an electronic form.

A digital signature provider must be a licensed certification authority registered with the Malaysian Communications and Multimedia Commission in order for the digital signature to be recognised as valid. There is no such requirement for e-signature providers.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

No. Digital contracts will be given the same treatment as physical or non-electronic contracts.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

The advertising or selling of financial services or products digitally or via the internet may be regulated if it involves any business, or includes an activity, that is regulated in Malaysia.

The conduct of any business involving banking (including internet banking and digital banks), Islamic banking, international Islamic banking, investment banking, insurance (including internet insurance), takaful, international takaful, financial advisory, Islamic financial advisory, insurance broking, money broking (money changing or remittance), takaful broking, merchant acquiring, adjusting (in relation to insurance or takaful claims), operation of a payment system, issuance of designated payment instruments or issuance of designated Islamic payment instruments is regulated by the Central Bank of Malaysia under the Financial Services Act 2013 or the Islamic Financial Services Act 2013.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

#### Electronicmoney

The issuance of electronic money (prescribed as a 'designated payment instrument' pursuant to the Financial Services Act 2013) requires the prior approval of the Central Bank

of Malaysia and electronic money issuers are required to comply with the Guidelines on Electronic Money.

**Digitalassetsanddigital currencies**

Pursuant to the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019, all digital currencies and digital tokens that satisfy the requirements stated therein are prescribed as 'securities' for the purpose of the Capital Markets and Services Act 2007 (CMSA) and may need to comply with the CMSA. Further, the Malaysian Securities Commission has issued the Guidelines on Digital Assets prescribing the requirements relating to fundraising activity through digital token offering, operationalisation of initial exchange offering platform and provision of digital asset custody. It should be noted that digital currencies and digital tokens have not to date been recognised as legal tender or as a form of payment instrument that is regulated by the Central Bank of Malaysia.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Certain digital and crypto wallets are governed under the Financial Services Act 2013 and Capital Markets and Services Act 2007. In particular, electronic money wallets are governed under the Guidelines on Electronic Money and digital assets wallets are governed under the Guidelines on Digital Assets.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

The operation of electronic payment systems in Malaysia is generally regulated under the Financial Services Act 2013 or the Islamic Financial Services Act 2013. The operation of electronic payment systems in Malaysia falling under the ambit of the Financial Services Act 2013 or the Islamic Financial Services Act 2013 requires the prior approval of the Central Bank of Malaysia.

The Financial Services Act 2013 and the Islamic Financial Services Act 2013 contain secrecy provisions that prohibit disclosure of information relating to the affairs or account of any customer of a financial institution/Islamic financial institution (supplemented by the Management of Customer Information and Permitted Disclosures Policy Document issued by the Central Bank of Malaysia setting out requirements and expectations with regard to financial service providers' measures and controls in handling customer information).

### Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Based on the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions Policy Document, reporting institutions (with respect to the requirements imposed under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001) may rely on third parties to conduct customer due diligence or to introduce business provided that such third parties are reporting institutions that are supervised by a relevant competent authority and the reporting institution must satisfy certain requirements. The relationship between reporting institutions and the third parties relied upon by the reporting institutions to conduct customer due diligence shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties.

Notwithstanding the foregoing, the ultimate responsibility and accountability for customer due diligence measures shall remain with the reporting institution relying on the third parties. Reporting institutions shall have in place internal policies and procedures to mitigate the risks when relying on third parties and are prohibited from relying on third parties located in certain identified high-risk countries.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

MYNIC is the official .MY domain registry, recognised by the Internet Corporation for Assigned Names and Numbers (ICANN), which administers the registration of domain names. Registration of .MY domain names will be via MYNIC's official resellers.

It is not possible to register a country-specific domain name without having a presence in Malaysia. Entities looking to register a country-specific domain name must be incorporated in Malaysia, or if it is a representative or regional office, it must be supported by an official letter from the Malaysian Ministry of International Trade and Industry showing the registration of the representative or regional office. If it is a foreign office, it must be supported by an official letter from the Malaysian Ministry of Foreign Affairs regarding the approval of the setting up of a foreign office.

There are no regulatory restrictions around the use of URLs to direct users to websites, online resources or metaverses.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Yes. Where an owner of a trademark can successfully prove (1) that the disputed domain name is identical or similar to a trademark or service mark of the said owner, and (2) that the 'pirate' registrant registered or used the disputed domain name in bad faith, subject to the pirate registrant proving its rights and legitimate interests in the disputed domain name, the registration of the disputed domain name will be transferred to the owner or deleted.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

The general rules, legislation and self-regulatory codes governing online advertising in Malaysia include (among others):

- Content Code registered with the Communications and Multimedia Commissioner;
- Consumer Code registered with the Communications and Multimedia Commissioner;
- Communications and Multimedia Act 1998;
- Consumer Protection Act 1999; and
- Trade Descriptions Act 2011.

In addition to the above, the advertisements relating to specific products (eg, advertisements relating to medical products, treatment and facilities and food and advertisements involving professionals) may be governed under specific legislation.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

The use of any personal data relating to individuals for the purpose of targeted advertising would generally require the consent of the data subjects and the data user shall issue a privacy notice (in both Malay and English languages) to the data subjects informing them of the minimum information prescribed by the Personal Data Protection Act 2010.

Pursuant to the Personal Data Protection Act 2010, a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing. 'Direct marketing' means the communication by whatever means of any advertising or marketing material that is directed to particular individuals. The data use should comply with the data subject's opt-out requests.

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

Rules against misleading online advertising in Malaysia include:

- The Consumer Protection Act 1999, which prohibits bait advertising and false or misleading statement and conduct. The Consumer Protection Act 1999 applies to business-to-consumer transactions.
- The Trade Descriptions Act 2011, which prohibits false trade descriptions and false or misleading statements (including statements in any advertisement through electronic means), conduct and practices in relation to the supply of goods and services generally.
- The Communications and Multimedia Act 1998, which prohibits the provision of any content which is indecent, obscene, false, menacing or offensive in character with the intent to annoy, abuse, threaten or harass any person. This statutory obligation is imposed on a content applications service provider or other person using a content applications service.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

Advertisements relating to the following non-exhaustive list of products or services are generally unacceptable:

- digital betting or gambling;
- digital materials that are indecent, sexually explicit or impolite; and
- other illegal or infringing digital products or services.

Advertisements of sector-specific digital services or products (on the internet or otherwise) may be regulated under specific legislation.

## Direct email marketing

### 21 | What regulations and guidance apply to email, SMS and other direct marketing?

Unsolicited direct marketing (which the Personal Data Protection Act 2010 defines as the communication by whatever means of any advertising or marketing material directed to particular individuals) is allowed, however the recipient of such marketing must be provided with the right to opt out from such direct marketing.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

The concept of an innocent carrier in the Content Code provides that any service provider that provides access to any content, but that has neither control over the composition of such content nor any knowledge of such content, is deemed an innocent carrier for the purpose of the Content Code. An innocent carrier is not responsible for the content provided. Despite the foregoing, it is pertinent to note the following:

- the Communications and Multimedia Act 1998 indicates that it is the responsibility of the content applications service provider (internet content hosts and internet access service providers) or other persons using a content applications service (the website operator) to ensure that content provided is not indecent, obscene, false, menacing or offensive in character with the intent to annoy, abuse, threaten or harass any person; and
- the Federal Court of Malaysia has held an online news portal liable for contempt for comments posted by third parties although such comments were removed promptly once the offensive statements were known. This decision imposed an onerous burden on what would traditionally be regarded as mere conduits willing to comply with the flag and takedown process.

The said decision is likely to only affect online intermediary platforms that have editorial control over third party comments. The decision may be distinguished from, and on balance should not affect, the liability of providers that have no control over third-party user content. Providers may limit liability by introducing strict filter systems that detect offensive content and ensuring that they are prompt in removing any offensive content once they have knowledge of them.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

A digital platform or online content provider will be liable for mistakes in information it provides online when a complaint is made to the relevant authorities. Content liability may be mitigated by including disclaimers in the platform terms of use.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Although technically a provider may do so, depending on its policy and the terms entered with its users, this is not commonly undertaken. Section 263(2) of the CMA may however be relied on by the Communications and Multimedia Commission or other authorities to request providers to disable access by end users to an online location for the purpose of preventing the commission or attempted commission of an offence under any written law in Malaysia. Whether a court order is required prior to such action being undertaken has yet to be judicially determined, although recent reported media statements seem to suggest that the authorities would require a court order.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

There is no specific protection for data or databases under copyright. The compilation table of the data would be protected under copyright but not the data itself.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Generally a link (or more precisely a 'hypertext' link) to a third-party website can be done without first seeking permission. If, however, the third-party website expressly indicates that it does not allow linking, then it would be best practice to seek permission first.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

No, as such use of third-party content without permission from the third-party content provider would expose the website owner to severe consequences such as civil actions initiated by the third-party content provider for copyright or trademark infringement (or both).

If the use of the third-party content is alleged to circumvent, or cause or authorise circumvention of any effective technological measures, such use could be an offence under the Copyright Act 1997 and may attract criminal sanctions.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

As at the time of writing, there are no reported cases in Malaysia with regard to enforcement of IP rights in a metaverse.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

The concept of exhaustion of rights is recognised in Malaysia, however it is unclear as to whether this concept applies in relation to digital products.

## Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

The enforcement authorities have the power to carry out dawn raids in connection with the offences of counterfeiting a trademark under the Trademarks Act 2019 (sections 121 and 122) and dealings with infringing copies of copyrighted works under the Copyright Act 1987 (section 44). However, the power to grant freezing/Mareva injunctions against IP infringers vest in the courts, and not the enforcement authorities.

## Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

The common remedies for IP owners whose IP rights are found to have been infringed are an order for injunction and damages or an account of profits.

Besides the aforesaid common remedies, the relief of statutory damages is available for copyright owners typically in cases where there are difficulties in ascertaining and proving actual damages or account of profits for infringement of copyright. In addition, the award for additional damages for trademark infringement and copyright infringement is also stipulated for under the Trademarks Act 2019 and Copyright Act 1987 in cases where the court is satisfied that such award is proper having regard to several factors such as flagrancy of the infringement, the unjust benefits accrued to the infringer and the need to punish the infringer.

In IP infringement suits, pending disposal of the full trial, an IP owner may apply for the appropriate interim measures from the court such as Anton Piller Order (which bears some

resemblance to a search warrant) and freezing/Mareva injunction, the grant of which are subject to the relevant requirements being fulfilled by the IP owner.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Personal data includes any information in respect of commercial transactions that relates directly or indirectly to an individual, who is identified or identifiable from that information, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

There is also a category of 'sensitive personal data' and the processing of such data requires the explicit consent of an individual.

In the event data is anonymised to the extent that an individual is not identifiable from such data, such data will not be categorised as personal data.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Parties that fall within the class of data users in the Personal Data Protection (Class of Data Users) Order 2013 are required to register as data users with the Department of Personal Data Protection.

The law does not expressly require the appointment of a data protection officer however, the Personal Data Protection Regulations 2013 require the contact details of the data user's contact person to be provided to data subjects.

### Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

Local data protection laws may apply to organisations or individuals resident outside Malaysia if they use equipment in Malaysia for processing personal data. Where the organisations or individuals are not established in Malaysia, there must nominate a representative in Malaysia.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

The most common reason or basis for processing and exporting or transferring personal data to another jurisdiction is consent of the individual whose personal data is being processed or transferred to another jurisdiction.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Any transfer of personal data:

- outside of Malaysia requires consent (though not explicit) of the individual; or
- through removable media device and cloud computing service is allowed upon the written consent of an officer authorised by the top management of an organisation.

Malaysia is catching up with the concept of data sovereignty which is reflected in existing framework and policies under the Communications and Multimedia Act 1998. Data localisation is not common, however there is a requirement under the Employment Regulations 1957 for an employer to keep a register containing employee information in the office within the place of employment where the employees are employed.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

No. It is an offence to sell personal data to third parties. If a party is found to be liable for selling personal data, such party will be liable to a fine not exceeding 500,000 ringgit or imprisonment for a term not exceeding three years, or both.

## Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Individuals have the right to access, correct and prevent processing of their personal data for direct marketing purposes and to withdraw consent previously given. An individual aggrieved in relation to their rights may lodge a complaint with the Department of Personal Data Protection. These rights are available to any data subjects irrespective of whether they are citizens or foreign individuals.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

The law in Malaysia does not regulate the use of non-personal data.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Most documents or records can be converted solely to a digital representation however certain documents are required to be kept in original paper. Examples include wills, negotiable instruments, and documents or forms relating to land matters.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Yes. The Companies Act 2016 requires companies to retain records related to their transactions and financial position for seven years after they complete the relevant transaction. The Income Tax Act 1967 requires taxpayers to keep sufficient records for a period of seven years from the end of each reporting period to enable the Director General of Inland Revenue to ascertain income or loss from the business.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

The Personal Data Protection Standard 2015 issued pursuant to the Personal Data Protection Act 2010 established security standard prescribing steps to be taken by data users to (1) ensure personal data processed electronically and non-electronically could be protected from personal data breaches, and (2) guarantee cybersecurity of personal data contained in communications, online transactions and payment information.

Malaysia's Cybersecurity Strategy 2020–2024 contains high level cybersecurity initiatives to manage cyberattacks, however there is no specified level of cybersecurity or specific procedures to avoid data breaches or any commonly used cybersecurity standards.

### Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

There are no mandatory data breach notification requirements that apply to digital business in Malaysia. The Department of Personal Data Protection has recently, however, recommended that personal data breaches be reported within 72 hours.

### Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Yes the authorities are permitted lawful access to data under various types of legislation when they have reasonable cause to believe that an offence has been committed. The relevant legislation is general in application, therefore all types of companies may be subject to search and seizure rights for the purposes of investigations of offences.

In the specific case of offences under the Digital Signatures Act 1997, police officers conducting a search (with a warrant) or a search and seizure (without a warrant) are to be given access to computerised data whether stored in a computer or otherwise, including being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Betting, gaming and lotteries are generally governed and prohibited under the Common Gaming House Act 1953 and the Betting Act 1953 (unless approved by the relevant authority), which are enacted to suppress gaming and betting in Malaysia. As these Acts were drafted prior to the advent of the internet, they do not explicitly prohibit online betting or gaming.

Taking a purposive approach, the operation of an online betting or gaming business (involving the element of chance) would arguably not be permissible (unless with the approval of the relevant authority).

Shariah law bans all forms of gambling among Muslims in Malaysia.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

The advertisement of, and provision of access to, an online betting or gaming business located in a jurisdiction outside of Malaysia or in a metaverse are generally not permissible applying a purposive approach of the Common Gaming House Act 1953 and the Betting Act 1953 discussed above (unless approved by the relevant authority). Based on publicly available sources, from 2020 until the end of 2022 the Malaysian Communications and Multimedia Commission blocked 6,381 websites found to be promoting online gambling.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

One of the key legal issues to consider when outsourcing services to a provider either inside or outside Malaysia is confidentiality and data security as the accessibility of confidential information by the outsourcing partner may increase the risk of security breaches. When the provider is outside Malaysia, the potential cross-border transfer of personal data must be considered. Another legal issue would be the ownership of pre-existing and newly developed intellectual property rights when the outsourcing contract is not specific on the ownership of such rights.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

There is no general prohibition on outsourcing in relation to digital business services. Outsourcing in certain specific sectors may be regulated. For example, outsourcing arrangements by financial institutions (banks, investment banks, Islamic banks, insurers, takaful operators and other prescribed financial institutions) are regulated under the Guidelines on Outsourcing issued pursuant to the Financial Services Act 2013 and Islamic Financial Services Act 2013, which set out the scope of arrangements relevant to the outsourcing policy, and the requirements and expectations on financial institutions to maintain appropriate internal governance and outsourcing risk frameworks. In certain outsourcing scenarios, prior approval by the regulator may be required.

## Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

Where the processing of personal data is carried out by a data processor on behalf of a data user, the data user is required by data protection laws and standards to bind the data processor with a contract that contains sufficient guarantees in respect of technical and organisational measures governing the processing to be carried out.

The Central Bank of Malaysia has issued an outsourcing policy document which sets out a list of terms that must be included in any outsourcing agreements entered into by financial institutions, including the financial institution's continuous and complete access to its data held by the service provider in the event of a dispute with the service provider, or termination of the arrangement.

## Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

If outsourcing results in redundancy and retrenchment, retrenched employees are to be given notice of retrenchment in accordance with their employment contracts or collective agreement (if there is one in place), provided that the notice period is not less than that provided for in the Employment Act 1955 (EA) as set out below:

- less than two years of service – four weeks' notice;
- two years to less than five years of service – six weeks' notice; and
- five years of service or more – eight weeks' notice.

The right to consultation will be in accordance with policies or collective agreements that are in place. If there are none, it is nevertheless good practice to speak to the impacted employees to inform them of the decision to retrench.

As for compensation, employees who fall within certain categories set out in the 1st Schedule of the EA and who have been employed under a continuous contract of employment for at least 12 months before the retrenchment are statutorily entitled to termination benefits at a rate not less than that set out in the formula stated in the Employment (Termination and Lay-off Benefits) Regulations 1980 (the Regulations) as follows:

- less than two years of service – 10 days' wages per year of service (prorated for an incomplete year);
- two years to less than five years of service – 15 days' wages per year of service (prorated for an incomplete year); and
- five years of service or more – 20 days' wages per year of service (prorated for an incomplete year).

The categories of employees who are statutorily entitled to termination benefits are:

**Read this article on Lexology**

- those whose wages are up to 4,000 ringgit monthly; or
- regardless of wages:

    - employees who are engaged in manual labour;
    - employees who are engaged in the operation or maintenance of any mechanically propelled vehicle operated for the transport of passengers or goods or for reward or for commercial purposes;
    - employees who supervise and oversee other employees engaged in manual labour; or
    - employees engaged in any capacity in any vessel registered in Malaysia and who:

        - are not officers certificated under the Merchant Shipping Acts of the United Kingdom as amended from time to time;
        - are not holders of a local certificate as defined in Part VII of the Merchant Shipping Ordinance 1952; or
        - have not entered into an agreement under Part III of the Merchant Shipping Ordinance 1952.

What are considered 'wages' is defined in the Regulations and 1st Schedule of the EA.

The rights of employees who are not statutorily entitled to termination benefits are subject to their employment contract or company policies. In the absence of such provision, most employers do exercise their discretion to pay termination benefits, adopting the common law principle that employers should as far as possible, pay compensation to employees who have lost their job due to retrenchment.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

There are no specific rules or restrictions regarding the development or use of artificial intelligence, machine learning, automated decision-making or profiling (technology). If such use of the technology entails the processing of personal data, the operator is required to comply with the Personal Data Protection Act 2010 by, among others, providing notice to an individual that their personal data is being collected using the technology, and obtaining explicit consent from the individual if sensitive personal data is being processed. It is not mandatory to conduct an impact assessment for the development or use of the technology, however, it is recommended that one should do so bearing in mind that there may be an impact from medical, confidentiality, data protection and privacy, and consumer protection perspectives.

### IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

There are no specific rules or guidelines that govern intellectual property (IP) and artificial intelligence (AI) or machine learning. IP legislation still recognises that authors of works or inventions must be human therefore, if a human controlled the AI that resulted in the creation of a work or an invention that could be protected by IP, then perhaps that type of work or invention is protectable and can be owned by the human author or inventor or the party that commissioned it. For training data sets and other data, as there is no specific protection accorded to data and databases at this point in time, it is unlikely that any protection is accorded by extension to data created by AI.

### Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

No rules or guidance have been issued on the ethics of artificial intelligence and machine learning; however, the Malaysia Artificial Intelligence Roadmap 2021–2025 issued by the Ministry of Science, Technology and Innovation suggests some strategic initiatives.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

The scope of Malaysian income tax is territorial. Income accruing or deriving from Malaysia will be taxed in Malaysia. There is withholding tax on royalties and service fees made to non-residents at the rate of 10 per cent of the gross amount. In so far as digital products are concerned, if any of the payment is seen as royalty, this could be subject to withholding tax at the rate of 10 per cent of the gross amount. The scope of withholding tax on service fees is extremely wide, and the Malaysian Inland Revenue Board has indicated that it will apply not only to technical services but also to any non-technical services. However, effective from 6 September 2017, services that are performed and rendered outside Malaysia are exempt pursuant to the Income Tax (Exemption) (No. 9) Order 2017.

In addition, with effect from 1 January 2020, (1) foreign service providers who provide any digital service to any consumer, and (2) any person who operates an online platform or marketplace and provides digital services, including providing an electronic medium that allows suppliers to provide supplies to customers or transactions for provision of digital

services on behalf of any person, are required to charge 6 per cent service tax. For a particular service to fall within the scope of digital services:

- the service must be delivered or subscribed over the internet or other electronic network;
- the service must be one that cannot be obtained without the use of information technology; and
- the delivery of the service must be essentially automated.

The focus is very much on how a particular service is delivered. If it is 'digitally' delivered, then service tax applies, regardless of its nature. The Royal Malaysian Customs Department currently appears to apply the definition of digital service in a wide manner to the extent that the provision of online software, mobile applications, online games, music, streaming services, online advertising space, platforms to trade products or services, online data warehousing, and other digital content such as images, tax and information, are caught.

## Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

The scope of Malaysian income tax is territorial. In essence, it is about what has been done to earn the income and where it was done. The location of a server, platform or metaverse in Malaysia by a company incorporated outside Malaysia would, in our view, increase the risk of income of that company being seen as derived from Malaysia.

## Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

Under the Service Tax Act 2018, every registered person who provides any taxable service must, within one year from the date the taxable service was provided or such extended period as may be approved by the Director General of Customs, issue an invoice containing prescribed particulars in the national language or English language to the customer in respect of the transaction. A registered person shall be treated as having issued an invoice to a customer notwithstanding that there is no delivery of any equivalent document in paper form to the customer if the prescribed particulars are recorded in a computer and are transmitted or made available to the customer by electronic means or are produced on any material other than paper and are delivered to the customer.

Every foreign registered person who provides any digital service shall issue an invoice or a document (whether issued electronically or in paper form) containing prescribed particulars to the consumer in respect of the transaction.

Further, in July 2023, the Inland Revenue Board of Malaysia introduced guidelines for the gradual implementation of e-invoices for taxpayers as follows:

- 1 June 2024: taxpayers with an annual turnover or revenue of more than 100 million ringgit;
- 1 January 2025: taxpayers with an annual turnover or revenue of more than 50 million ringgit and up to 100 million ringgit;
- 1 January 2026: taxpayers with an annual turnover or revenue of more than 25 million ringgit and up to 50 million ringgit; and
- 1 January 2027: all taxpayers and certain non-business transactions.

To facilitate taxpayers' transition to e-invoice, the Inland Revenue Board of Malaysia has developed two e-invoice transmission mechanisms:

- a portal (MyInvois Portal) hosted by the Inland Revenue Board of Malaysia; and
- application programming interface (API).

The following formats will be available for transmission of e-Invoice: Extensible Markup Language (XML) and JavaScript Object Notation (JSON). The guideline also sets out a list of required fields for an e-invoice.

When a sale or transaction is concluded, the supplier is required to create an e-invoice in accordance with the defined structure (ie, XML or JSON) and submit it to the Inland Revenue Board of Malaysia for validation.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are currently no specialist courts in Malaysia for online- or digital-related issues.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

Parties may agree to settle their online or digital disputes through mediation or arbitration.

The Asian International Arbitration Centre (Malaysia) (AIAC) provides specialised dispute resolution services in relation to generic top-level domain names approved by the Internet Corporation for Assigned Names and Numbers, domain name disputes and sensitive names disputes.

ADR is not common for online or digital disputes, however, many defamation cases, online or otherwise, will usually be directed by the courts to attempt mediation.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

With the increase in the provision of digital content and services, there has been a corresponding increase in cybercrime. This has led to calls for national cybersecurity legislation, however, as at the time of writing, no bill is in the pipeline. The protection of personal data, especially in the context of doing business online, is an increasingly hot topic and the regulator has proposed that the Personal Data Protection Act 2010 be amended to tighten measures for the protection of personal data. However, as at the time of writing, no such amendment has been discussed.

There is currently no other pending legislation that is likely to have consequences for digital transformation and doing business online.

* *The authors wish to thank Raja Eileen Soraya, Yvonne Ong, Tham Li Vyen and William Wong for their assistance in the preparation of this chapter.*


Tong Lai Ling tonglailing@rdl.com.my
Jed Tan Yeong Tat jedtan@rdl.com.my

Level 26, Menara Hong Leong, No. 6 Jalan Damanlela,
Bukit Damansara, 50490 Kuala Lumpur, Malaysia
Tel: +603 2632 9999
https://rajadarrylloh.com

# Portugal

Ana Rita Paínho, Verónica Fernández, Teresa Pala Schwalbach, Rita Canas Da Silva and Ana Mira Cordeiro
Sérvulo & Associados

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The Portuguese government's attitude is globally welcoming towards these matters. Legislative initiatives in the past few years include:

- The government's INCoDe.2030 Programme – an initiative to enhance digital competences;
- Decree Law 67/2021 – a legal framework establishing Technological Free Zones (TFZs);
- Council of Ministers Resolution 29/2020 – encouraging the development of a legislative framework facilitating research, simulation and testing activities for innovative technologies, products, services and models (artificial intelligence, blockchain, virtual reality, big data, 5G, Internet of Things) by creating TFZs; and
- Council of Ministers Resolution 30/2020 – Action Plan for Digital Transition, foreseeing a strategic framework for the integration of Public Administration in the cloud.

Despite the positive attitude and evolution, still a lot more could be done in practical terms, by means of direct incentives aimed at the markets and the global public.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

Aside from sector-specific applicable regulation, digital content and services are mostly regulated by legislation on:

- consumer protection including e-commerce/distant transactions and contracts for the supply of digital content and digital services;
- advertisement and unfair practices;
- unfair competition;
- electronic communications;
- audio-visual and media services;
- privacy;
- cybersecurity;
- authorship and related rights; and
- industrial property.

The government's 2020 Action Plan for Digital Transition and the Portuguese Charter of Human Rights in the Digital Age are also worth mentioning.

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The responsible regulatory bodies are as follows:

- Inspectorate General for Cultural Activities (IGAC): powers of supervision, control, removal and prevention of access in the digital environment to authorship and related rights, protected content over intermediary service providers.
- General Directorate of Consumer Affairs (DGC): supervisory competences in consumer protection and Laws.
- Food and Economic Safety Authority (ASAE): supervisory competences in consumer laws and overall economic activities.
- Portuguese Data Protection Authority (CNPD): supervisory powers including ePrivacy regulations.
- National Communications Authority (ANACOM): regulation of the entire communications sector, including telecommunications, with regulatory, supervisory, oversight and sanctioning powers.
- Regulatory Authority for the Media (ERC): regulation of social media platforms whenever they host or are used as broadcast media outlets.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

In business-to-business transactions, parties are free to set choice of law and venue clauses, which will most likely be held up in Portuguese Courts. Unless otherwise agreed by the parties, the general rule under the law is that the action must be brought before the competent court in the country of residence of the defendant. For cases in which the dispute refers to provision of services to be provided in Portugal, Portuguese courts have jurisdiction.

In business-to-consumer transactions, if the plaintiff is a consumer resident in Portugal, they can choose to initiate proceedings either in Portugal, or in the EU member state in which the provider is headquartered, regardless of choice of law and venue that may be set on the underlying contract. If the contract contains a jurisdiction clause, the competent court shall be determined in compliance with the general terms of the Brussels I Regulation and the Rome I Regulation as per the applicable law, even if one of the parties is not resident in a member state. In this case, the ultimate target is to protect the interests of the consumer and choice of law or venue (or both) is made for his or her benefit.

To date, as far as we are aware, there is no record of legal disputes on transactions in the metaverse.

### Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

No immediate differences apply to the establishment of businesses based on their digital or non-digital nature. The main exception is the online betting and gambling industry in Portugal, in which licencing schemes for operators' online or offline betting and gambling products are substantially different, as well as regulated and supervised independently.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

As a rule, a contract whose validity is not subject to special requirements can be entered into online.

However, where the agreement itself or sector-specific laws require a handwritten signature, such agreement must be signed by means of a qualified electronic signature, as required under EU Regulation 910/2014 (the eIDAS EU Regulation). Examples include consumer financing, licence and transfers of authorship rights and protected content, contracts relating to security deposits and real estate transactions.

### Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Yes. For business-to-consumer online contracts, pre-contractual information, including the agreement itself (T&Cs), must be presented in Portuguese and, by statutory provisions of consumer laws, regardless of what the agreement might state, the applicable law and dispute forum shall be Portuguese. Businesses also are required to offer consumers information on alternative dispute resolution (ADR) forums.

In business-to-business contracts, despite the generally accepted principle of freedom of choice and forum, a preventive case-by-case analysis based on the applicable sector specifications is recommended.

### Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Portuguese legislation follows the eIDAS EU Regulation, complemented by Decree-Law 12/2021 regarding competences and responsibilities of the State Electronic Certification System's (SECS) managing board.

Under the eIDAS EU Regulation, the provision of electronic signature services with (1) simple or standard, (2) advanced and (3) qualified different legal effects, requires pre-assessment and approval of their conformity to be included in the European Commission's Qualified Trust Service Providers list and the qualified trust services provided listed in the Portuguese Trusted List.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

No. The same judicial and alternative dispute resolution methods are available for all types of contracts, regardless of their material support. Jurisdiction and competence are determined based on the subject matter and material applicable law.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

Advertising and selling of such products by digital means or via the internet are not regulated in Portugal by specific legislation, but by laws and regulations applicable to the general advertising of such types of services and products. In addition to the Advertisement Code (Decree-Law 330/90), specific regulations issued by the Bank of Portugal, the Portuguese Securities Markets Commission (CMVM) and the Insurance and Pension Funds Supervisory Authority (ASF) must be observed, depending on the nature of the services or products; once such matters are subject to the regulation and supervision of said institutions.

Regarding the advertising of financial products and services subject to the supervision of the Bank of Portugal, Notice 10/2008 and Notice 5/2017 apply. All advertising materials related to public offers are subject to prior approval by the CMVM. As for insurance, Regulation 3/2010-R of ASF establishes the principles and rules to be complied with by insurance companies, intermediaries and pension fund management entities.

The sale of financial products and services, digitally or via the internet, shall also comply with the provisions of Decree-Law 95/2006 of 29 May, which transposed Directive 2002/65/EC on the distance marketing of consumer financial services.

## Electronic money and digital assets

### 11 Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Yes. According to Decree Law 91/2018 of 12 November – legal framework on payment services and electronic money (transposing Directive 2015/2366 (the PSDII)) – the issue of electronic money is restricted to the following entities:

- credit institutions having their head office in Portugal including the issue of electronic money in their corporate purpose;
- electronic money institutions having their head office in Portugal;
- credit institutions having their head office outside Portugal that are legally authorised to pursue the activity in Portugal;
- electronic money institutions having their head office in another EU member state that are authorised to operate in Portugal;
- branches of electronic money institutions having their head office outside the EU;
- the Portuguese state, autonomous regions and services and bodies under direct and indirect state government when not acting in their capacity as public authorities; and
- The European Central Bank, the Bank of Portugal and all other national central banks when not acting in their capacity as monetary authority or in the exercise of other public powers.

The law sets out the applicable procedures to be complied with by issuers of electronic money in connection with the issuance, distribution and reimbursement of electronic money. These matters are subject to a limited but significant set of conduct rules that should be taken into due account in the contractual relationship between issuers and holders of electronic money.

The issue of digital assets or use of digital currencies is not yet regulated under Portuguese legislation.

## Digital and crypto wallets

### 12 Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Yes. Further to the publication of Law 58/2020, of 31 August – which transposed the Fifth Money Laundering Directive – entities providing services allowing the safekeeping or administration of crypto actives were included within the scope of the (non-financial) entities obliged to comply with the prevention of money laundering and terrorist financing (ML/CFT) obligations under the applicable legislation, specifically Law 83/2017 of 18 August 2017, which lays down preventive and punitive measures relating to AML/CFT.

The provision of such types of services became thus subject to the prior registration of the service providers with the Bank of Portugal (under Bank of Portugal Notice 3/2021).

The Bank of Portugal has been entrusted with the responsibility for verifying compliance with the legal and regulatory provisions governing the prevention of AML/CFT by crypto wallets service providers. It should be noted that the Bank of Portugal's supervision over crypto wallet service providers is limited in scope to AML/CFT purposes, and does not cover other areas of a prudential, market conduct or any other nature.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Electronic payment systems are mainly regulated by Decree-Law 91/2018, which transposed PSD II. The provision of certain services that allow third-party access to digital information in bank accounts, such as Payment initiation Services (PIS) and Account information Services (AIS), is also subject to regulation by the law.

## Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Yes. Article 41 of Law 83/2017 of 18 August expressly entitles obliged entities to comply with AML/CTF obligations to use third parties to execute the identification and due diligence procedures, provided that such obliged entities:

- ensure that such third parties are qualified to perform identification and due diligence procedures as their third-party entities;
- assess, based on information in the public domain, the reputation and suitability of such third parties;
- complete the information collected by third parties or carry out a new identification, in case of insufficient information or when the associated risk justifies it;
- fulfil all document conservation requirements; and
- ensure that such third parties: (1) gather all the information and comply with all identification, due diligence and document conservation procedures with which the obliged entities themselves must comply; and (2) when requested, immediately provide a copy of the identification and identity verification data and other relevant documentation about the customer, their representatives or beneficial owners who have been subject to the identification and due diligence procedures.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

Registration and management of '.pt' domains is ensured by DNS.pt Association (delegated competences by the Internet Corporation for Assigned Names and Numbers (ICANN)).

Applicants' place of residence is not a requirement for registration of country-specific domain names.

With regard to embedded linking, no local specific regulations apply. However, there is an increased tendency for website and digital product owners to adopt legal disclaimers excluding liability for access to third parties' websites in view of the latest decisions by the Court of Justice of the European Union on whether directing users to third parties' websites containing IP-protected content should be regarded as a communication to the public and thus require the rights holder's prior authorisation.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

No. Registration of domain names grants protection of the name as a digital asset but does not guarantee any special protection as intellectual property. However, if a domain name is the same as or similar to the reproduction of a word trademark, there may be grounds for an IP legal dispute.

Compared to the standard regime in force in the European Union, no local specificities apply.

In the event of a dispute, the most appropriate and effective mechanism is arbitration through the Arbitration Centre for Industrial Property, Domain Names, Trade Names and Corporate Names (ARBITRARE).

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

Online advertising is subject to the same rules as offline advertising, provided for in the Advertisement Code and in Decree-Law no 57/2008 (transposing Directive 2005/29/CE, concerning unfair business-to-consumer commercial practices).

When advertisements are displayed via the use of cookies or other tracking technologies, Law 41/2004 (transposing Directive 2002/58/CE – ePrivacy Directive) shall also apply; and, if the use of cookies implies processing of personal data, then the General Data Protection Regulation (GDPR) also applies. The content of the advertisement is subject to the Advertising Code and, in the case of regulated industries (eg, financial services), any relevant specific provisions.

On 25 January 2022, the Portuguese Data Protection Authority (CNPD) issued Guideline/2022/1 on electronic direct marketing communications, under which data subjects must be able to provide consent specifically, entity by entity, even with regard to companies within the same corporate group or affiliates, otherwise the consent cannot be deemed as valid, nor all subsequent data processing activities engaged on that data collected on the legal grounds of consent.

Under this guideline: (1) as most direct marketing activities involve large-scale data processing and frequently use innovative technologies, a DPIA may be required; and (2) controllers must maintain an up-to-date list of persons who have expressly and freely given their consent to receive marketing communications, as well as clients who have not objected to receiving it, under the ePrivacy Directive.

Members of the Portuguese Advertising Self-Regulation Association are also bound by their own code of conduct and guidance on marketing communications and online behavioural advertising.

Online advertisement on the metaverse is not yet subject to specific requirements.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Most targeted and online behavioural advertising practices in digital environments result from the use of cookies or other tracking technologies. Thus, Law 41/2004 (transposing Directive 2002/58/CE – ePrivacy Directive) shall apply and, where the use of cookies implies processing of personal data, the GDPR also applies.

Such practices require the user's prior consent, collected based on the GDPR criteria and requirements.

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

Online advertising follows the general rules of the Advertisement Code (Decree-Law 330/90) and Decree-Law 57/2008 (transposing Directive 2005/29/CE). There are no specific rules applicable to online advertising, or industry-specific rules, as rules are general and apply to any form of advertising, regardless of the medium used for its dissemination.

All claims regarding the origin, nature, composition, properties and acquisition of goods or services advertised must be accurate and verifiable at all times. Advertisers are advised to keep evidence of all these elements. Advertisement communications containing false information, or even truthful content that leads or may lead the consumers to errors in perception, is deemed misleading advertising. Advertisement communication omitting information in such a way that the consumer is misled is also deemed misleading and is thus forbidden.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

Advertising restrictions are based on the nature of the specific products (alcohol, tobacco, medical treatments or medicines, products containing high energy value, salt content, sugar, saturated fatty acids and processed fatty acids, gambling, pornography, etc) or the advertising targets (specifically minors or made in the vicinity of schools), not by the media through which the advertising is communicated.

## Direct email marketing

### 21 | What regulations and guidance apply to email, SMS and other direct marketing?

Distance marketing practices are regulated by Law 41/2004 (transposing Directive 2002/58/CE – ePrivacy Directive) and by the GDPR, while the content is subject to the Advertising Code, as well as, in the case of regulated industries (eg, financial services), any relevant specific provisions.

Members of the Portuguese Advertising Self-Regulation Association are also bound by the association's own code of conduct and guidance on marketing communications.

In line with the ePrivacy Directive, unsolicited marketing communications require the individual's prior, explicit and specific consent, except where it is sent by data controllers with whom they have a previous commercial relationship, and advertising similar products or services to those previously transacted. In such cases, data subjects must be granted the right to object at any time, easily and free of charge, to receiving direct marketing communications. These rules apply to all messaging systems potentially used for direct marketing.

The Portuguese Data Protection Authority (CNPD) recently issued Guideline/2022/1 on personal data protection and privacy in communications, which stresses these principles and where practical examples of (non) admissible practices are provided.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Liability of content providers and mere hosts (such as ISPs) follows the general rules on the attribution of liability, in addition to the rules provided by Decree law 7/2004 on e-commerce on the internal market and processing of personal data (transposing Directive 2000/31/CE).

Under these principles, the party directly responsible for the creation of the (illegal) content is ultimately responsible for the damages it may cause. With regard to ISPs, there is a general principle of absence of duty of supervision of the content provided, not being subject to a general obligation to monitor the information they transmit or store or to investigate any illicit activities carried out within their scope.

Thus, ISPs that only carry out the activity of transmitting information on a network, or providing access to a communications network, without being at the origin of the transmission or intervening in its content, are exempt from all responsibility for the information or content transmitted.

Nonetheless, according to EU Regulation No. 2022/2065 of 19 October on the single market for digital services, such responsibility exemption only exists as long as the internet service provider:

- does not have effective knowledge of the illegal content or activity, and
- once they acquire such knowledge, diligently acts to suppress or deactivate the access to the illegal content.

On the other hand, internet service providers must ensure that mechanisms are available that allow users to easily report illegal content, so that the provider can have knowledge of, and act upon, the illegal content.

Nonetheless, Decree Law 84/2021 (transposing Directive 2019/770 (the DSM Directive)) assigns an active role in preventing copyright infringement to ISPs, who must seek to obtain prior authorisation for the use of protected content, for instance by entering into a licensing agreement. If no authorisation is granted, they will be liable for unauthorised acts of communication to the public.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

Liability mostly depends on the authorship of content. Consequences for online display of wrong or inaccurate information varies depending on whether the provider's activity is subject to any industry-specific regulation (inaccurate or fake news in the case of media agents or information to consumers), that may lead to administrative offence proceedings. In such cases, liability cannot be excluded (and never in wilful intention or gross negligence) and any disclaimers or notices with such purpose would have no legal effect.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Yes, ISPs may remove content or shut down web pages in the case of illegal content, regardless of the nature of the illegality, including based on defamatory material (which is a crime under Portuguese law), without a court order and regardless of a request of an interested party, provided (1) they have notice of the illegal content; and (2) they consider such illegality to be obvious, meaning that the ISP, in its reasonable opinion, finds the content to be illegal.

Under Decree law 7/2004, if the illegality is not obvious, the ISP is not obliged to remove the contested content or to prevent access to the information solely based on an interested party's claim.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

Yes. Electronic or non-electronic databases benefit from protection by IP rights under Decree-Law 122/2000 (transposing Directive 96/9/CE), provided they meet the originality requirement. The rights holder, unless special circumstances apply, should be the intellectual creator of such database. Databases created inside a company are presumed to be collective works and not employees' IP rights, and the patrimonial rights belong to the employer. The database manufacturer is granted a sui generis and exclusive right over the content, regardless of the structure being protected by copyright.

## Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Yes; however, if a third-party website or platform contains authorship rights protected work, linking or URL embedding may require the rights holder's prior consent, thus prior due diligence is a recommended practice. Content providers are advised to include legal disclaimers warning users they are exiting their environment for cybersecurity and personal data protection purposes.

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

If such content is protected under authorship rights, prior consent by either its rights holder or a legitimate representative (eg, a collective management entity) is required.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

There is no stand-alone definition for metaverse in Portuguese law, nor specific guidelines on IP rights on a metaverse.

Therefore, the general rules apply.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Yes, both the Industrial Property Rights Code and the Authorship and Related Rights Code foresee the exhaustion of rights principle, as a limit to the distribution right or circulation of tangible copies, in line with Directive 2001/29/EC (InfoSoc Directive).

The implementation of the InfoSoc Directive did not result in the adoption of any policies on digital exhaustion in particular, therefore the debate on the limits of distribution of digital copies and communication to the public follows the evolution of CJEU decisions, namely the *UsedSoft* (C-128/11 – on software resale) and *Tom Cabinet* (C-263/18 – on ebooks resale) case rulings. This matter has not reached national courts.

