

DIGITAL BUSINESS

Israel



Digital Business

Consulting editors

Ashley Winton

Mishcon de Reya LLP

Quick reference guide enabling side-by-side comparison of local insights into legal and regulatory framework; contracting on the internet; security, including security of payment; domain names; advertising; financial services; defamation; intellectual property; data protection; taxation; gambling; outsourcing; online publishing; dispute resolution; and recent trends.

Generated 24 October 2022

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. © Copyright 2006 - 2022 Law Business Research

Table of contents

LEGAL AND REGULATORY FRAMEWORK

Government approach

Legislation

Regulatory bodies

Jurisdiction

Establishing a business

CONTRACTING ON THE INTERNET

Contract formation

Applicable laws

Electronic signatures

Breach

FINANCIAL SERVICES

Regulation

Electronic money and digital assets

Digital and crypto wallets

Electronic payment systems

Online identity

DOMAIN NAMES AND URLS

Registration procedures

IP ownership

ADVERTISING

Regulation

Targeted advertising and online behavioural advertising

Misleading advertising

Restrictions

Hosting liability

Email marketing

ONLINE PUBLISHING

Content liability

ISP liability



Shutdown and takedown

INTELLECTUAL PROPERTY

Data and databases

Third-party links and content

Metaverse and online platforms

Exhaustion of rights and first-sale doctrine

Administrative enforcement

Civil remedies

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

Registration and appointment of data protection officer

Extraterritorial issues

Bases for processing

Data export and data sovereignty

Sale of data to third parties

Consumer redress

DOCUMENT DIGITISATION AND RETENTION

Digitisation

Retention