It will be interesting to follow whether, with the evolution of the digital content market and associated technologies, notably the growth of streaming, this debate will continue to be relevant or whether it will become anachronistic or of limited applicability.

### Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Yes; both measures for obtaining evidence (raids) and measures for the preservation of evidence (freezing injunctions) are available, but resorting to these measures depends either on appropriate judicial proceedings before the competent court, or administrative offence proceedings before the competent authorities.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

The Intellectual Property Court is the competent judicial forum for settling civil disputes on industrial property and authorship rights. Rights holders can resort to interim and urgent measures (either to obtain or preserve evidence) or main actions on the merits (infringement of rights).

Compensation for pecuniary damages on the profit made by the infringer or loss of profit suffered by the injured party, and, in certain cases, compensation for non-pecuniary damages, can be sought.

The most sought type of remedy is the application for accessory measures (eg, temporary inhibition of the exercise of certain activities and penalty clauses).

At the plaintiff's request, the court may grant any appropriate measures to prevent imminent violations, or to prohibit a current violation of the alleged right. As a rule, these measures are granted after the defendant is notified, except where this would cause irreparable harm to the plaintiff.

In cases where the dispute is brought before the institutionalised arbitration centre competent for matters related to industrial property rights, .pt domain names, trade names and corporate names (ARBITRARE), the arbitration tribunal also has power to determine some interim or urgent measures.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Local data protection laws do not provide additional criteria regarding these definitions compared to the ones provided for in the GDPR.

The Data Protection Act (Law 58/2019 of 8 August) does provide additional confidentiality requirements for employees, contractors and overall data processors concerning the processing of personal data concerning health.

Under Regulation No. 1/2018 of the Portuguese Data Protection Authority (CNPD), certain types of data processing activities, in addition to those provided for in article 35(3) of the GDPR, must be preceded by a data protection impact assessment (DPIA). Such types of data include, among others, data of a 'highly personal nature' using new technologies or obtained by way of novel use of existing technologies (articles 9(1) and 10 of the GDPR).

## Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Following the accountability principle under the GDPR, data processing activities do not require prior registration or authorisation by the CNPD, apart from exceptional cases.

In addition to the cases of mandatory appointment of data protection officers (DPOs) under article 37 of the GDPR, private entities are also required to appoint a DPO where the activity primarily carried out – either as controllers or processors – involves (1) regular and systematic monitoring of data subjects on a large scale; or (2) large-scale processing operations of special categories of data pursuant to article 9 of the GDPR or of personal data relating to criminal and administrative offence convictions pursuant to article 10 of the GDPR.

DPO appointments must be communicated to CNPD, pursuant to article 37(7) of the GDPR.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

In line with the general framework provided by the GDPR, data protection laws apply to processing operations of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.

In addition, the Data Protection Act (Law 58/2019) shall also apply to activities of controllers and processors not established in the EU in the cases provided for in article 3(2) of the GDPR, as well as operations:

- of an establishment situated in the national territory;
- concerning data subjects located in the national territory; and
- concerning personal data of Portuguese residents held by Portuguese consular offices abroad.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

The legal bases for processing personal data and for transfer of personal data to another jurisdiction do not go beyond the GDPR (article 6), thus being mostly consent, performance of a contract, or necessary for compliance with a legal obligation to which the controller is subject.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

No local particularities beyond the required level of harmonisation with the GDPR and Directive 2016/680, of 27 April 2016 (transposed by Law 59/2019), on processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, shall apply.

## Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

Portugal follows closely the GDPR and general EU guidelines when it comes to personal data protection.

Portuguese law does not provide for direct restrictions to the sale or license of personal databases per se. However, in line with the GDPR rules on the lawfulness of processing, it must be ensured that both the operations of the transfer itself as well as the subsequent use of such data are executed under a valid legal basis and that, in case the sale or license implies a data transfer to countries outside the EU, such transfer is lawful under the GDPR.

Thus, the buyer's objective cannot be incompatible with the seller's original objective. Notably, in cases where the personal data was initially collected on the basis of consent, (1) data subjects must have provided specific consent for its sharing with third parties for use under a specific purpose (eg, direct marketing) and (2) such consent must have been validly collected.

### Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Provisions of Chapter III (data subjects' rights) and Chapter VIII (remedies and liability) of the GDPR directly apply, and no national particularities apply. Remedies are provided to all data subjects falling under the material and territorial scope of the GDPR, regardless of citizenship.

Data subjects can also claim damages before national courts for any losses suffered from violation of data protection laws and can resort to all judicial mechanisms available.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

No. There is no specific regulation for non-personal data, other than the right to privacy in general terms and overall confidentiality matters (including industrial or commercial/business secrecy).

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

The Portuguese government has been demonstrating an increased commitment to the multi-sectorial adoption of digital-friendly policies and procedures in the dematerialisation of relations of individuals and corporations with the public administration and in setting record-keeping obligations for compliance demonstration purposes, notably aiming to transition paper-based documentation in equivalent valid and binding alternative electronic versions, under the eIDAS Regulation.

The range of documents whose value depends solely on its original paper format is progressively decreasing. Among the most relevant cases where paper format documents are still considered to be 'originals' are the following:

- corporate and tax governance rules still require company by-laws, board decisions and tax documents to be kept in original paper form; and
- public documents issued by ministries, courts, registry offices and notaries (including notarised copies) originally issued or signed in paper versions (public deeds and powers of attorney regarding transmission of real estate) may still need to be presented on paper, namely before public entities.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Yes. There are multiple industry-specific document or data retention periods prescribed by statutory laws. Without prejudice to the right of keeping documentation containing personal data for performance of a contract, or based on legitimate interest (to ensure defence rights in case of litigation), under the GDPR and subject to the data minimisation principle, some of the most relevant sectorial data retention periods prescribed by law are:

- accounting records and supporting documents, including for VAT purposes: 10 years;
- contractual, preparatory and compliance documentation referring to employment relationships: five years; and
- client identification data, in case of entities subject to money laundering prevention legislation: seven years.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

All entities processing personal data must adopt the proportionate technical and organisational measures that, on a case-by-case basis, are deemed adequate to ensure data and systems security, under the general terms of article 32 of the GDPR.

Additionally, industry-specific cybersecurity requirements may apply, for example:

- critical infrastructure operators, essential services providers (financial services and digital infrastructures), digital service providers as well as any other entities using networks and information systems are also subject to Law 46/2018, of 13 August, the national legal framework on cybersecurity (transposing Directive 2016/1148 of 6 July (the NIS Directive)); and
- operators providing public communications networks or publicly available electronic communications services are also subject to the National Communications Authority's (ANACOM) Regulation 303/2019 on security and integrity of electronic communications networks and services.

The 2020 CNCS' National Cybersecurity Framework and ISO/IEC 27032, ISO 22301, ISO/IEC 22000, ISO/IEC 27000, ISO/IEC 27001 and ISO 9000 are commonly used cybersecurity standards.

## Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Yes. In cases where a breach of security leads to a data breach under the GDPR, the procedures provided for in article 33(1) of the GDPR must be followed, with no applicable local law specificities. The Portuguese Data Protection Authority (CNPD) makes available an online form (in Portuguese only) that may be used for reporting breaches.

In cases where the data breach or loss of integrity occurs within certain regulated industries, additional (and, where applicable, cumulative) requirements to notification obligations apply:

- providers of publicly available electronic communications services must notify the occurrence of any personal data breaches to CNPD and, depending on the seriousness of the risks presented, to the data subjects (eg, subscribers, users, or clients);
- providers of publicly available electronic communications services or networks must notify the respective sectorial national regulatory authority (ANACOM) where the occurrence entails significant impact to the functioning of networks and services;
- entities subject to the legal framework of cyberspace security must also notify, in certain terms, incidents with serious impact on the safety of their networks and information systems or on the continuity or provision of their services, depending on the type of entity, to the National Cyber Security Centre (CNCS); and
- entities subject to financial services regulation must also report cybersecurity incidents 'likely to compromise business operations and/or threaten information security' to the Portuguese central bank (Banco de Portugal), as per Notice 21/2019. Incidents must be reported through an online portal at www.bportugal.net.

## Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Under the GDPR, companies may need to process personal data (of clients, employees, users, etc) for compliance with legal obligations. Typical examples are reporting obligations to the employment and tax authorities for compliance purposes.

Other than these cases, sharing or granting access to personal data to public authorities is only lawful when expressly provided for by law and to the extent that it is necessary for the performance of a task carried out by the competent authority for the purposes of envisaged prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or for protection of vital interests of the data subjects.

Companies are only required to share or grant access to personal data to public entities or authorities where the respective applicable legal grounds are duly demonstrated by such entities or upon a court order.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Yes. Portugal has a regulated market for online games of chance and betting, whose regulator and supervisory authority is the Gambling Regulation and Inspection Authority (SRIJ). There are four different types of licences available: fixed-odds sports betting; parimutuel and fixed-odds horse racing bets; bingo; and games of chance (casino gaming and poker), and a comprehensive list of permissible and non-permissible subtypes.

Some specific online varieties are operated under an exclusive rights system by Santa Casa da Misericórdia de Lisboa (SCML) (a private charity institution of public administrative utility which traditionally holds exclusive rights for certain types of gambling) and are subject to the supervision of the social security ministry.

Engagement with these services requires prior online registration on the licensed operator's website and identity verification. Gambling is prohibited for minors (under 18 years old).

Operators cannot grant gamblers any sort of credit or loans to gamble, and gamblers cannot hold a negative credit balance with the gambling operators (ie, may not owe outstanding debts to the operators).

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

National law is applicable to online gambling provided to customers located in Portugal even where gambling is served and hosted from places outside Portugal.

Advertising gambling services is permitted by law but only by operators licensed in Portugal and specifically targeting consumers based in Portugal. Also, advertisement campaigns are subject to restrictions on format and content and must never target or feature minors.

Although operators cannot grant users access to any other non-licensed '.pt' domain platforms, in specific cases, users may play in other duly licensed and supervised platforms, provided there is a shared liquidity agreement in place.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Regarding the internal control systems applicable to credit institutions and financial entities, regulated by Notice 3/2020 of the Bank of Portugal, special attention should be given to rules governing specific topics such as the outsourcing of operational tasks underlying the pursuance of internal control functions (which can only occur in an occasional way), and the outsourcing of the IT system to support the reporting of serious irregularities concerning its administration, accounting organisation, internal monitoring and occurrence of a breach of its obligations.

Simultaneously, EBA (EBA/GL/2019/02) and ESMA guidelines on outsourcing shall be considered.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

There are no specific rules.

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

Under the general applicable law, no specific rules apply to contractual terms regarding outsourcing activities, despite sector-specific rules that may be imposed, depending on the scope of the contract or activities and the quality of the parties (a case-by-case analysis must be carried out).

Where the processing of personal data is included or implied within outsourcing contracts, service providers will most likely act as processors, performing data processing activities on behalf of the counterparty or controller (in which case the elements of article 28 GDPR must be included in the contract) or both parties will act as joint controllers (in which case the elements of article 26 GDPR must be included in the contract).

Credit institutions, investment firms, payment institutions and electronic money institutions subject to the supervision of the Bank of Portugal should take into due account EBA Guidelines (EBA/GL/2019/02) on outsourcing arrangements.

In labour relationships additional limitations are imposed, pursuing employees' protection.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

Under new article 338º-A of the Portuguese Labour Code, it is prohibited to outsource activities that were performed by an employee whose contract was terminated in the previous 12 months by collective dismissal or individual redundancy due to the elimination of the job.

Where an outsourcing does not trigger the application of the Transfer of Undertaking (Protection of Employment) (TUPE) provisions, the employer may afterwards terminate the employment contracts of the employees who carried out the outsourced activities. The dismissal should be carried out through a redundancy procedure applicable to all employees.

This procedure (either individual or collective dismissal, depending on the number of affected employees versus the company's total headcount) is foreseen in articles 359 et seq of the Portuguese Labour Code (PLC). The procedure entails a negotiation and consultation phase with existing or created ad hoc representative structures, or with the affected employees (in case of individual redundancy). The labour authorities are present at this stage. After the consultation and negotiation are carried out, in the absence of an agreement the employer may issue the dismissal decision with 15 to 75 days' notice depending on the seniority of the employee. The dismissed employees are entitled to severance corresponding to between 12 and 14 days of salary, and seniority allowances for each year of service up to 30 April 2023 and from 1 May 2023 respectively, according to article 366 of the PLC.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

Other than the standard applicable framework on intellectual property law, consumer protection laws and data protection regulations, there are no country-specific statutory provisions nor relevant case law on the development or use of these types of technologies.

In cases where the technology enables decision-making solely based on automated processing of personal data, including profiling, article 22 of the GDPR shall apply.

## IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

No. To the present date, there is no local specific law nor case law in this regard. However, Portugal follows closely the European discussion on this topic (eg, the latest EPO Legal Board of Appeal decisions).

## Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Under article 9 of Law No. 27/2021 of 17 May (Portuguese Charter for Human Rights in the Digital Age), the use of artificial intelligence and robots must be guided by respect for fundamental rights, ensuring a fair balance between the principles of explainability, security, transparency, and accountability, taking into account the circumstances of each specific case and establishing processes designed to avoid any bias and forms of discrimination.

On 14 June 2023, the European Parliament adopted its final position regarding the European Artificial Intelligence Regulation proposal, which aims to regulate the development and use of artificial intelligence, ensuring that it is safe, transparent, trackable, non-discriminatory and respectful of the environment.

As at the time of writing, there is no local specific law or guideline.

# TAXATION

## Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

The sale of digital products or rendering of digital services is taxable in Portugal, if these are performed by a Portuguese resident company or a non-resident entity with a permanent establishment located herein, and are reflected in the company's accounting. Regarding non-resident entities' permanent establishment, it is the Portuguese tax authorities' opinion that corporate income tax may be due and tax obligations exist for entities whose servers are located in Portugal.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

The Portuguese tax authorities' opinion in this regard is that a permanent establishment exists in Portugal when a non-resident entity installs a server or other physical platforms in the country. If a permanent establishment is deemed to exist in Portugal, the income derived by such establishment should be taxable in Portugal, under both domestic legislation and the terms of double taxation treaties (as per the OECD model convention).

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The invoicing rules in Portugal do not distinguish between the type of business, market or segment, being applicable to all. Invoices in Portugal are issued electronically and must contain several elements (eg, a QR code and an ATCUD code). The invoicing programs used by resident entities must be certified by the Portuguese tax authorities and there are obligations of immediate or monthly reports of the same to the Portuguese tax authorities.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no specialist courts based on the online or digital-related nature of the subject matter of a legal action per se.

However, based on the type of claim or type of service underlying the claim, the following venues may be competent for certain matters, among others (such as ADR methods), deemed relevant for online/digital business:

- The Intellectual Property Court (specialist court for IP matters), which is competent for settling disputes on authorship, industrial property rights and domain names; unfair competition and, in some cases, violation of trade secrets; and appeals against decisions of the General Inspectorate of Cultural Activities (IGAC), in administrative infringement proceedings.
- The IGAC (Inspectorate General for Cultural Activities), which has powers of control, removal and prevention of access in the digital environment to protected content and may apply administrative offence fines to intermediary networking service providers. It

is also responsible for handling complaints from holders of the infringed authorship or related rights (see Decree Law 47/2023 transposing Directive 2019/790).

## ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

As a principle, resort to ADR methods in Portugal is done on a voluntary basis.

There are no specialist ADR methods based on the online or digital-related nature of the subject matter of a legal action. Based on the type of claim or type of service underlying the claim, cases can be dealt with through one of the following:

- consumer alternative dispute resolution entities integrated with the European Online Dispute Resolution (ODR) platform under Regulation (EU) 524/2013: competent for disputes concerning products or services bought online in the EEA;
- mediators and justices of peace, in certain cases; and
- ARBITRARE (institutionalised arbitration centre): competent for matters related to industrial property rights, .pt domain names, trade names and corporate names.

Suppliers of goods or services providers (including credit, financial and payment institutions and electronic money institutions) must inform consumers about the competent ADR centres for settling a dispute. For consumer disputes up to €5,000, resort to arbitration or mediation is mandatory, upon the consumers' express request.

# UPDATE AND TRENDS

## Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The past few years have seen huge momentum for technological breakthroughs, due in part to challenges relating to reliability of communications networks, and to the dematerialisation of consumer patterns, resulting in massive digitalisation of business.

This coincided with a period of revolution in the Portuguese communications paradigm, with the introduction of the fifth generation of mobile services (5G) in communications networks, as well significant proliferation of new legislation in the aftermath of the transposition (finally) of the European Electronic Communications Code and the changes in consumer protection laws (implementation of Directives 2019/771, 2019/770 and Directive 2019/2161/Omnibus), which have been ongoing since 2022.

2023, as anticipated, has been and is expected to continue to be a fruitful legislative year in these areas, mainly for consolidation of recent trends.

The implementation of the legislative package (ePrivacy Regulation, Artificial Intelligence Act, Digital Markets Act and Digital Services Act) and upcoming full entry into force will necessarily have a major impact on digital transformation and doing business online, enabling harmonisation of the legal framework throughout the EU market and the reinforcement of consumer protection and confidence, which is bound to increase growth in this sector, as well as to force companies, individuals and all interest holders to adapt their behaviours to the new reality and markets.

In respect of digital assets in the financial sector, there are two main regulations that should now be taken into consideration: (1) Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA); and (2) Regulation (EU) 2022/858, of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (DLT Regime).

On one hand, MiCA sets out a pioneering pan-European harmonised and comprehensive regulatory framework covering the issuance, offer and trading of crypto-assets and the provision of related services, which also considers the environmental impact disclosure for investors. To that extent MiCA:

- regulates the issuance and admission to trading of crypto-assets (including transparency and disclosure requirements);
- introduces licensing for crypto-asset service providers, issuers of asset-backed tokens and issuers of e-money tokens;
- clarifies regulatory obligations applicable to asset-linked token issuers, e-money token issuers and crypto-asset service providers, including consumer protection rules for the issuance, trading, exchange and custody of crypto-assets;
- strengthens confidence in crypto-asset markets by establishing a market abuse regime that prohibits market manipulation and insider trading; and
- clarifies the powers, including the framework for cooperation and sanctions, entrusted to competent authorities.

The next steps for MiCA will entail: (1) the entry into force of new requirements for stablecoins issuers (asset reference tokens, e-money tokens and overall crypto-assets issuers) by June 2024; (2) the publication of Regulatory Technical Standards (RTS) by ESMA and EBA; which will lead to (3) the entry into force of the Regulation for crypto-asset service providers (CASPs) 18 months later (by December 2024).

On the other hand, the Distributed Ledger Technology (DLT) Regime establishes the applicable requirements for DLT market infrastructures and their operators, setting out:

- the applicable requirements for existing permissions – and exemptions - to operate DLT market infrastructures;
- the requirements for mandating, modifying and withdrawing the conditions attached to exemptions and for mandating, modifying and withdrawing compensatory or corrective measures;
- the requirements for operating DLT market infrastructures;

**Read this article on Lexology**

- the requirements for supervising DLT market infrastructures; and
- the rules on the cooperation between operators of DLT market infrastructures, competent authorities and the European Supervisory Authority.

From a tax standpoint, tokens and cryptocurrency are a hot topic, since Portugal enacted a personal income tax regime for income arising from cryptocurrency, which came into force on 1 January 2023. In a nutshell:

- sale of NFTs are excluded from taxation;
- gains arising from the sporadic sale of cryptocurrency are not subject to taxation if held for at least 365 days;
- nonetheless, if the trading in cryptocurrency is perceived as a business activity – due to the regularity with which it is performed – as well as mining, it will be subject to tax at the level of the individuals, at the progressive rates;
- staking will qualify as capital income and be subject, as a rule, to a flat 28 per cent rate;
- from a corporate income tax perspective, and as it happened prior to 2023, if the gains are reflected in the accounts, they should be subject to tax; and
- there will also be stamp duty charges on crypto-asset service providers.

From a labour standpoint, the alterations to the Portuguese Labour Code reflecting the government's Agenda on Dignifying Work and Valuing Young People in the Labour Market, which entered in force on 1 May 2023, include the following measures:

- creating a legal assumption of the existence of an employment contract between platforms and gig workers and between the latter and customers;
- imposing on employers a duty of information to the Labour Inspectorate, employees and their representatives, on the criteria of algorithms and artificial intelligence mechanisms used to make decisions on access to and retention of employment, as well as working conditions, including profiling and monitoring of professional activity; and
- forbidding the acquisition of third-party services to satisfy needs that have been assured by an employee whose contract terminated in the previous 12 months due to collective dismissal or redundancy, in a measure meant to prevent the replacement of employees' work with outsourcing.

Sérvulo & Associados | Sociedade de Advogados, SP, RL

| | |
|---|---|
| Ana Rita Paínho | arp@servulo.com |
| Verónica Fernández | vf@servulo.com |
| Teresa Pala Schwalbach | tps@servulo.com |
| Rita Canas Da Silva | rcs@servulo.com |
| Ana Mira Cordeiro | ami@servulo.com |

Rua Garrett 64, Lisbon 1200-204, Portugal
Tel: +351 21 093 30 00
www.servulo.com

**Read more from this firm on Lexology**

**Read this article on Lexology**

# Taiwan

Robin Chang and Eddie Hsiung
Lee and Li Attorneys at Law

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

In 2016, the Executive Yuan (ie, Taiwan's cabinet) initiated the Digital Nation & Innovative Economic Development Program 2017–2025 (DIGI+ Program) and Smart Nation Program to establish the Taiwanese government's digital policies, including implementing the digital foundations for and increasing the coverage of 5G broadband, enhancing digital innovation, establishing digital governance to facilitate legal innovation and forming digital inclusion to close the digital divide.

On 11 November 2017, the Consumer Protection Committee of the Executive Yuan expressed the government's position towards digital business by announcing the Guidelines for Consumer Protection in the Context of Electronic Commerce (E-commerce Guidelines), which require that online transaction-related information, including payment methods or terms and conditions, as disclosed to the consumers, must be sufficient, correct, clear and easy to understand. The E-commerce Guidelines also indicate the government's current commitments in respect of internet issues are to ensure fair online transactions, encourage the sound developments of e-commerce and implement relevant responsibilities towards businesses and related organisations.

On 27 August 2022, the Ministry of Digital Affairs (MODA) (which is under the Executive Yuan) was formally established for matters in relation to facilitating Taiwan's digital development of its telecommunications, information, cyber security, internet and communications industries, coordinating national digital policies, supervising national cyber security policies, managing communications and digital resources and assisting digital transformation. Also, the MODA established two subordinate agencies, the Administration of Digital Industries and the Administration of Cyber Security, to plan and implement policies in relation to facilitating the development of digital economy related industries and reviewing and supervising national cyber security programmes.

On a separate note, on 30 June 2022, the National Communication Committee (NCC) issued the draft Digital Intermediary Service Act (DISA), which would govern digital intermediary (DI) service providers, onshore and offshore (if having a 'substantial connection' with Taiwan). The DISA provides for relevant general obligations for all DI service providers, for example obligations to disclose their basic information and contact information and to designate an agent in Taiwan (applicable to DI service providers without a commercial presence in Taiwan), as well as obligations for providers of hosting services, online platform service providers and the online platform service providers designated by the NCC. However, it is reported that as there were concerns that the DISA would harm freedom of speech, discussion on the draft DISA was temporarily suspended, and whether the draft will be passed by the Legislative Yuan is uncertain.

## Legislation

### 2 What legislation governs digital content and services, digital transformation and the conduct of business online?

At the time of writing, in Taiwan there are no general laws governing digital content and services, digital transformation and the conduct of business online. From a Taiwanese legal perspective, generally e-commerce is not treated differently from non-e-commerce businesses, and is equally subject to the same Taiwan laws and regulations, including the Taiwan Civil Code (specifically provisions governing contracts), and the Personal Data Protection Act (PDPA) to the extent personal data is involved.

Relevant specific legislations in respect of online business matters also include, without limitation:

- the Electronic Payment Institutions Act (E-payment Act), which governs electronic payment institutions and related services;
- the Consumer Protection Act (CPA), enacted to protect the interests of consumers; and
- the Electronic Signatures Act (ESA), which aims to encourage the use of electronic transactions, ensure the security of electronic transactions, and facilitate the development of e-government and electronic commerce.

## Regulatory bodies

### 3 Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

Since there is no single set of regulations governing digital content and services, e-commerce and artificial intelligence, regulatory bodies concerned may vary in respect of different aspects of operations, business models and, depending on the products, industries and regulations involved. For example, if a consumer purchases a cell phone via the internet, the purchase itself should be subject to the CPA; the advertisement of such product will be governed by the CPA as well as the Fair Trade Act; the payment may be subject to the Banking Act, credit card-related regulations, the E-payment Act, etc, and the information concerning said consumer will be subject to the PDPA; the Taiwan regulatory bodies of the aforementioned laws and regulations are the Fair Trade Commission (FTC), the Executive Yuan, Financial Supervisory Commission and National Development Council respectively. In addition, telecommunications-related regulations are governed by the NCC.

## Jurisdiction

### 4 What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

The jurisdiction for online transactions or disputes in relation to digital businesses should depend on the agreement of the contractual parties unless there exist any mandatory rules

for the purposes of civil procedures. However, in case a Taiwanese customer is involved, we cannot rule out the possibility that the Taiwan court would still accept and review a case in order to protect the Taiwan consumer's rights and interests even if the parties have agreed to submit to the jurisdiction of foreign court in the terms and conditions entered into by the parties.

### Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

From the perspective of company establishment, there are no special regulatory or procedural requirements to establish a digital business and for the sale of digital content and services in Taiwan compared to a brick-and-mortar business.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

In Taiwan, digital contracts and agreements can be formed by way of meeting of minds and other elements such as offer and acceptance, and these can be expressed and evidenced by way of electronic records, unless otherwise provided by law (eg, requirements regarding 'execution', 'writing' and certain other requirements), depending on the types of contracts or agreements.

In addition, on 27 June 2023, the Ministry of Digital Affairs (MODA) issued the draft amendment to the Electronic Signatures Act (ESA) to specify, among others, that 'electronic documents' and 'electronic signature', as defined in the ESA, would be functionally equivalent to physical documents and signature respectively, and the consent of the counterparty would not be required for the use of electronic documents or electronic signature, considering that the use of documents or signature in practice is not limited to legal acts with a counterparty. However, where the use of documents or signature involves a counterparty, the counterparty must be given an opportunity to refuse using electronic form or be provided with alternative options. The draft is still under review and it is uncertain whether it will be passed.

## Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

There are no general laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts. However, the Consumer Protection Act (CPA, which provides for a relevant protection mechanism for customers) would apply if the contract is regarding consumption by a consumer. One of the guiding principles of the CPA is 'full disclosure' to customers, so if the CPA applies, it might not be appropriate for business-to-consumer e-commerce operators to use language other than the local language (ie, mandarin Chinese) for the contract with customers.

## Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Digital or e-signatures are governed by the ESA. Pursuant to the ESA, there are two types of electronic contracting that could address the relevant legal requirements of 'wet-ink execution' (ie, by way of wet-ink signatures or chops) or 'physical writing' under Taiwan law unless otherwise specified: digital signature (for wet-ink execution) and electronic document (for physical writing).

In the context of the ESA, digital signature is an electronic signature generated by the use of a mathematical algorithm or other means to create a certain string of digital data encrypted by the signatory's private key that can be verified by a public key. On the other hand, documents may be executed in electronic form (ie, electronic document) once the following requirements are met:

- the consent of the counterparty has been obtained;
- the content of the documents can be displayed in its entirety;
- the content of the documents remains accessible for subsequent verification; and
- the use of electronic documents is not specifically excluded by other laws, regulations or public announcements of government agencies.

Specifically, under the ESA, if a digital signature is used, the contract must be evidenced by a certificate issued by a certification service provider in accordance with the requirements of the ESA. Such certificate service providers must refer to those that have been approved by the competent authority under the ESA.

However, according to the draft amendment to the ESA issued by the MODA on 27 June 2023, the consent of the counterparty would not be required for the use of electronic documents or electronic signature, considering that the use of documents or signature in practice is not limited to legal acts with a counterparty. In addition, the draft amendments also provide that the administrative authority shall not exclude the application of this Act through orders

or announcement, except where the application of technology and procedures for electronic documents and electronic signature are separately regulated or announced.

### Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

There are no forums for dispute resolution, nor remedies specifically available, for breach of digital contracts (as opposed to non-electronic contracts).

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

In general, regulations in respect of advertising and selling financial services products via the internet are set out in the Fair Trade Act, Measures for Financial Services Industry Engaged in Advertising Business Recruitment and Business Promotion Activities, and the Financial Consumer Protection Act. In addition, considering the diversity and complexity of financial services products, industry-specific or product-specific regulations may apply. For example, a securities investment consulting enterprise may not use exaggerated or biased representations in advertising, public information meetings, or other promotional activities, and must report every advertising campaign, public information meeting, or other promotional activities to the competent authority within 10 days of occurrence of the activity.

### Electronic money and digital assets

**11** Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

In Taiwan, there are no rules or restrictions regarding the issue of digital currencies, except in relation to those with the nature of securities, which are commonly called 'security tokens' and encompass all the following attributes of an investment:

- funding provided by investors;
- funding for a common enterprise or project;
- investors expecting to receive profits; and
- profits generated primarily from the efforts of the issuer or third parties, and their offerings are commonly called 'security token offerings'.

The issuance, transfer and use of security tokens is subject to the sets of regulations governing security token offerings (STO) as set out by the Financial Supervisory Commission (FSC) and the Taipei Exchange.

Also, in respect of anti-money laundering, the Money Laundering Control Act (AML Act), which took effect on 7 November 2018, has included cryptocurrency platform operators in the regulatory scope of anti-money laundering. Meanwhile, the Executive Yuan (Taiwan's cabinet) issued a ruling stating the scope of enterprises of 'virtual currency platforms and trading business' under the AML Act, which includes, among others:

- exchange between virtual currencies and New Taiwan dollars, foreign currencies or currencies issued by Mainland China, Hong Kong or Macao;
- exchange between virtual currencies, transfer of virtual currencies, custody and administration of virtual currencies and providing instruments enabling control over virtual currencies; and
- participation in and provision of financial services related to issuance or sale of virtual currencies.

Furthermore, the FSC promulgated the Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises of Virtual Currency Platforms and Trading Business (Crypto AML Regulations), which took effect on 1 July 2021, indicating that the designated operators of crypto assets and exchanges are required to establish, among others, an internal control and audit mechanism, a procedure for reporting suspicious transactions and the know-your-customer procedure.

The FSC, however, issued a press release on 30 March 2023 stating that it will serve as the competent authority for virtual asset platforms of a financial investment or payment nature, and will establish nine guiding principles, which include information disclosure of virtual asset platforms, product launch and discontinuation review, separate custody of customer and platform assets, fair and transparent transactions, anti-money laundering, protection of customer rights, information security, operating systems and hot and cold wallet management and institutions review, to strengthen industry self-discipline and information disclosure before the end of the third quarter of 2023. It would be prudent for industry players to pay attention to the potential regulatory developments in Taiwan.

## Digital and crypto wallets

### 12 Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Assuming the digital currencies do not have the nature of securities, the provider of crypto wallets will be subject to the Crypto AML Regulations if such provider is considered as within the scope of enterprises of 'virtual currency platforms and trading business' (specifically, 'custody and/or administration of virtual currency or providing instruments enabling control over virtual currencies').

From the perspective of the holders of digital assets, there are no restrictions on the use of crypto wallets or other methods of digitally storing currencies.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

The E-payment Act governs the online payment sector in Taiwan. Under the current amended E-payment Act, the scope of business of a new e-payment institution includes core businesses, and ancillary and derivative businesses. The core businesses under the E-payment Act are:

- collecting and making payments for real transactions as an agent;
- accepting deposits of funds as stored-value funds;
- small amount domestic and cross-border remittance services; and
- foreign exchange services relating to the core businesses.

The amended E-payment Act also permits qualified non-e-payment institutions to apply to become a cross-border remittance service provider exclusively for foreign workers in Taiwan.

As to third-party access to digital information in bank accounts, the FSC has requested the Bankers Association to set out relevant self-regulatory rules to implement the concept of 'open banking' in Taiwan to reflect relevant advocacy from some industry experts and market players. From a policy viewpoint, the FSC decided not to set out any mandatory disclosure rules for banks, but, instead, requested the self-regulatory organisation (ie, the Bankers Association) and the Financial Information Service Co to set out relevant rules and information security standards for banks to follow. According to the relevant newsletters, a 'three-phase approach' is adopted by the FSC for open banking. Phase I was launched in 2019, during which public product information was made searchable by the third-party service providers (TSP). Phase II involves access to customer data. Phase III will involve processing of transactions – it is reported that Phase III will be launched in 2024 at the soonest.

## Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Under Taiwan laws, entities required to carry out KYC and AML under Taiwan's AML law (Money Laundering Control Act) are financial institutions and certain non-financial ones. Generally, those institutions are required to carry out customer due diligence by themselves unless otherwise approved by the competent authorities. Also, it is possible that use of the services of third parties (if approved by the competent authorities) may be considered 'outsourcing' of the institution's operation to a third party, which might be further subject to the outsourcing regulations applicable to such institutions.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

There are no specific procedures or restrictions governing the licensing and use of domain names or URLs. Neither are there any regulatory restrictions around the use of URLs to direct users of websites, online resources or metaverses in Taiwan.

The application procedures for registering '.tw' (ie, Taiwan) domain names are as follows:

- choose the accredited registrars and finish registration of certain information;
- reply to the email to confirm the application;
- complete the payment process; and
- set up the domain name system. It is possible to register a .tw domain name without being resident in Taiwan, subject to certain restrictions.

### IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Under the Taiwan Trademark Act, registration of a domain name or URL that is identical or similar to a well-known third-party registered trademark may constitute a trademark infringement.

According to the Domain Name Dispute Resolution Rules established by the Taiwan Network Information Centre (TWNIC) for resolving disputes relating to domain names and URLs, in the event that the registrant's domain name or URL is identical or confusingly similar to a trademark, mark (label), personal name, business name or other emblem of a third party, apart from taking legal action, such party may file a complaint to the eligible domain name dispute resolution service provider (ie, a neutral body recognised by TWNIC, currently the Science & Technology Law Institute and the Taipei Bar Association) to determine whether the domain name or URL will be cancelled or transferred.

## ADVERTISING

### Regulation

**17** What rules govern online advertising?

In general, the laws and regulations applicable to advertising should also apply to advertising on the internet (including in the metaverse). The main laws include, among others, the Consumer Protection Act (CPA) and the Fair Trade Act (FTA) (and relevant enforcement rules, guidelines, etc).

Pursuant to the newly amended Disposal Directions (Guidelines) on Online Advertisements of the Fair Trade Commission (FTC), online advertising refers to the actions, for the purposes of selling its products or services, that a business adopts to disseminate information, via the internet, with regard to products or services in order to attract trading opportunities, including advertising for the business' website, shopping website advertisements, online store advertisements, social networking site advertisements, email advertisements, and fax advertisements. In addition, the amended FTC Disposal Directions stipulate that advertisement hosts will include bloggers, internet influencers and livestream hosts.

Advertisement refers to the conduct of disseminating messages or content of promotion by means of television and radio broadcasting, films, slides, newspapers, magazines, flyers, posters, signboards, arches, computers, facsimiles, electronic video, electronic voicemail or other, to the general public pursuant to the CPA.

### Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Pursuant to the Disposal Directions (Guidelines) on Online Advertisements promulgated by the FTC, online advertising refers to the actions, for the purposes of selling its products or services, that a business adopts to disseminate information, via the internet, with regard to products or services in order to attract trading opportunities, including advertising for the business' website, shopping website advertisements, online store advertisements, social networking site advertisements, email advertisements, and internet fax advertisements. In addition, advertisement refers to the conduct of disseminating messages or content of promotion by means of television and radio broadcasting, films, slides, newspapers, magazines, flyers, posters, signboards, arches, computers, facsimiles, electronic video, electronic voicemail or others, to the general public pursuant to the Consumer Protection Act.

There are no rules governing targeted advertising and online behavioural advertising, but compliance with the Personal Data Protection Act (PDPA) (ie, obtaining informed consent) is required if collection, processing and use of personal data would be involved.

## Misleading advertising

### 19 | Are there rules against misleading online advertising?

Both the Consumer Protection Act and the FTA adopt the concept of 'truthful representations' and 'full disclosure'. For example, pursuant to the FTA, no enterprise shall make or use false or misleading representations or symbols in matters that are relevant to goods and sufficient to affect trading decisions, such as the price, quantity, quality, content, production process, production date, valid period, method of use, purpose of use, place of origin, manufacturer, place of manufacturing, processor and place of processing. The FTC's Disposal Directions also provide examples of false or misleading representations or symbols with respect to online advertising (eg, the advertisement does not clearly specify time, methods of use, or types of online sweepstakes). Further, a business operator violating the Disposal Directions would be deemed as violation of the FTA.

While not required under the law, in practice it is suggested that a business operator must be able to substantiate claims (eg, reports by independent and credible third parties, survey results from qualified market research companies or certificates from regional or national standards boards), and file and record all substantiation if the authorities (eg, the FTC) request copies. The above rules apply to all products and services, and there would be additional rules applying to industry-specific industries.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

There exists no specific prohibition on 'online advertisement' for 'digital' products or services in Taiwan, if they are legal. However, please note the following illegal activities for online advertisement:

- advertisement of regulated products or services that have not been approved by the regulator, such as online advertisement of a 'digital' banking service that does not have the prior approval or licence from the Financial Supervisory Commission; and
- advertisement of digital products or services that involve defamation (articles 309 and 310 of the Criminal Code) or distributing obscene material (article 235 of the Criminal Code).

## Direct email marketing

### 21 | What regulations and guidance apply to email, SMS and other direct marketing?

Currently, no law regulating email, SMS and other distance marketing has been specifically promulgated in Taiwan. Compliance with the PDPA (ie, obtaining informed consent) is required if collection, processing and use of personal data would be involved.

The draft Regulations on the Administration of Commercial E-mail Spam were proposed by the Congress to ensure accessibility online and for the government to promote a more secure and efficient IoT (Internet of Things) environment. The draft Regulations only target commercial emails, not other messaging systems such as WhatsApp, Facebook Messenger,

Messages by Google, Signal and Telegram. However, the draft is still under review by Taiwan's congress, and it is uncertain whether this draft will be passed.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

In Taiwan, the liabilities of parties (eg, internet service providers (ISPs), telecommunications providers and other parties that merely host and display the content written or published by third parties) for hosting the content would depend on the actual act involved with the liability of content providers (eg, liabilities under the Copyright Act (CA) for copyright infringement, liabilities for misleading advertising under the Fair Trade Act (FTA) and the Consumer Protection Act (CPA), and liabilities for defamation under the Civil Code and the Criminal Code). For example, for misleading advertising, relevant Taiwan court precedents hold that an ISP (or other website provider) may be deemed an advertising medium and will be subject to the FTA and the CPA, under which it may be jointly and severally liable with the violators if it knows or should have known such advertisement to be misleading but fails to delete such advertisement.

Providers that merely host and display the content written or published by third parties may be able to mitigate their liability. For example:

- to be exempted from liability for copyright, an ISP may adopt measures that satisfy all the conditions required for 'safe harbour' under the CA;
- for other civil and criminal liability, an ISP:
    - must clearly inform the users of the ISP's policy to protect the rights of all users and have in place relevant technical measure for the above purpose;
    - must have the content providers agree with the terms and conditions under which the content providers shall comply with laws in full and shall not upload, post or otherwise provide any content that might infringe or breach the right of others; and
    - may, for example, take down the content at the sole discretion of the ISP, if the ISP receives notice from the legitimate right holders that the content provider has breached or infringed the rights of the right holders, or the ISP otherwise has knowledge of such breach or infringement.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

In Taiwan, there is no specific law regulating information provided by a digital platform or online content provider. The liability of a digital platform or online content provider for

mistakes in information and whether such liability can be avoided will depend on the nature of such information (eg, if the information infringes the copyright of a third party, the website provider may be liable under Taiwan Copyright Act; and if the information contains misinformation regarding communicable disease, the website provider may be liable under the Communicable Disease Control Act).

Generally, a website provider, including a social media platform, would not be responsible for reviewing or supervising the information provided by its users. However, pursuant to the Copyright Act and the draft Digital Communications Act, once receiving a notice stating that the content infringed their rights, the website provider must immediately remove the infringing content and notify the provider of the content to avoid liabilities for infringements.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

An ISP or telecommunications provider can shut down a web page containing defamatory material without court authorisation if it is permitted by the terms and conditions of use offered to and agreed by its users or otherwise required by applicable law.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

Under Taiwan law, databases are copyright-protected (provided that certain requirements are met, such as that the selection and arrangement of materials of the database must have a certain degree of creativity). The owner of the copyright has the right to stop other people from using or reproducing data from those databases.

### Third-party links and content

**26** Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Under the Taiwan Copyright Act, a website, digital platform or other online content provider (including a metaverse) that shares the content of third-party websites or platforms (or digital content within those websites or platforms) by embedding the web link to said websites without actually reproducing such content would not be considered copyright infringement since no reproduction or public transmission by said website owner would be actually involved. Therefore, a permission to link to third-party websites may not be required. However, the website owner may be liable for copyright infringement if he or she knowingly embeds the link that has infringed copyright of any third parties (in which case, such website owner would be deemed to be in violation of the right to public transmission of the copyright owner).

**27** Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

A website, digital platform or other online content provider (including a metaverse) cannot use third-party content, obtained via automated scraping or otherwise, without permission from a third-party content provider unless the use is considered a fair use under the Copyright Act. Unless otherwise provided for in the Copyright Act, for determining whether the exploitation of a work would be deemed a fair use, all circumstances and facts involved will be taken into account, and in particular the following facts will be noted as the basis for determination:

- the purposes and nature of the exploitation, including whether such exploitation is of a commercial nature or is for non-profit educational purposes;
- the nature of the work;
- the amount and substantiality of the portion exploited in relation to the work as a whole; and
- effect of the exploitation on the work's current and potential market value.

The use of third-party content on one's website in violation of the Copyright Act may result in civil or criminal liabilities (or both).

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

While Taiwan has not promulgated any laws or regulations specifically for metaverses, a particular intellectual property-related issue would be the jurisdiction or country in which the intellectual property is used in the context of metaverses. There would then be difficulties as to determining, for example, the location of the IP infringement.

Also, a hotly discussed issue is the classification of goods and services for trademark registration in relation to the metaverse. For example, the class for sneakers in the 'real world' should be different from the 'virtual sneakers' in a metaverse.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Yes, the concept of exhaustion of rights (or the first-sale doctrine) is recognised by Taiwan's Copyright Act, Trademark Act and Patent Act. It is generally understood that the Copyright Act recognises 'national exhaustion', while the Trademark Act and Patent Act adopt 'international exhaustion'. As to metaverses, there have not been many discussions about whether any such rights would be exhausted by placing the digital product on a metaverse. The key factors to determine the application of the first-sale doctrine would include: (1) whether the

doctrine should cover 'sale' on a metaverse or 'sale' of digital products; and (2) whether the sale on a metaverse would be considered to occur in Taiwan.

## Administrative enforcement

### 30 Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Under Taiwan law, only judges, prosecutors, judicial police officers, or judicial police are authorised to take search and seizure actions in accordance with the Code of Criminal Procedure. A search warrant issued by the competent court and signed by a judge is usually required for competent authorities to conduct a search or a seizure. Therefore, no dawn raids can be carried out unless criminal proceedings have been initiated with regard to the IP infringement.

From the perspective of civil remedies, depending on the circumstances and the facts involved, the infringed may apply for provisional remedies (provisional attachment, preliminary injunction, or injunction maintaining the temporary status quo) in connection with the intellectual property rights in accordance with the Intellectual Property Case Adjudication Act and Taiwan Code of Civil Procedure.

## Civil remedies

### 31 What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

The civil remedies available to IP owners may vary depending on the type of the IPR being infringed (ie, copyright, trademark, patent, etc). Civil remedies will include, but not be limited to, removal of infringement, damages, and appropriate measures necessary for the restoration of the IP owner's reputation (eg, indication of the author's name or appellation, correction of content).

Depending on the circumstances and the facts involved, the IP owner may apply for provisional remedies (provisional attachment, preliminary injunction, or injunction maintaining the temporary status quo) in accordance with the Intellectual Property Case Adjudication Act and Taiwan Code of Civil Procedure.

Only in criminal proceedings may a search warrant be applied for in accordance with the Code of Criminal Procedure.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

According to the Personal Data Protection Act (PDPA) and the Enforcement Rules of the PDPA (Enforcement Rules), 'personal data' refers to a natural person's name, date of birth, ID card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other data that may be used to directly or indirectly identify a natural person.

'Sensitive personal data' refers to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records, which should not be collected, processed or used unless otherwise specified by applicable laws. Sensitive personal data must not be collected, processed or used unless:

- it is expressly required by law;
- it is within the necessary scope for a government agency to perform its statutory duties or for a non-government agency to fulfil its statutory obligation;
- the personal data has been disclosed to the public by the data subject or has been made public lawfully;
- it is necessary for statistics gathering or academic research by a government agency or an academic institution;
- it is necessary to assist a government agency in performing its statutory duties or a non-government agency in fulfilling its statutory obligations; or
- the data subject has consented to the collection, processing and use of his or her personal data in writing.

### Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Under the PDPA, there is no such registration system, nor a requirement regarding appointment of an in-house data protection officer.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

Pursuant to article 51 of the PDPA, the PDPA would also apply to government and non-government entities when they collect, process or use the personal data of Taiwan individuals from offshore. However, according to a ruling issued by the Ministry of Justice in 2018, article 51 of the PDPA would apply only when the collector is a Taiwanese government entity or a Taiwanese non-government entity. Therefore, there is no requirement for a foreign organisation or individual to appoint a representative in Taiwan. Please note that this point of view is still subject to court test. In addition, it is possible that collecting personal data via the internet may be challenged as collecting personal data 'in Taiwan' and therefore, the PDPA will apply.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

Under the PDPA, unless otherwise specified, a non-governmental entity is required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing or using personal data, subject to certain exemptions. In other words, obtaining 'informed consent' from the data subject is required.

Although the PDPA provides for certain other legal bases for a non-governmental entity to collect or process personal data, obtaining informed consent from the data subject is the most common and least controversial approach in practice.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

The cross-border transfer of personal data constitutes 'international transmission' as defined in the PDPA, which is, in principle, permitted unless the competent authority issues any order to prohibit or restrict such transfer.

Under the current regulatory regime, there are no data sovereignty or national security rules that require data, data servers or databases to remain in Taiwan.

### Sale of data to third parties

**37** May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

Selling personal data is prohibited under the PDPA and a non-governmental agency's non-compliance may result in civil, criminal and administrative liabilities.

### Consumer redress

**38** What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Article 3 of the PDPA provides that a data subject can exercise certain rights with regard to his or her personal data – for example, the right to supplement or correct his or her personal data, the right to demand the cessation of the collection, processing or use of his or her personal data, and the right to delete his or her personal data – by contacting the data collector in any manner. A data subject may also seek damages against the data collector in case of the data collector's violation of the PDPA.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

No law directly regulating the use of non-personal data has been specifically promulgated in Taiwan. However, the use of non-personal data may still be regulated, depending on the information involved. For example, the Trade Secrets Act would apply if any method, technique, process, formula, program, design, or other information that may be used in the course of production, sale or operations and that meets the 'trade secret' conditions as stipulated in the Trade Secrets Act is involved. In addition, the Copyright Act would apply if any creation that is within a literary, scientific, artistic, or other intellectual domain that meets the 'word' conditions as stipulated in the Copyright Act is involved.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Under Taiwanese laws and regulations, there are still many documents that cannot be executed in electronic form, such as:

- notarised deeds, as well as deeds of attestation;
- formalities regarding creation and perfection of mortgage (both real estate mortgage and chattel mortgage); and

- formalities regarding pledge over shares with physical certificates and listed shares in Taiwan.

However, according to the draft amendments to the Electronic Signatures Act issued by the Ministry of Digital Affairs on 27 June 2023, the administrative authority shall not exclude the application of this Act through orders or announcement, except where the application of technology and procedures for electronic documents and electronic signature are separately regulated or announced.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Under Taiwanese laws and regulations, there are still many requirements regarding minimum periods for which documents or other record types should be kept. For example, a company's minutes of board meetings and shareholders' meetings should be kept permanently, while the attendance sheet should be kept for one year generally. Also, there are record-keeping requirements for a company's accounting records. For example, a company's financial statements should be kept for 10 years, while the vouchers for relevant accounting items should normally be kept for five years.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

According to the Mandatory and Prohibitory Provisions of Standard Contracts for Retail Industry and Other Online Transactions (promulgated for the purpose of consumer protection under the Consumer Protection Act (CPA)), business operators are required to establish a security mechanism that meets transaction needs and inform consumers of the security level of such mechanism. In addition, the E-commerce Guidelines also instruct businesses to take specific measures to guarantee transaction security, such as taking appropriate measures to protect payments and personal data transmitted to and stored in the database of the businesses.

For personal data protection, the central competent authorities have the power to stipulate rules concerning a 'security and maintenance plan for personal data files' in the industry sectors under their supervision. For example, the central competent authority in charge of the online retail industry has stipulated such rules for this sector and requires relevant business operators to have in place relevant plans and measures for ensuring the security of personal data.

## Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

There are no cybersecurity laws specific to e-commerce. Pursuant to Taiwan's Cyber Security Management Act, which is the first piece of cybersecurity-focused legislation in Taiwan, companies are required to comply with certain obligations (such as requirements for meeting a specific security level) only if they are designated by the Taiwan government as the 'critical infrastructure providers'.

Under the Personal Data Protection Act (PDPA), if any personal data is stolen, leaked, altered, or otherwise infringed upon due to a violation of the PDPA by a government or non-governmental agency, the data subject must be notified after the relevant facts have been clarified.

Although the PDPA does not require that data breaches be reported to the government authorities, the central competent authorities have the power to stipulate further rules concerning a 'security and maintenance plan for personal data files' in the industry sectors under their supervision. For example, the central competent authority in charge of the online retail industry has stipulated such rules for this sector and requires relevant business operators to report any incident that is material and may impact on the normal operations of the business or the interests of numerous data subjects.

## Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

According to the PDPA, a government agency may collect personal data for specific purposes and on any of the following bases:

- where it is within the necessary scope to perform its statutory duties;
- where consent has been given by the data subject; or
- where the rights and interests of the data subject will not be infringed upon.

Also, under relevant sector-specific regulations (regardless of whether such regulations are about data or not), a company would usually be required by the competent authority to provide materials and information (which may include personal data) for the authority's supervision and investigation, etc.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Gambling is prohibited under Taiwan law, except for Public Welfare Lottery and Sports Lottery, which are specifically permitted under relevant laws and regulations. According to court decisions, an online gambling website still constitutes a 'place of gambling'. Under Taiwan's Criminal Code, anyone who operates an online gambling business with the intent to make a profit in Taiwan may be subject to criminal liabilities.

Pursuant to article 266 of the Criminal Code, from the perspective of customers, only those who 'gamble in a public place or a place open to the public' (Public Requirement) would be committing a criminal offence. A Supreme Court decision that has been cited very often (Ref No. 107-Tai-Fei-Zi-174) held that gambling via the internet with required login (ie, using a registered account and password) by customers is not a gambling offence since such activity is not publicly accessible by third parties (ie, it fails to meet the Public Requirement).

However, in response to the controversies stirred up by the above-mentioned Supreme Court decision, the Executive Yuan (Taiwan's cabinet) proposed a draft amendment to the Criminal Code in 2020, under which gambling through 'telecommunication devices, electronic communications, the Internet or other comparable tools' would be considered a criminal offence. However, the draft is still under discussion, and whether this draft will be passed by the Legislative Yuan (the Congress) is uncertain.

Notwithstanding the above, since the Social Order Maintenance Act (SOMA) also regulates gambling activities and there is no Public Requirement in the SOMA, users of online casinos and betting websites would be in violation of the SOMA.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

From the perspective of the players, those who 'gamble in a public place or a place open to the public' or 'gamble via telecommunication equipment, electronic communication, internet, or other similar means' would be committing a criminal offence (article 266 of the Criminal Code). From the angle of the provider, any person who intends to make a profit, furnishes a place to gamble or assembles persons to gamble will be committing a criminal offence (article 268 of the Criminal Code). Given so, we think that whether advertising or providing access to an online betting or gaming business located in another jurisdiction or in a metaverse would be considered a criminal offence should depend on whether any of such activities are carried out in Taiwan.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Unless otherwise restricted by sector-specific regulations (eg, outsourcing of financial institutions' operations), outsourcing of a company's services or functions is allowed and the rights and obligations of both parties will depend on the outsourcing agreement between the parties and whether the requirements under the Personal Data Protection Act (PDPA) are satisfied (such as with the consent of customers if their personal data will be used by the third-party outsourcing service provider).

With respect to a company's use of the services rendered by a third party, the PDPA will be applicable if such company using the third-party service provider's service will carry out the activities of collecting data from the data subjects, which would then be passed to a service provider for processing and use. Pursuant to the PDPA, such company may be held liable to its customers if the service provider does not comply with the PDPA.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

There may be sector-specific regulations that impose relevant restrictions and limitations on outsourcing activities. For example, according to the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation (the Banks' Outsourcing Regulations), a bank is required to comply with the Banks' Outsourcing Regulations in the case of any proposed outsourcing of its business operations. Under the Banks' Outsourcing Regulations, if a bank outsources certain business operations to service providers located overseas, the bank must submit relevant documents and obtain the Financial Supervisory Commission's prior approval.

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

There may be sector-specific regulations that impose relevant restrictions and limitations on outsourcing activities. For example, a bank is required to comply with the Banks' Outsourcing Regulations in case of any proposed outsourcing of its business operations, and the Banks' Outsourcing Regulations provide that certain items be specified in the outsourcing contract.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

Under Taiwanese law, there are no specific rights of employees in connection with the outsourcing of a company's services or functions. However, any contemplated dismissals or job transfers will be subject to Taiwan's labour laws, including the Labor Standards Act, the Act for Worker Protection of Mass Redundancy and the Personal Data Act (if the personal data of employees will be used by a third-party outsourcing service provider).

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

Under the current regulatory regime of Taiwan, there are no rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence (AI), machine learning, automated decision making or profiling, except that compliance with the Personal Data Protection Act (ie, obtaining informed consent) is required if collection, processing and use of personal data would be involved.

However, according to relevant newsletters, in order to enhance the supervision of AI-related technologies, the Financial Supervisory Commission (FSC) intends to upgrade the regulatory level of the rules governing robo-advisers from 'self-regulatory rules' (as announced by the Securities Investment Trust and Consulting Association (SITCA)) to the Securities Investment Trust and Consulting Act, which is expected to be finalised in the first half of 2024 and addresses the following two issues:

- adding the material principles of robot wealth management; and
- authorising the SITCA to establish a review team.

In addition, it is noteworthy that the Executive Yuan is currently drafting the Basic Act for Development of Artificial Intelligence to set out fundamental principles for AI development and for the government to promote the development of AI technologies, including regulations regarding IP rights, fake news and the ethics of artificial intelligence. The draft is scheduled for release in September 2023.

## IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

### AI and IP protection

Copyright is protected by the Taiwan Copyright Act, without registration or filing requirements. However, there are certain features that qualify a copyright, such as 'originality' and 'expression'. Therefore, whether AI is copyrightable depends on whether the subject AI has the required components (like the features described above) – especially the feature 'expression'. An algorithm itself is not generally recognised as a copyrightable work under the Copyright Act; however, this depends on whether the AI application has the required components.

As to patents, an inventor should file an application with the Taiwan Intellectual Property Office and obtain its approval to be granted the patent right in accordance with the Taiwan Patent Act. The subject of a patent right should be an 'invention', such as a 'creation of technical ideas, utilising the laws of nature'. As for a software-implemented invention, if it coordinates the software and hardware to process the information, and there is a technical effect in its operation, it might become patentable. Given the above, whether an algorithm or AI is patentable would depend on whether it has the required components.

### Intellectual property created by AI?

There have been no legislative amendments proposed by the competent authority in relation to AI-generated intellectual property. The issue of whether AI is able to create an 'original expression' under the copyright law or to be an 'inventor' under the patent law is still under observation. Such issues will be more important when AI has evolved to have the ability of independent 'thinking', and therefore can create an 'expression' and make an invention like a human. Such issues might not be solved under the current IP regime in Taiwan; it is a challenge faced by and needing to be addressed by the government, legislators, representatives of the court system and other legal practitioners, along with AI developments.

According to relevant newsletters, the Executive Yuan is currently drafting the Basic Act for Development of Artificial Intelligence to set out fundamental principles for AI development and for the government to promote the development of AI technologies, including regulations regarding IP rights, fake news and the ethics of artificial intelligence. The draft is scheduled for release in September 2023.

## Ethics

### 53 Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

The Ministry of Science and Technology under the Executive Yuan announced the AI Technology R&D Guidelines in September 2019 to demonstrate the government's commitment to improving Taiwan's AI R&D environment. Considering that AI developments may bring changes to various aspects of human existence, the Taiwan government expects participants to always be aware of such factors when conducting relevant activities and is endeavouring to build an AI-embedded society with three core values: 'human-centred values', 'sustainable developments' and 'diversity and inclusion'. Deriving from the three core values, eight guidelines were published under the AI Technology R&D Guidelines for the guidance of AI participants, so that a solid AI R&D environment and society that connects to the global AI trends may be established. The eight guidelines are:

- common good and wellbeing;
- fairness and non-discrimination;
- autonomy and control;
- safety;
- privacy and data governance;
- transparency and traceability;
- explainability; and
- accountability and communication.

Also, according to relevant newsletters, currently the Executive Yuan is drafting the Basic Act for Development of Artificial Intelligence to set out fundamental principles for AI developments and for the government to promote the development of AI technologies, and the draft is scheduled for release in September 2023. The following issues will be addressed in the draft:

- definition of AI terms;
- AI-related privacy protection;
- AI-related data governance;
- risk-based regulation of AI products or services;
- legalisation of AI ethical principles;
- government-based industrial development strategy; and
- compliance and legality of AI applications.

# TAXATION

## Online sales

### 54 Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Sale of online products would be subject to Taiwan taxation if the sale is carried out in Taiwan (eg, through a Taiwan website). As to sale of online products through an offshore website,

pursuant to Taiwan's Value-Added and Non-Value-Added Business Tax Act (VAT Act), foreign suppliers selling cross-border electronic services to domestic individual purchasers must make relevant registration with the tax authority and pay Taiwan VAT. In addition, the sales amounts collected by foreign profit-seeking enterprises selling cross-border electronic service would be deemed as income sourced from Taiwan and thus be subject to Taiwan income tax. The prevailing income tax rate is generally 20 per cent on the net taxable income.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Taiwanese tax laws do not specifically provide what tax liabilities would ensue from placing servers outside the jurisdiction of Taiwan or whether the placing of a server, platform or metaverse in Taiwan by a foreign company would expose that company to local taxes. However, Taiwanese tax laws target entities that have income sourced from Taiwan or sell cross-border electronic services to domestic individual purchasers.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The e-invoicing mechanism in Taiwan is not for any specific market segment. Generally, a business entity (ie, the provider of goods or services) may use 'electronic uniform invoices' to replace other, traditional, types of paper-based uniform invoice as long as it is registered with the local tax authority, subject to relevant requirements (a system with information security measures, connection with the Ministry of Finance, etc). However, under certain circumstances, the business entity may still need to provide hard copies of the evidence for the invoice, in case the buyer requires paper-based evidence due to its business needs.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

In Taiwan, there are no specialist courts or other venues established in accordance with applicable laws that specially deal with online or digital issues and disputes.

## ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

From a Taiwan legal perspective, the method of alternative dispute resolution should depend on the agreement of the contractual parties, unless otherwise expressly provided by law. In local practice, although arbitration is sometimes specified in the terms and conditions for digital business, it seems to be more common to agree upon the dispute resolution by local courts.

Pursuant to the Consumer Protection Act, when a consumer dispute arises, apart from bringing a lawsuit, the consumer may first file complaints to the business operator, consumer protection institutions, or consumer service centres. If the complaints are not properly handed, a request for mediation can be made with the consumer dispute mediation committee of local government.

# UPDATE AND TRENDS

## Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

On 30 June 2022, the National Communication Committee (NCC) issued the draft Digital Intermediary Service Act (DISA), which would govern digital intermediary (DI) service providers, onshore and offshore (if having a 'substantial connection' with Taiwan). The DISA provides for relevant general obligations for all DI service providers (eg, the obligation to disclose their basic information and contact information and to designate an agent in Taiwan (applicable to DI service providers without a commercial presence in Taiwan)), as well as obligations for providers of hosting services, online platform service providers and the online platform service providers designated by the NCC, etc. Nonetheless, the draft DISA is still under discussion, and whether it will be passed by the Legislative Yuan (the Congress) is uncertain.

Regarding data privacy, in recent years, legislators have repeatedly proposed to the Legislative Yuan the draft amendments to the Personal Data Protection Act to obtain the 'adequacy decision' from the EU authority concerning the GDPR. The proposed amendments include, but are not limited to, establishing a single government agency with responsibility for personal data protection matters, and adopting the same restrictions on international transfers of personal data as those applicable under the GDPR. Whether the draft amendments will be passed is uncertain.


Robin Chang robinchang@leeandli.com
Eddie Hsiung eddiehsiung@leeandli.com

8th Floor No 555 Sec 4, Zhongxiao East Road, Taipei 11072, Taiwan
Tel: +886 2 2763 8000
www.leeandli.com

**Read more from this firm on Lexology**

**Read this article on Lexology**

# Turkey

Sinem Mermer, İsra Tekin and Dila Küçükali

Boden Law

RETURN TO CONTENTS

## Summary

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

**1** How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

Due to its candidate status, Turkey has enacted regulations following the footsteps of the EU regarding many aspects of digital issues so far. For example, Turkish legislation reflects the main EU principles especially in consumer protection. Turkey also enacted a law on personal data protection, and the Human Rights Action Plan (Action Plan) published in April 2021 states that the personal data protection legislation will be aligned with the GDPR standards. The Action Plan also indicates that the government aims to adopt digital transformation in public administration, and the Digital Transformation Office within the Presidency has many ongoing projects in the fields of digital transformation, AI, big data and cybersecurity. Amendments to the Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications were introduced taking the example of Germany's Network Enforcement Act, or NetzDG. Regulation of crypto assets has been a priority for the government due to increased public attention to these assets during the pandemic, the high risks these transactions pose for most users, and fraud allegations in this area. Turkey has also adopted a preservationist approach towards cross-border data transfers and relevant legislation contains provisions encouraging or obligating companies operating in digital sectors to store domestic users' data in Turkey. E-commerce regulation was significantly revised in July 2022 to prevent unfair competition and monopolisation with an aim to promote the steady growth of the market. These revisions on e-commerce, which entered into force in 2023, foresee the requirement of obtaining a licence for certain e-commerce players, among other obligations which altogether will force market players to change or rebuild their business models.

### Legislation

**2** What legislation governs digital content and services, digital transformation and the conduct of business online?

The primary legislation applicable to online business is as follows:

- Law No. 6563 on the Regulation of Electronic Commerce (E-commerce Law);
- Law No. 6502 on Consumer Protection;
- Law No. 6698 on Personal Data Protection;
- Law No. 5651 on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications;
- Law No. 5809 on Electronic Communications;
- Law No. 6493 on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions; and
- Law No. 5070 on Electronic Signatures.

There is a variety of secondary legislation (regulations, communiques and guidelines) detailing the application of the primary regulations. Secondary regulations in this area are regularly amended in line with global and local economic trends. Other main legislation on

customs, IP, product liability, competition and tax, inter alia, is applicable in most cases to companies doing business online. Moreover, specific legislation may be applicable to companies operating in, for example, the banking, capital markets, energy and insurance sectors.

## Regulatory bodies

**3** Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The Ministry of Trade is authorised to take measures and carry out inspections with regard to e-commerce. For commercial advertisements in particular, the Advertising Board under the Ministry of Trade is authorised. The Personal Data Protection Authority is responsible for the regulation of matters related to personal data protection. The Turkish Competition Authority may conduct investigations into companies conducting business online. The Information and Communication Technologies Authority has the power to regulate the electronic communications sector. The Banking Regulation and Supervision Agency and the Central Bank are authorised to regulate fintech operations, crypto assets and digital coins.

## Jurisdiction

**4** What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

International Private and Procedure Law numbered 5718 (IPPL) regulates the jurisdiction of Turkish courts in disputes with foreign elements. Accordingly, the parties have the freedom to determine the jurisdiction for online transactions or disputes arising thereof. In the absence of such agreement, Turkish courts have jurisdiction when the defendant has an ordinary residence in Turkey, or the contract's characteristic obligation is performed in Turkey.

The IPPL sets forth mandatory rules on the jurisdiction of consumer contracts without making any distinction between contracts concluded online or offline. At the customer's choice, Turkish courts in places where the consumer's domicile or ordinary residence or the other party's domicile or ordinary residence is located are competent. On the other hand, Turkish courts at the consumer's residence have jurisdiction if any claims are brought against the consumer. Separately, in business-to-business online transactions, the parties are free to insert choice of forum clauses. That said, the validity of arbitral clauses that are concluded via clickwrap should be evaluated on a case-by-case analysis.

Even if the parties select a foreign law in their contract and refer their disputes to foreign courts, Turkish law may still find application as per IPPL. Directly applicable rules of Turkish law and violations of public policy are two concepts that have the power to limit the applicability of a foreign law. There is no single definition of directly applicable rules, they are shaped through the decisions of the Court of Appeals and academic opinions. On the other hand, Turkish law may become applicable if Turkish public policy is violated. A case-by-case

analysis should be made to determine whether the application of a foreign law can result in violation of public policy or Turkish directly applicable rules apply.

To the best of our knowledge, Turkish courts have not evaluated the choice of forum and governing law clauses applicable to transactions in the metaverse.

### Establishing a business

**5** What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

Generally, there are no distinctive regulatory and procedural requirements for the establishment of digital businesses; the Turkish Commercial Code relevant to brick-and-mortar businesses would apply. The E-Commerce Law requires service providers and intermediary service providers to register with the E-Commerce Information System (ETBIS) before initiating their operations.

In addition, the new provisions of the E-Commerce Law, which has undergone a comprehensive amendment, introduced new actors such as electronic commerce service providers and electronic commerce intermediary service providers. The amendments introduced a new licensing requirement, which also requires the payment of a licence fee calculated based on the transaction volume of a given year. The obligation to obtain a licence must be fulfilled as of 1 January 2025 and the licence fee will be calculated based on the transactional volume of the preceding year.

Depending on the sector that each digital business operates in, other specific legal requirements should be met. These range from data localisation requirements for specific permit applications and approvals from the relevant governmental authorities.

## CONTRACTING ON THE INTERNET

### Contract formation

**6** Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Electronically forming and concluding contracts is possible in Turkey and subject to the same requirements of concluding traditional contracts regulated under the Turkish Code of Obligations No. 6098. However, not all contracts are eligible to be concluded electronically, and there are certain form requirements stipulated in different sets of laws. For example, bank letters of guarantee, surety agreements, contracts regarding rights on real estate, inheritance law contracts, contracts that must be made officially before a notary public, and other legal transactions that are subject to an official form or special procedure by law cannot be concluded by using a secure electronic signature.

To conclude a contract via electronic means, there must be an offer and a corresponding acceptance. If the seller or provider has indicated all the objective essential elements of the contract online, there is a valid offer, and the contract is concluded by the consumer (usually) with a click on the acceptance button (click-wrap contracts).

Yet, there are other specific obligations for forming and concluding contracts electronically arising from regulations on electronic commerce, such as the Law on the Regulation of Electronic Commerce and the Consumer Protection Law. For example, service providers (ie, legal or natural persons engaged in electronic commercial activities), as well as intermediary service providers (ie, legal or natural persons providing an electronic commerce platform for third-party economic and commercial activities), are obliged to provide certain information to customers before concluding contracts electronically, as per the named regulations. Further, the Consumer Protection Law sets forth that electronic contracts concluded with consumers shall entail certain rights in favour of consumers such as the consumer's right of withdrawal from the contract within 14 days of the delivery of the goods or services. It should be emphasised that other liabilities may arise depending on the product or service presented online that would fall into the scope of other specific regulations such as financial services, timeshare vacation, long-term holiday products, package holidays, package tours, subscription contracts and consumer loans.

## Applicable laws

**7** Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Parties are free to choose the governing law applicable to digital contracts as per Law No. 5718 on International Private and Procedural Law (IPPL), in principle. However, IPPL stipulates certain limitations to the application of foreign law. For example, foreign law rules that are against public policy will not apply and the directly applicable rules of Turkish law may find application instead of the rules of the selected foreign law. Concerning consumer contracts, parties cannot exclude the minimum protection afforded to consumers in Turkey by selecting a foreign law.

Parties may refer their disputes to foreign courts if there is a foreign element in the legal relationship and the dispute arises from an obligation. Parties can refer their disputes to arbitration, however Turkish law has strict rules on special authority to conclude arbitration agreements and the arbitration clause must satisfy particular form requirements. That said, Turkish courts have the exclusive authority in disputes arising from consumer contracts, thus any disputes arising thereof cannot be brought before foreign courts or referred to arbitration. Regarding the language of the contract, Law No. 805 on the Compulsory Use of the Turkish Language dated 1926 applies to business-to-business contracts. This controversial law obliges all Turkish companies and enterprises to execute contracts that they conclude in Turkey with other Turkish parties in Turkish. The Court of Appeals has rendered varying decisions on the effects of non-compliance, ranging from invalidity of the contract to not taking specific provisions into account in a dispute. There is no specific requirement that consumer contracts have to be concluded in Turkish. That said, as the seller or provider

is required to inform the consumer as to many aspects of the contract, it is not certain whether the seller or provider can fulfil such duties in a language other than Turkish.

## Electronic signatures

**8** How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Article 3(b) of the Electronic Signatures Law No. 5070 defines an electronic signature as 'electronic data that is joined or linked logically to another electronic data and which is used to authenticate an identity'. If the e-signature (1) is exclusively linked to an individual, (2) is generated with a device at the disposal of the signer only, and (3) allows authentication based on a qualified electronic certificate and detection of data alteration, it qualifies as a secure electronic signature. The Electronic Signatures Law does not contain provisions on the signatures that do not meet the said requirements other than the definition of these as basic digital signatures. As per article 5 of the Electronic Signatures Law and article 15 of the Turkish Code of Obligations, only secure electronic signatures have the same legal effect as (ie, are equal to) handwritten signatures.

Electronic certificate service providers must notify the Information and Communication Technologies Authority (ICTA) prior to starting their operations. ICTA is authorised to enforce the Electronic Signatures Law, inspect electronic certificate service providers and regulate the application of the Electronic Signatures Law.

E-signatures are generally used in public transactions and commercial contracts. For instance, electronic signatures are used in inter-institutional communication, tax payments, passport applications, internet banking, e-contracts, registered electronic mail systems, commercial registry transactions, e-ordering applications and e-government practices.

## Breach

**9** Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

There is a wide range of remedies available for resolving consumer disputes, offering various options to address different types of issues. Within the scope of the Law on the Protection of Consumers, two of these remedies are specifically regulated as special conditions for litigation. As a matter of principle, these special litigation conditions are related to applications to consumer arbitration committees for consumer disputes below a certain amount, and to mediation for consumer disputes within the jurisdiction of consumer courts. For 2023, applications can be made to provincial or district consumer arbitration committees for consumer disputes with a value below 66,000 Turkish Lira. In disputes with a monetary value above this amount, it has become mandatory to refer the matter to mediation in the first instance. If this mediation process fails, a lawsuit may be filed before the consumer court. Consumers can apply to consumer arbitration committees through the e-government application and proceed with the dispute process online.

These provisions are in compliance with Directive 2013/11/EU of the European Parliament and the Council, which addresses the use of alternative dispute resolution in consumer disputes. This alignment ensures that the chosen dispute resolution mechanisms adhere to the standards set by the European Union for consumer protection and dispute resolution.

Additionally, in business-to-business contracts, the remedies specified in the Turkish Code of Obligations (specific performance, damages and termination) will be available. In business-to-consumer contracts, consumers have the right of withdrawal without giving any grounds or paying any fines, if such right is exercised within 14 days of the conclusion of the contract or delivery of the goods. If the seller fails to fulfil its obligation to provide information to consumers, the right of withdrawal can be extended to one year. Consumers also have the right to terminate the contract if the seller fails to deliver the goods within 30 days following receipt of the order by the supplier or provider, except for products that are prepared as requested or specifically needed by the consumer; however, this period shall not apply to contracts for goods prepared in line with the consumer's wishes or personal needs.

Finally, the amendment to the Regulation on Distance Contracts stipulates that the consumer cannot exercise the right of withdrawal in certain contracts, unless otherwise agreed by the parties, such as contracts for services performed instantly in electronic media or contracts for intangible goods delivered to the consumer instantly.

## FINANCIAL SERVICES

### Regulation

**10** Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

Banks' digital sales of financial services products is regulated by the Regulation on Methods Utilised by Banks for Distant Identity Verification and Concluding Contracts via Electronic Mediums, and the Regulation on Banks' Information Systems and Electronic Banking Services. To form a binding contract, banks shall send all terms and conditions of the contract to customers via mediums listed in the relevant regulation and the customer, in return, shall send its declaration of intent securely. Only thereafter will contracts concluded via electronic mediums be deemed to fulfil the written form requirement. Significantly, not all financial services products are eligible to be sold online, as sales of some services and products are subject to particular form requirements. The Regulation on the Operational Principles of Digital Banks and Service Model Banking regulates the principles and procedures regarding the activities of branchless banks that operate only through electronic banking services distribution channels and the provision of banking services to fintech companies and other businesses as a service model. All banking regulations referenced here are executed by the chairperson of the Banking Regulation and Supervision Agency (BDDK). The BDDK has also recently been given the authority to regulate the procedures and principles related to artificial intelligence-based verification processes.

Suppliers of financial services products shall comply with more specific obligations outlined in the Regulation on the Distance Contracts of Financial Services (the Regulation) if the counterparty is a consumer. Suppliers are required to provide certain information

to consumers prior to the conclusion of the distance contract in the form explained in the Regulation. The supplier shall communicate this information and any additional information after the conclusion of the distance contract to the consumer on paper or a durable data medium. The Regulation further elaborates on consumers' right of withdrawal, suppliers' and consumers' obligations, the legal effect of the right of withdrawal on ancillary contracts, exceptions to the right of withdrawal, the termination method of the distance contract, burden of proof, data retention obligation of the suppliers and rules on distance communication costs for consumers. Further, the Regulation on Commercial Advertisements and Unfair Commercial Activities contains provisions on the advertisement of financial products targeting consumers, and the Ministry of Trade is authorised to execute the provisions of these regulations.

## Electronic money and digital assets

### 11 Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Electronic money (e-money) is defined as the monetary value that is stored electronically and issued in exchange for funds by the issuing institution which is accepted as a payment instrument by third parties and used to make particular payments defined in the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions. According to this definition, only intangible assets that are created virtually, distributed over digital networks and issued in exchange for one-to-one fiat money can be considered e-money. Only banks, the Postal and Telegraph Corporation and authorised e-money institutions can issue e-money. E-money institutions are subject to licence and capital requirements (the minimum capital requirement was raised to 41 million Turkish lira in 2023). E-money institutions must transfer funds collected in exchange for e-money issuance to a separate bank account. These institutions are not authorised to provide loans and they cannot make interest payments or provide any other benefits to e-money holders.

Crypto assets have been regulated since April 2021. The Regulation on Prohibiting the Use of Crypto Assets in Payments (the Regulation) defines crypto assets not as mediums of exchange but as intangible assets that are formed virtually using distributed ledger technology, or similar technology, and distributed over digital networks. It is explicitly stated in the Regulation that crypto assets do not qualify as fiat currency, fiduciary money, electronic money, payment instruments, securities or other capital market instruments. As per the Regulation, the direct or indirect use of crypto assets in payments or provision of payment services and electronic currency exports is prohibited as of 30 April 2021. Payment service providers are banned from developing any business model that falls within the prohibition's scope and from providing services according to such business models. Further, payment and electronic money institutions are prohibited from acting as an intermediary for transferring funds to and from platforms that buy or sell, deposit, transfer or export crypto assets. All in all, the prohibitions introduced by the Central Bank can be categorised as a ban on payments via crypto assets, rather than an overall ban on investing in crypto assets. Additionally, the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism was amended on 1 May 2021 to hold crypto asset service providers liable for obligations as per the anti-money laundering regulations. Crypto asset service providers must comply with the measures introduced by the Financial Crimes Investigation Board (MASAK), such as customer identification (KYC) obligations and

transaction limits, among others. MASAK may impose administrative fines for violations of KYC obligations, obligation to provide continuous information and notification of suspicious transactions.

## Digital and crypto wallets

**12** Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Crypto wallets have not yet been regulated under Turkish law. A draft regulation on crypto assets and crypto wallets is on the horizon, but, as at the time of writing, no draft regulation has yet been made available for public consultation.

## Electronic payment systems

**13** How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions (Payment Services Law) is the framework legislation on the use of electronic payment systems and payment service providers. The Payment Services Law was amended in line with the EU Payment Services Directive 2 in 2020. As per the Payment Services Law, only banks, electronic money institutions, payment institutions and the Postal and Telegraph Corporation qualify as payment service providers. The Central Bank is authorised to regulate and audit payment service providers. Payment institutions must meet capital requirements stated in the Payment Services Law (except for account information service providers) and obtain an operating licence from the Central Bank. Payment service providers are prohibited from developing business models that use crypto assets directly or indirectly for the provision of payment services and electronic money issuance, and from providing any services related to such business models as per the Regulation on Prohibiting the Use of Crypto Assets in Payments (the Regulation).

The secondary legislation on the application of the Payment Services Law was revised in December 2021. As per the Regulation, banks may deny access to the payment account by payment initiation service providers (PISPs) and account information service providers (AISPs) based on an objective and demonstrable ground (eg, cases where there is fraudulent or unauthorised access). Access should be granted again when the reason to deny access ceases, and the bank should notify their customers and the Central Bank of the reasons for access denial. If the customer duly authorises the PISP or the AISP, banks should ensure secure communication and make all the necessary customer data available for the provision of payment services as soon as possible and in a non-discriminatory manner. PISPs cannot store and AISPs cannot obtain sensitive customer data. Both PISPs and AISPs must follow purpose limitation and data minimisation principles and process data in accordance with the information security and privacy regulations, including personal data protection rules. The Communiqué on the Information Systems of Payment and Electronic Money Institutions and Data Sharing Services of Payment Service Providers in Payment Services contains more detailed and technical rules on data sharing between banks and payment service providers.

### Online identity

**14** Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

The Regulation on the Measures Regarding Prevention of Laundering Crime Revenues and Terrorism Financing states that financial institutions may rely on third parties to satisfy KYC requirements; however, reliance on third parties does not release the financial institution from its obligations. Reliance on third parties is possible when the financial institution ensures that the third party; (1) has implemented measures to comply with the KYC rules, and (2) can provide certified copies of identification immediately when requested. Reliance on third parties is nevertheless not possible if the third party is based in either a risky country or a country where it is not subject to any regulations on AML as per international standards. Nevertheless, as per the amendments to the Regulation on Remote Identification Methods to be used by Banks and the Establishment of Contractual Relationships in Electronic Media dated July 2023, not all persons are competent for distant identity verification. Accordingly, only real persons, real person merchants and real person representatives of legal entities are listed as persons who can use distant identity verification.

In late 2022, the Financial Crimes Investigation Board published Counter-Terrorism Financing Guidelines for Certain Non-Financial Businesses and Professions and Counter-Terrorism Financing Guidelines for Financial Institutions. These guidelines were issued in parallel with the European Union's Global Facility on Anti-Money Laundering and Terrorist Financing.

## DOMAIN NAMES AND URLS

### Registration procedures

**15** What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

For an extended period of time, 'Nic.tr Administration' within Middle East Technical University had been responsible for registering the country code top-level domain '.tr'. Later, the Regulation on Internet Domain Names (the Regulation) opened the market to different registrars, prescribed the establishment of a central '.tr network information system' (TRABIS), and authorised the Information and Communication Technologies Authority (ICTA) to enact regulations in this field. TRABIS started accepting new applications and renewal requests as of 14 September 2022. According to TRABIS system operation, all domain name owners must select a new registration organisation operating under TRABIS and transfer their domain names. New domain name applicants will submit their requests to one of the registration organisations, and the organisation will process their request on TRABIS.

The Regulation adopts two methods for domain name allocations. The 'first come, first serve' rule applies to undocumented domain name applications. '.com.tr', '.net.tr' and '.org.tr' are open to undocumented applications. A connection between the applicant and the domain name is not required in undocumented applications; therefore, natural persons and legal entities located abroad can submit undocumented domain name applications. On the other hand, certain domain name applications require documentation and approval by the authorities. For instance, the allocation of the domain name '.av.tr' has been limited to the use of attorneys registered with the Turkish Bar Union, law offices, and lawyer partnerships. The ICTA has been authorised to decide on the cancellation of domain names in the event of certain limited circumstances.

## IP ownership

**16** Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

Domain names can be registered as trademarks and benefit from the protection afforded by the Industrial Property Law. If the trademark owner does not exploit the priority granted by the Communiqué on Domain Names (the Communiqué) with first-time domain name allocations, the registrars are not obliged to cross-check whether the domain name infringes a registered trademark. Yet, the ownership of a trademark would assist in challenging a domain name. The complainants may allege that (1) the disputed domain name is identical or similar to their trademark, business title or other; (2) the party who registered the domain name has no legal connections with the domain name; or (3) the domain name has been registered or used in bad faith. Particular use of domain names is assumed to be bad faith – for instance, when the domain name owner registered the trademark in order to prevent the trademark owner's registration or when the domain name is registered to harm competitors' operations or activities. Such complaints related to domain names will be resolved by arbitrators or an arbitral tribunal of three arbitrators appointed among the Dispute Resolution Service Providers (DRSP) as per the Communiqué and the Communiqué on the Domain Names Dispute Resolution Mechanism (Dispute Resolution Communiqué). In order to establish a registry mechanism to ease many domain name-related matters, the ICTA has established TRABIS, as regulated in the Communiqué, and the registry system became operational on 14 September 2022. TRABIS brought several changes to the rules and procedures regarding the allocation, transfer and renewal of '.tr' domain names, including the ability to make the required payment within two months in order to reactivate an expired domain name. As a result, any complaints made to the registrar in line with the Communiqué will be immediately notified to TRABIS for the DRSP to resolve in light of information based on the parties' TRABIS registration.

## ADVERTISING

### Regulation

**17** | What rules govern online advertising?

The Consumer Protection Law governs commercial advertising that is aimed at consumers in Turkey. The definition of commercial advertising is defined broadly in the law and includes online advertising. The competent authority is the Board of Advertisement, which has the authority to investigate and monitor all advertising activities and to impose administrative fines. All advertisements shall be true and fair, and shall not violate public order, public morality, personal rights, and principles issued by the Board of Advertisement. Any unfair commercial activity (eg, misleading or aggressive activities) is also prohibited and the Board of Advertisement may issue administrative fines in violation thereof. The Regulation on Commercial Advertisements and Unfair Commercial Activities provides more details on the rules established by the Consumer Protection Law. This regulation was amended in 2022 and the amendments include, among others, personalised price definition, procedures regarding online reviews by customers and online ranking of products. Further, the Law on the Establishment and Principles of Radio and Television Broadcasting applies to on-de-mand broadcasters. Any advertisement via such broadcasts would be subject to this Law.

Relying on the Consumer Protection Law and the Regulation on Commercial Advertisements and Unfair Commercial Activities, the Ministry of Trade published the 'Guideline on Commercial Advertisements and Unfair Commercial Activities by Social Media Influencers' in May 2021. This guideline introduced new restrictions on online advertisements by social media influencers. Additionally, the Guideline on Advertisement and Commercial Practices with Price Information and Discounted Sales was published in April 2022. This guideline includes rules on ads with price and discount information and should be taken into account by sellers, providers and intermediary service providers in e-commerce.

The advertisement of specific products and services is also regulated. For example, advertising financial services is subject to the specific rules outlined in the Regulation on Commercial Advertisements and Unfair Commercial Activities.

The Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications (the Internet Law) introduced an online advertising ban on social network providers without making any distinction as to the advertised product or services. Accordingly, the Information and Communication Technologies Authority may impose an advertising ban on a social network provider that has more than 1 million daily users from Turkey if said provider does not designate a representative in Turkey. With the amendment in 2023, the real person representative of a social network provider, which is required to have a representative in Turkey, must be a Turkish citizen and resident in Turkey.

## Targeted advertising and online behavioural advertising

**18** What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Two separate laws contain relevant provisions on targeted advertising via cookies: (1) the Electronic Communications Law, which is heavily influenced by EU Directive 2002/58/EC, and (2) the Personal Data Protection Law (PDPL). Cookies would qualify as personal data if they can identify individuals when combined with other information.

Parallel to Directive 2002/58/EC, article 51(3) of the Electronic Communications Law requires that users are informed clearly and comprehensively regarding data processing activities and that they have provided their explicit consent when electronic communications networks store information or gain access to information stored in users' terminal equipment other than to provide services. This provision covers only authorised operators, those who provide electronic communications services or electronic communication networks and operate the infrastructure. Operators can rely on explicit consent as it is a statutory requirement.

That said, any other party that falls outside the Electronic Communications Law's scope shall conduct their processing activities via cookies as per the PDPL. In 2020, the Board of Advertisement (the Board) issued a decision concerning the use of cookies by an e-commerce website (Decision No. 2020/173). The Board assessed the cookies notice found on the website, which was of a general nature, and noted that the cookies notice was not made available to first-time visitors. The Board added that the data controller failed to inform data subjects about processing methods (such as cookies) and did not request the explicit consent of visitors.

Data controllers may rely on two separate exceptions to explicit consent: performance of the contract, or their legitimate interests when they process cookies that are strictly necessary. In any case, data controllers must rely on explicit consent when they aim to use cookies for marketing or profiling activities. This is confirmed by the Turkish Personal Data Protection Authority in its Guidelines on Cookie Applications. Controllers are advised to avoid opt-out mechanisms in this regard and provide a separate link or explanation regarding cookie processing activities in their consent management tool.

## Misleading advertising

**19** Are there rules against misleading online advertising?

Misleading advertising is regulated in the Consumer Protection Law and the Regulation on Commercial Advertising and Unfair Commercial Activities. Accordingly, advertisers are obliged to prove that their advertised claims are true. Advertisers shall substantiate their claims with scientific documents and information. If need be, the Board of Advertisement may also request the advertiser to submit information or documents obtained from the universities or accredited research or test facilities. Surreptitious advertising is not allowed under any circumstances; the advertiser must be identifiable by the target audience. There are also specific rules on practices that fall under the scope of commercial advertisement, such as customer reviews and price comparisons in online sales. These rules may be

subject to different sector-specific standards, but all are centrally supervised by the Board of Advertising.

## Restrictions

### 20 | Are there any digital products or services that may not be advertised online?

Currently, there are several products and services that cannot be advertised as per various regulations. According to the Pharmaceuticals and Medical Preparations Law, any advertisement of medicines and human medicinal products is prohibited. In addition, any advertisement of alcoholic beverages and tobacco is prohibited by the Spirits and Alcoholic Beverages Law and the Prevention and Control of Damages Arising from Tobacco Products Law. Health and legal services, betting, gambling and accountancy services can be given as examples of other sectors and services that cannot be advertised. Although the above-mentioned regulations do not mention online advertising specifically, they apply due to the broad definition of advertisement found therein. Furthermore, as per the Regulation of Betting and Games of Chance in Football and Other Sports Competitions, any advertisement of online betting will be subject to criminal charges and administrative fines. In addition, all access will be restricted to these websites in line with the Law on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts.

## Direct email marketing

### 21 | What regulations and guidance apply to email, SMS and other direct marketing?

Any message (in the form of data, sound or image) transmitted electronically (by any kind of messaging system) for commercial purposes qualifies as a 'commercial electronic message' under the Law on the Regulation of Electronic Commerce (the E-Commerce Law), which is the main regulation on commercial communication in e-commerce. Commercial electronic messages are further regulated in the Regulation on Commercial Communication and Commercial Electronic Messages, which outlines how obligations under the E-Commerce Law must be fulfilled. Other than the regulations on e-commerce, the Electronic Communications Law regulates commercial electronic messages sent to subscribers and customers by operators.

First, all natural and legal persons who wish to send commercial electronic messages must register themselves on the Message Management System (abbreviated in Turkish as IYS). IYS is a national database in which all service providers must register the consents given by persons for receiving commercial electronic messages. Commercial electronic messages shall only be sent after obtaining prior consent from recipients (ie, opt-in mechanism). Individuals can monitor all consents given by them and may revoke any consent given in the past via the IYS platform. If the service provider obtains consent in writing or electronically, it must register this with IYS within three business days, otherwise the consent becomes invalid. In addition, if consent is obtained using a method other than the IYS platform (eg, in writing or electronically by service providers), the burden of proof on the existence of consent is on the service provider. As per the relevant legislation, the authorities may issue administrative fines to service providers and intermediary service providers for sending commercial electronic messages in violation of the above-mentioned and other mandatory rules. All in

all, (potential) customers have more control over what kind of marketing messages they would like to receive with the introduction of the IYS platform.

Operators need to obtain prior consent for marketing purposes as well (opt in). Exceptionally, operators do not need to obtain consent when contact details are given in the context of the sale of a product or service, provided that subscribers and users are informed about communication and given the opportunity to object. However, operators' use of contact details is restricted.

The powers of the Ministry of Trade have been expanded with the new E-Commerce Law, by way of which the Ministry of Trade will be able to obtain the subscriber information of real or legal persons who send commercial electronic messages via voice calls and text messages from the ICTA.

## ONLINE PUBLISHING

### Hosting liability

**22** What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Content providers are primarily liable for the content they publish online. Hosting providers and access providers are not obliged to monitor the content they store or transmit. That said, hosting and access providers shall, in any case, comply with judicial or administrative decisions regarding removal of, or blocking access to, the content.

Intermediary service providers are not liable for the content, products or services that are offered by the service providers, as confirmed by the Court of Appeals. However, Law No. 6563 on the Regulation of Electronic Commerce was significantly revised in July 2022. Similar to the EU Digital Services Act, the new rules, which mostly entered into force in 2023, bring an addition to the exemption and state that electronic commerce intermediary service providers are required to remove illegal content offered by electronic commerce service providers without any delay after they become aware of the situation, and notify the relevant public institution accordingly. Further, if an IP holder files a complaint together with the necessary documents about a product regarding an IP violation, the electronic commerce intermediary service provider shall remove the product offered by the electronic commerce service provider and notify the IP holder and service provider.

### Content liability

**23** When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

As per the law, content providers are liable for the content they publish online, and hosting providers do not have a general obligation to monitor the content delivered by the content provider. However, hosting providers must comply with judicial or administrative decisions

on the removal of, or blocking access to, unlawful content; otherwise, they will be subject to administrative or judicial fines. Furthermore, civil liability may arise as per the general terms applicable to torts. For a tort liability to arise, mistakes in information published online must cause damages to a third party and the hosting provider must be at fault. The burden of proof would lie with the website user. Hosting providers cannot exclude themselves from the above-mentioned liabilities via posting notices or general terms and conditions.

The scope of liability is broader for social network providers. If the content is found unlawful by a court order and the social network provider fails to remove the unlawful content within 24 hours, the social network provider would be liable for all damages. It is not required that the damaged party first seeks damages from, or initiates a lawsuit against, the content provider.

Finally, the spread of online disinformation is newly regulated in Turkey; the Law on the Amendment of the Press Law and Certain Matters added a new offence to the Turkish Penal Code under the heading of 'Crimes Against Public Peace'. This crime is defined as 'publicly disseminating misleading information'. Those who commit this offence will be sentenced to imprisonment of between one and three years; aggravating circumstances have also been regulated.

### Shutdown and takedown

**24** Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

The Information and Communication Technologies Authority (ICTA) issued administrative fines to an ISP in 2012 for blocking access to various websites without any judicial or administrative measures taken by the courts or the ICTA itself. The ICTA's decision regarding the ISP's blocking access to certain websites was evaluated within the scope of regulation on online content and the ISP's failure to take all necessary measures to keep all systems running.

## INTELLECTUAL PROPERTY

### Data and databases

**25** Are data and databases protected by IP rights?

Turkish law affords legal protection to original and non-original (sui generis) databases. Copyright protection is granted to original databases if the data and materials therein are selected and compiled for a specific purpose and plan, and thus constitute the author's own intellectual creation. However, the protection applies to the database itself, not to the materials or data constituting the database. On the other hand, non-original (sui generis) databases have special protection if the creator of a database has substantially invested in the construction, verification or representation of the database. The creator of the database can cease the transfer, distribution, sale, rental or communication to the public of a non-original database by a third party if the violation concerns all or a significant part of the database. Yet, it is possible for third parties to create a similar sui generis database if

they put their own effort and investment into their database. Additionally, the IP protection granted to databases is not absolute. For instance, a dominant database owner may be forced to grant a licence or access to third parties if enforcing IP rights is found to be an abuse of dominance practice.

## Third-party links and content

### 26 Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

A website owner can surface a link (ie, direct internet users to third-party websites' home-pages) without permission even when the content is under IP protection. When an owner presents the work to the public online without any further technological restrictions or in other words, when it is freely available on the internet, it is assumed that the owner has given implicit consent regarding internet users' access to the work.

A deep link allows internet users to reach a particular web content instead of the home-page. Internet users do not see the advertisements on the homepage; as a result, the linked website's advertisement revenues may decrease. Deep linking may also cause unfair competition.

The mere act of linking does not violate the owner's IP rights arising from the Law on Intellectual and Artistic Works (the Law). To speak of an infringement, linking itself should also violate the owner's rights to distribute, adapt, or any other right. In addition, linking does not constitute an act to publicise in principle since the content is already made freely accessible to users by the owner.

### 27 Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Framing allows the display of several documents on a web page without the linked websites' URL addresses. Therefore, internet users may not realise they have accessed a different web page. In contrast, inline linking allows the display of another web page's content automatically without leaving the website that has embedded the link. The inline linker does not place a copy of the content on its internet server. The internet users do not see the linked website's URL and therefore may be under the impression that the linked content belongs to the website that has integrated the inline link. Since framing and inline linking may mislead internet users about the work's owner, the owner's right to be recognised as the owner of the work may be violated as per article 15 of the Law.

Websites cached by online search engines may sometimes contain photos or texts that are protected by the Law. Such caching would be deemed as having the owners' implicit consent provided that the owner has not objected to the use of their work to search engine operator, the use of the work is in line with the owners' interests, the work is used to the extent that is required.

Keyword advertising and the use of metatags are considered within the framework of the Industrial Property Law. Accordingly, the owner may allege infringement of its trademark

due to the use of keywords provided that (1) an identical or similar sign is used online by others, (2) this use has a commercial effect, and (3) the perpetrator has no right or legitimate connection to such use. Decisions of the Court of Appeal on keyword advertising establish that using a sign as a keyword that has a commercial effect and thus causing confusion is a trademark violation and constitutes unfair competition.

## Metaverse and online platforms

**28** Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Turkish law does not foresee particular rules on establishing or defending copyright, database rights or trademarks on a metaverse. That said, parallel to global trends, whether the existing rules on establishing and defending IP rights would provide sufficient protection on a metaverse, or whether novice rules regarding IP rights on a metaverse are necessary, is a topic under discussion among academics and practitioners.

## Exhaustion of rights and first-sale doctrine

**29** Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Both the Law on Intellectual and Artistic Works and the Industrial Property Act recognise the concept of exhaustion of rights or the first-sale doctrine. If the author of a work has duly exercised their right of distribution by transferring ownership of the original or copies of a work in Turkey, or the rights holder has put the good that is protected by an industrial property right on the market or authorised such an action, they cannot prohibit or prevent the resale of the work or product. It is not clear whether the first-sale doctrine applies to digital products that are obtained or placed online.

## Administrative enforcement

**30** Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

While there are civil remedies available for all IP rights, criminal remedies are granted only to registered trademarks and copyrights. However, submission of a complaint by the IP owner is required for criminal remedies to be carried out. If the IP owner follows one of these procedures, the competent court may order a search warrant to seize evidence or an interim measure to cease the infringement.

### Civil remedies

**31** What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

An IP owner whose IP rights are infringed can request the competent court (civil courts or specialised IP courts where applicable) to:

- determine whether the act constitutes an infringement;
- prevent an imminent infringement or to cease an existing infringement;
- order compensation for damages;
- confiscate infringing products, manufacturing equipment and machinery;
- transfer infringing products' ownership to the IP owner claimant;
- implement measures against recurring infringements, including the destruction of infringing products; and
- publish the judgment.

IP owners might also apply for an interim measure for the cessation or prevention of the infringement, including the seizure of the infringing products.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

**32** How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

The Personal Data Protection Law (PDPL) defines personal data as any information relating to an identified or identifiable natural person. Legal persons are excluded from the definition of personal data and the scope of the PDPL.

The PDPL defines personal data revealing racial, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing and attire, association, foundation or trade union membership, health, sex life, criminal conviction and security measures, biometric or genetic information, as special categories of personal data. In line with the GDPR, special categories of personal data can also be defined as 'sensitive personal data'. As a rule, sensitive personal data can only be processed with the data subject's explicit consent. Exceptionally, sensitive personal data can be processed without explicit consent when authorised by law. However, personal data concerning health and sexual life may only be processed, without seeking explicit consent of the data subject, by persons subject to a secrecy obligation or competent public institutions and organisations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of healthcare services as well as their financing. In its Decision No. 2018/10, the Board within the Personal Data Protection Authority (the Board) listed the adequate measures to be taken by data controllers to process sensitive personal data, which are to be followed by controllers as per article 6(4) of the PDPL. Encryption of servers and logging for any access to sensitive personal data can

be given as examples to adequate measures. The Board also published guidelines on the processing of biometric data in 2021, which foresee detailed administrative and technical measures to be taken by data controllers.

Anonymisation is defined as 'rendering personal data impossible to link with an identified or identifiable natural person in any way including matching with other data'. Although processing anonymised data would fall outside the scope of the PDPL, processors shall comply with the Regulation on Erasure, Destruction or Anonymisation of Personal Data, which stipulates the methods of anonymisation of personal data.

## Registration and appointment of data protection officer

**33** Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Natural persons or legal entities that process personal data wholly or partly by automated means or conduct processing by unautomated means that form part of a data filing system fall into the material scope of the PDPL. Prior to data processing, natural persons or legal entities that process personal data shall register with the Data Controllers' Registry.

The Board may exempt certain controllers from the obligation to register. For instance, the Board exempted notaries, political parties and lawyers from the obligation with Decision No. 2018/32 and all controllers – either natural or legal persons – whose main field of activity is not processing sensitive personal data are exempt from the registration obligation as per Decision No. 2018/87, provided that they have less than 50 employees and their annual financial statement amounts to less than 25 million Turkish lira. The Regulation on Data Controllers' Registry requires data controllers located outside Turkey to authorise a legal entity located in Turkey or a Turkish individual for representation and registration.

As per the Communiqué on Procedures and Principles Regarding the Personnel Certification Mechanism (Communiqué), the procedures and principles pertaining to the certification of individuals within the scope of the Data Protection Officer Programme (Programme) have been determined in accordance with the EN ISO/IEC 17024 standard. Individuals will be eligible to be titled 'data protection officer', provided they have obtained the certificate of participation within the Programme and have been successful in the exam prepared by the Turkish Accreditation Agency. The employment of a data protection officer by a data controller or data processor (or both) shall not suppress the responsibility of a data controller or data processor (or both) to comply with the PDPL and the relevant legislation.

## Extraterritorial issues

**34** Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The PDPL does not have any specific provisions on its territorial application. While establishing the rules on data breach notifications, the Board stated that data controllers located abroad must notify the Board of data breaches provided that the results of such breaches

affect persons located in Turkey and the affected persons benefit from the services and products within Turkey. Accordingly, in recent years, the Board issued administrative fines to companies located abroad due to data breaches that affected persons residing in Turkey. Therefore, the lack of a specific provision on the territorial application does not exclude the application of the PDPL to persons or organisations located outside Turkey.

Foreign nationals can enforce rights granted to data subjects in the PDPL. However, the application should be made in Turkish as per the Communique on Principles and Procedures for Application to Data Controller.

The PDPL does not require organisations or individuals residing or established abroad to appoint a representative. However, the Regulation on Data Controllers' Registry requires data controllers located outside Turkey to authorise a legal entity incorporated in Turkey or a Turkish individual (data controller representative) for registration and communication purposes.

## Bases for processing

**35** What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

Contract performances and legitimate interests pursued by the controller are the two most commonly asserted reasons for processing personal data. The Personal Data Protection Authority (DPA) stipulates that if there is a legal basis available other than consent, controllers should rely on that reason and obtain consent from data subjects only when there is no other processing ground applicable. The DPA finds relying on consent when other processing grounds are available as an abuse of rights. However, on some occasions, controllers may have to rely on consent for practical reasons. For instance, sensitive personal data processing grounds available in the PDPL other than consent are quite limited. When employers are to process health data of their employees, consent appears to be the only available mechanism even though the validity of consent in an employment context can be challenged. For cross-border data transfers, controllers tend to rely on consent until they obtain approval from the DPA. Nevertheless, a case-by-case analysis shall be conducted to determine which processing ground can be relied upon.

## Data export and data sovereignty

**36** Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Personal data may only be transferred outside Turkey with the data subject's explicit consent, or if another lawful processing ground exists. The recipient country must have adequate protection, or the parties requesting to transfer personal data abroad must obtain approval from the DPA. The DPA will evaluate whether the laws regarding data transfer between the subject country and Turkey are reciprocal. The DPA has not yet issued an adequacy decision, although it was announced in 2020 that the DPA has been in collaboration with several ministries to work on a list of countries with adequate protection. Due to

the lack of adequacy decisions, data controllers must obtain approval from the DPA by filing a commitment letter or by undertaking binding corporate rules in case of cross-border data transfers. In 2021 and 2022, the DPA approved several applications for cross-border data transfers. However, Turkey's approach to data export continues to be rather conservative; in 2022 the Personal Data Protection Board issued administrative fines to a global hotel chain for transferring personal data abroad without obtaining approval.

There are several rules that require data servers to remain in Turkey, and these rules vary depending on the sector. For instance, banks, payment and e-money institutions, financial leasing and factoring companies located in Turkey are required to keep their first and second information systems and duplicate data centres in Turkey. Social network providers with more than 1 million daily users from Turkey are required to implement measures to keep these users' data in Turkey.

## Sale of data to third parties

### 37 May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

Personal data might be sold to third parties within Turkey as per article 8 of the PDPL on the transfer of personal data. In this regard, data controllers may rely on the explicit consent of the data subject or other processing grounds listed in the PDPL. In either case, the general principles on personal data processing must be observed. As processing shall be undertaken for specified, explicit, and legitimate purposes, data subjects must be informed regarding the transfer and recipients. If the buyer of personal data wishes to use personal data for marketing purposes, the seller must obtain explicit consent from data subjects. Data subjects have the right to know the third parties to whom their personal data is transferred.

Personal data that has been made public by the data subjects themselves can be sold by a website owner provided that the transfer is consistent with the data subject's purpose for making their data public. On the other hand, sensitive personal data may be sold to third parties only with the data subject's explicit consent. In the case of a personal data transfer, the seller and the buyer are liable as data controllers exclusively for violations of the PDPL.

## Consumer redress

### 38 What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

As per article 11 of the PDPL, data subjects have the right to:

- learn whether their personal data is being processed or not;
- demand information as to whether their personal data has been processed;
- learn the purpose for the processing of their personal data and whether this personal data has been or is being used in compliance with the purpose;
- know the third parties to whom their personal data has been or is being transferred in the country or abroad;

- request the rectification of incomplete or inaccurate data;
- request the erasure or destruction of their personal data under the conditions referred to in article 7;
- request reporting of the transfer operations to third parties to whom their personal data has been transferred;
- object to a detrimental decision which is based solely on automated processing; and
- claim compensation for damages arising from the unlawful processing of their personal data.

These rights would extend to foreign individuals residing in Turkey; however, the application to the data controller can only be made in Turkish.

### Non-personal data

**39** Does the law in your jurisdiction regulate the use of non-personal data?

There is no regulation directly addressing non-personal data or the use of non-personal data in Turkey. Nonetheless, there are a few regulations that include provisions indirectly regarding non-personal data. As per the Law on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications, all Turkish and foreign social network providers with more than one million users accessing the network from Turkey must take precautions regarding the maintenance of the anonymised data of their users in Turkey. In addition, the E-Scooter Regulation reads that the database kept by e-scooter companies related to their operations must be kept within the borders of Turkey.

## DOCUMENT DIGITISATION AND RETENTION

### Digitisation

**40** Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Digital transformation has impacted document management systems both in the public and private sectors. For instance, the Regulation on the Principles and Procedures of Official Correspondence states that public institutions must handle official correspondence electronically and not keep physical documents with secure e-signature (except for confidential documents). If documents that are required to be stored in a physical form as per civil procedure, notary and enforcement rules are signed with secure e-signatures, physical copies are obtained only when necessary or upon request. Although the Notary Law has been revised in light of electronic transactions allowing certain documents to be stored electronically, most documents are still kept in physical form.

From a commercial law perspective, the Turkish Commercial Code and Tax Procedure Law allow merchants to send notices via registered electronic mail and keep their commercial books electronically. Additionally, the Ministry of Trade is authorised to oblige companies to keep their share ledgers, board resolutions and minutes of shareholder meetings electronically. Yet, technical infrastructure to keep commercial books electronically is under

development, and only particular commercial books (such as general ledgers) can be processed online. Therefore, only a small percentage of companies utilise e-book services, and share ledgers, board resolutions and minutes of shareholder meetings are usually kept physically, in practice.

### Retention

**41** Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

As per the Turkish Commercial Code, merchants should store their commercial books and the underlying documents, financial sheets and commercial letters for a period of 10 years. Tax Procedure Law requires the books to be kept for five years. Notary offices are obliged to keep their records for between five and 75 years or for an indefinite amount of time, depending on the type of document. Service providers and intermediary service providers are required to keep the information, documents, books and electronic logs under the Law on the Regulation of Electronic Commerce for three years from the date of the transaction.

## DATA BREACH AND CYBERSECURITY

### Security measures

**42** What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

There is no specific legislation dedicated to explaining the security measures that must be taken in online transactions. If the transaction has an aspect of personal data processing, the Personal Data Protection Law (PDPL), which has a broad scope of application, would apply. While the PDPL states that controllers should implement all necessary technical and organisational measures, it does not shed light on how controllers can ensure cybersecurity. The Personal Data Protection Authority (DPA) has published Guidelines on Technical and Organisational Measures, which contain, inter alia, the following measures:

- Controllers should first determine the existing risks and threats and evaluate whether they process sensitive personal data, the privacy level expected due to the characteristics of such data, and the possible outcomes of a breach. Controllers should train their employees and raise awareness in these matters.
- Controllers should develop a personal data security policy.
- Controllers should update their security walls and software and follow patch management procedures. They are encouraged to limit their employees' access to personal databases and follow the instructions regarding passwords therein. They should check software and services in operation, keep log records, develop a reporting mechanism and report security problems officially as soon as possible.
- Devices that contain personal data should be kept physically safe. Controllers should prefer internationally recognised encryption methods.

- When controllers use cloud services for personal data storage, they should check the security measures implemented by the cloud provider. The use of multi-factor authentication, encryption, different encryption keys for different cloud services, and the destruction of encryption keys at the end of the service are encouraged technical measures.
- Controllers should have separate backup servers that are controlled only by the system manager in case of a security breach and should ensure the physical safety of these backup systems.
- The DPA also advises the use of secure and up-to-date hashing algorithms, HTTPS and technologies that differentiate human and computer behaviour, the limitation of unsuccessful login attempts and the creation of a password policy to prevent the leakage of user login information.

In regulated sectors such as banking and finance, insurance and telecommunications, it is required, inter alia, to develop written network security policies, train employees and maintain backup servers. Banks, payment and e-money institutions shall allow access to sensitive customer information after strong authentication. Sensitive customer information shall be stored encrypted as per the national and international standards and transferred by an end-to-end secure transmission.

Additionally, the Turkish Presidency's Digital Transformation Office published a very detailed Guideline on Information and Communication Security in July 2020, and the Guideline on Information and Communication Security Audit in October 2021. These guidelines contain detailed examples and explanations of technical measures to determine a minimum level of security that ensures the confidentiality, integrity and accessibility of data. Public institutions and institutions providing critical infrastructure services fall within the scope of the guidelines. The guidelines mention use of the TS ISO/IEC 19790-24759 standard as a measure to prevent malicious transactions.

## Data breach notification

**43** Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

The PDPL stipulates that data controllers must take necessary technical and organisational measures to avoid any unlawful access or processing of personal data. In the event of a security breach, controllers must notify the Board of Advertisement (the Board) without delay and within 72 hours at the latest after they become aware of such breach. Controllers must also notify the data subjects as soon as reasonably possible after detecting persons affected by the breach. In a recent decision, the Board imposed a fine of 1.9 million Turkish lira on an online food delivery company, given that the company notified the breach eight days after the cybersecurity incident occurred, among other reasons (ie, the extent of the breach and lack of technical and administrative measures).

## Government interception

**44** Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Authorities are permitted lawful access to data under the Criminal Procedure Code. If the applicable conditions are met, the telecommunications operators are required to assist the authorities with the interception of communications.

Companies or operators do not have a specific obligation to decrypt communications or hand out private keys to the authorities. However, as per the Regulation on Detecting, Wiretapping, Evaluation of Signal Data and Recording the Communications (the Wiretapping Regulation), the National Intelligence Service or Intelligence Offices of Security General Directorate or Gendarme General Command have the authority to give written orders to wiretap communications for prosecution of specific crimes such as espionage, crimes against the constitutional integrity or national security. Upon written orders, the Information and Communications Technologies Authority's (ICTA) respective department may require communications service providers to integrate the tools, infrastructure, and other means to decrypt the concerned data.

Additionally, the Regulation on Principle and Procedures for Coded or Encrypted Communications of Public Entities and Natural or Legal Persons requires the manufacturers (or importers) to request approval from the ICTA by submitting the used cryptographic algorithms and keys as well as software or hardware enabling decryption, if need be, before making such services or products available in Turkey. Whether or not approval is mandatory will be determined based on the technical characteristics of the encryption communications. In case of violation of these rules, judicial fines may be imposed as per the Electronic Communications Law.

Finally, amendments were made to the Regulation Amending the Geographic Data Licence Regulation and the Regulation on Geographic Data Permissions, published in 2021. According to these regulations, licensees must submit or ensure the submission of all geographical data, along with data information, to the National Geographical Information Platform in line with the standards published in the Official Gazette within the licence period. All licensees, regardless of the licence type, must register the data and data information related to their activities with the Ministry of Environment, Urbanisation and Climate Change's electronic infrastructure, ensuring accuracy, security, and confidentiality. They should also provide access to information and documents subject to the licence during audits by authorised institutions.

## GAMING

### Legality and regulation

**45** Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Providing a platform for gambling is strictly forbidden by the Turkish Criminal Law. However, online betting is permissible under Turkish law, subject to strict regulations. As per the Regulation on Fixed Odds and Parimutuel Betting Based on Sports Competitions (the Betting Regulation), only legal persons can operate online betting platforms (also called online platform agencies) by obtaining a licence from the Spor Toto Organisation Presidency (Spor Toto). There are various requirements for a legal person to obtain an online platform agency licence from Spor Toto, such as being registered in Turkey as a joint-stock company whose capital meets the threshold determined by Spor Toto. Once the licence is issued, the online platform agency will enter into an agency contract with Spor Toto for a period of up to 10 years. The agency contract will be effective as long as the licence is valid and will automatically be terminated if the corresponding licence is cancelled.

Further, online betting agencies must comply with the necessary operational requirements set forth in the Betting Regulation, including, but not limited to, providing a guarantee for the amount that will be determined by Spor Toto. A natural person who operates an online betting platform without complying with the relevant legislation will be sentenced to between three and six years' imprisonment, and corresponding security measures would apply to any legal persons.

Gambling is considered a misdemeanour as per article 34 of the Misdemeanour Law. A resident or citizen of Turkey can be fined as a result of gambling and, in such case, all related earnings would be transferred to public funds.

While residents and citizens of Turkey are permitted to use online betting platforms, the regulatory age is set at 18. According to the Betting Regulation, online betting platform providers should prevent underaged persons from placing any bets, and no payment shall be made if that person earns a reward. Failure to comply with the provision regarding the regulatory age would result in termination of the licence obtained from Spor Toto.

### Cross-border gaming

**46** Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Enabling people to access parimutuel betting or games of chance operated abroad without permission is a criminal act, and perpetrators could serve four to six years in prison. It is permissible to provide access to a gaming business located abroad; however, access might be restricted as per Law No. 5651 on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications. Additionally, commercial businesses that allow users to connect and use the internet in a physical place cannot

provide access to online or offline games that may have a physical or psychological adverse effect on minors.

## OUTSOURCING

### Key legal issues

**47** What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Outsourcing is regulated within the scope of the Labour Law, which applies to all businesses. Not all services can be outsourced by an employer, but an employer can outsource auxiliary works, which are defined as works related to or dependent on the main operations. To outsource a part of main operations, the outsourced service should be an aspect of the main operations that requires technological know-how and expertise. Technological know-how and expertise are defined as works essential for undertaking the main operations and that are beyond the businesses' expertise. VAT will apply to outsourced services provided by a supplier to a local customer if the services are benefited from in Turkey. Stamp duty would also arise in case of an outsourcing contract.

### Sector-specific issues

**48** Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

Payment institutions and electronic money institutions cannot outsource payment services and e-money issuance activities. There are other related activities that are allowed to be outsourced only when:

- the institution complies with payment services and e-money regulations; and
- the scope of outsourced activities is determined and clarified in a contract between the institution and the other party.

The contract must include provisions to ensure compliance of third parties with the regulations as well; however, the payment and e-money institutions are still held liable. They also need to report their outsourcing transactions to the Central Bank. The Central Bank is authorised to cease outsourcing activities if it comes to the conclusion that the institution does not comply with the provisions on outsourcing, or the service provider has a negative impact on the institution's activities or prevents the Central Bank's audits.

### Contractual terms

**49** Does the law require any particular terms to be included in outsourcing contracts?

The Regulation on Banks' Information Systems and Electronic Banking Services states that outsourcing contracts must include, inter alia, provisions on risk management, data transfers and data destruction, confidentiality, and security incident notifications. Payment

institutions and e-money institutions are required to clarify the other party's obligations in an outsourcing contract. The Regulation on Subcontractors, which is a secondary legislation of the Labour Law, also sets forth the mandatory provisions to be included in outsourcing contracts. For instance, certifications or other relevant documents regarding the outsourced service should be attached to the contract if a service is outsourced owing to a need for technological know-how and expertise. Other provisions that must be inserted in outsourcing contracts include, but are not limited to, the business name and address of the main employer and subcontractor, work assigned, and main operations undertaken in the workplace.

### Employee rights

**50** What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

As per the Labour Law, the decision to outsource a part of the company's operations does not constitute a legitimate reason for employment termination even if the work of such employee is to be outsourced. The employee whose employment has been terminated due to a decision to outsource will be able to request compensation and indemnifications. If the court decides that the termination is unlawful, the employer would be obliged to reinstate its former employee within a month. If the employer fails to reinstate the employee upon the court's decision, it would be obliged to indemnify the employee. The aforementioned rights for reinstatement and compensation are applicable to all employees who fall under the scope of the Labour Law.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

### Rules and restrictions

**51** Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

Turkey published its National Artificial Intelligence Strategy for 2021–2025 (the Strategy) in August 2021. The Strategy places particular emphasis on stakeholders' trust in artificial intelligence (AI) technologies, these technologies' ethical compliance and the establishment of a legal framework for the promotion of AI applications. Proportionality, safety and security, fairness, privacy, transparency and explicability, responsibility and accountability, data sovereignty and stakeholder participation are the principles adopted in the Strategy. The Strategy aims for regulators to act in an agile and inclusive manner to accelerate socio-economic harmonisation.

Until Turkey adopts an AI regulation in light of the Strategy, stakeholders can take into account the Guide published by the Personal Data Protection Authority (DPA) on personal data protection in the field of AI. The Guide states that if the AI application poses a high risk for data subjects, an impact assessment shall be conducted. Each project should follow a

specific personal data protection compliance programme. If the application requires the processing of sensitive personal data, technical and administrative measures shall be implemented more strictly. Developers, manufacturers and service providers should implement privacy by design, and prevent the risk of discrimination and other adverse effects. They should refrain from designing AI products and applications that could result in automated decision-making without taking into account the individuals' opinions.

With regard to AI applications used for identity authentication in electronic communications, certain technical requirements apply. Operators and service providers need to submit a report from a standardisation institute to the Information and Communication Technologies Authority before they use an AI application to confirm an applicant's identity.

## IP rights

**52** Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Currently, there are no specific rules or case law concerning IP and artificial intelligence or machine learning. However, the topic is highly debated among academics. Considering the definition of a 'work' (ie, any intellectual or artistic product bearing the characteristic of its author) and other provisions in the Industrial Property Law, it is generally accepted that AI cannot be an author or inventor. Developers and companies can seek for legal protection afforded to original and non-original (sui generis) databases under the Law on Intellectual and Artistic Works, or file a lawsuit based on unfair competition provisions should there be any violations thereof, until there is more legal certainty.

## Ethics

**53** Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Turkey released its National Artificial Intelligence Strategy for the period 2021–2025 in August 2021. The Strategy focuses on building trust in AI technologies among stakeholders, ensuring the ethical compliance of these technologies, and creating a legal framework to foster AI applications. The Strategy is based on principles such as proportionality, safety and security, fairness, privacy, transparency, explicability, responsibility, accountability, data sovereignty and stakeholder participation. The main objective is to encourage regulators to take an agile and inclusive approach to promoting the harmonisation of socio-economic aspects related to AI. There are also ethical rules on the use of AI published by the Turkish Bar Association and IT Law Commissions of Bar Associations in Turkey, AI application and research centres of universities, NGOs and company managements (especially in sectors where the use of AI poses risks, such as banking). Although no central regulation has been established yet, all stakeholders drawing attention to AI ethics emphasise that AI systems should be impartial, transparent, explainable, resilient and accountable, and should put an emphasis on privacy, social benefit and sustainability.

## TAXATION

### Online sales

**54** Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

All services that are performed or whose benefits are consumed in Turkey would be subject to VAT. Other than VAT, special consumption tax (otherwise known as ÖTV) may be applicable for products such as electronic appliances.

All companies incorporated in Turkey or having a residence, business place, legal centre or business centre in Turkey are liable for VAT payment. In 2018, the Revenue Administration issued a ruling on the sale of online games by a company incorporated in Turkey and stated that all sales of online games are subject to VAT except for sales to users abroad. Sales to users residing abroad would be defined as services export, thus would be exempted from VAT.

As per article 9 of the VAT Law, the sale of online products by those who do not have a residence, workplace, legal centre or business centre in Turkey is subject to VAT as long as the services are provided electronically to natural persons who are not VAT payers in Turkey. In this case, VAT will be paid by the companies providing the service. Such corporations need to register with the Revenue Administration through the Special VAT Registration for E-Service Providers. In the case of business-to-business sales, the same corporations still need to fill out the VAT declaration, yet VAT would be paid by the buyer (ie, reverse charge mechanism).

Effective from March 2020, the sale of any audio, visual or digital content on digital platforms (including computer programs, applications, music, video, games, in-app purchases and other similar products) and digital services offered to listen, watch, play or record these contents in electronic media or use them in electronic devices are subject to digital services tax set at 7.5 per cent. The tax is calculated based on the revenue generated from Turkey. Digital services tax applies to all persons generating revenue from Turkey without making any distinction to a full or limited taxpayer status, save from certain exemptions listed in Law No. 7194 on Digital Services Tax.

In addition to the aforementioned taxes, stamp duty may be applicable in some instances. In accordance with the General Communique on Stamp Tax Law (Serial No. 60), any agreement concluded via an online platform would be subject to stamp duty if it is concluded via electronic signature, subject to certain exceptions.

### Server placement

**55** What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

Corporations are taxed based on the location of their legal or business centre. Those who have their legal or business centre in Turkey are defined as taxpayers with full liability, whereas those who do not are defined as taxpayers with limited liability. Full taxpayers are

taxed based on the revenues they generate globally, whereas limited taxpayers are taxed based on the revenue they generate only from Turkey. Therefore, establishing what constitutes a business centre is the key question that should be evaluated as per the Turkish tax law and the relevant bilateral agreements for the avoidance of double taxation. In most cases, a fixed place that is assigned for commercial activities constitutes a business centre. The Turkish Revenue Administration considers the server on which the website is stored and accessed as equipment with a physical location; thereby such location may constitute a fixed place of business of the company that operates the server. As a result of this definition, placing servers in Turkey may result in foreign corporations being declared as taxpayers with limited liability. Therefore, these corporations may be liable for paying corporate taxes, which will be calculated based on the revenue generated from Turkey.

### Electronic invoicing

**56** Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

As authorised by the Tax Procedure Code (Law No. 213), the Ministry of Treasure and Finance issued Communiqué No. 509 on the principles and procedures of forming, organising, transferring, storing and submitting fiscal documents electronically. The Communiqué states that 'e-invoice' and 'e-archive invoice' are not new types of documents and have the same legal characteristics as their physical equivalents. According to the new regulation published in late 2022, companies with a gross sales revenue of 3 million Turkish lira and above are required to transition to e-invoicing by 1 July 2023, and to e-book application by 1 January 2024. Taxpayers that are registered for the 'e-invoice' system must draw up 'e-invoices' electronically when they sell goods or provide services to each other. It is mandatory that:

- taxpayers use the document formats set out in the technical guides;
- e-invoices are transmitted through the e-invoice application; and
- e-archive invoices are stored electronically and submitted to authorities when requested.

Currently, taxpayers who are obliged to use e-invoicing and companies subject to independent audit must use e-book applications.

## DISPUTE RESOLUTION

### Venues

**57** Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

To ascertain which court has the jurisdiction to decide on a dispute, the nature of the dispute must first be identified. If a dispute arises from a transaction concluded online, the competent court will be determined based on its qualification as a consumer transaction or not. Any disputes arising from an online consumer transaction shall be first referred to consumer arbitration committees provided that the value of the dispute is lower than 66,000

Turkish lira. Decisions rendered by consumer arbitration committees can be appealed to consumer courts. Any disputes with a value higher than 66,000 Turkish lira can be brought directly before the consumer courts. If the online transaction is concluded with a trader or related to a commercial enterprise, parties first shall refer the dispute to mediators; only thereafter can the dispute be brought before the courts. There are specialist courts in the fields of cybercrime and financial crime under Law No. 6493 on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions.

### ADR

**58** What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

There is no ADR available specifically for online or digital disputes, other than those mentioned specifically in the relevant laws, such as consumer arbitration committees and arbitration committees for domain names. According to the Turkish Commercial Code, all commercial disputes shall first be referred to mediation before initiating a lawsuit before the competent courts. Online or digital disputes arising from business-to-business contracts can be referred to arbitration in principle. Depending on the technical and complex nature of such contracts, arbitration may be preferable since the parties can select and appoint arbitrators with the necessary technical knowledge. That said, concluding arbitration clauses electronically can raise issues, such as whether the parties have specific authority to sign such clauses.

## UPDATE AND TRENDS

### Key trends and developments

**59** Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The Turkish legal framework on digital business is becoming more extensive and complex every year. From the consumer law perspective, intermediary service providers' obligations have been expanded due to the amendments made in the Consumer Protection Law. Additionally, the Law on the Regulation of Electronic Commerce was significantly revised in July 2022 and mostly entered into force in 2023. Accordingly, e-commerce service providers and e-commerce intermediary service providers must go through a fundamental and challenging compliance process. When the Law on the Regulation of Electronic Commerce came into effect, the stakeholders applied to the Constitutional Court for the annulment of the provisions of the Law on the Regulation of Electronic Commerce regarding the obligations of the electronic commerce intermediary service provider and the electronic commerce licence, but the Constitutional Court rejected this application in July 2023.

On the other hand, the Personal Data Protection Law is expected to be revised in line with the standards of the European Union.

Court decisions on the seizure of crypto asset accounts and the sale of non-fungible tokens have attracted the attention of the public and legal practitioners. The new regulation on crypto assets has been one of the hottest topics, and further amendments in the capital markets regulations are expected to bring crypto assets within the scope of regulation. Another important development in 2022 was that the Banking Regulation and Supervision Agency specified the rules on digital banking and banking as a service model. Furthermore, the rise of open banking in Turkey and related developments in fintech that align with the global data liberalisation trend have been a hot topic.

The revisions to Law No. 5651 on Regulation of Publications on the Internet and Prevention of Crimes Committed by Means of Such Publications at the end of 2022 have been the product of the fight against disinformation and more effective online content moderation.

BODEN LAW

| | |
|---|---|
| Sinem Mermer | smermer@boden-law.com |
| İsra Tekin | itekin@boden-law.com |
| Dila Küçükali | dkucukali@boden-law.com |

Levent Loft 1, Buyukdere Cad No 201 D 27 Levent, Istanbul 34394, Turkey
Tel: +90 212 251 15 00
www.boden-law.com

# MORE TOPICS AVAILABLE ONLINE AT LEXOLOGY.COM/GTDT

## Including

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements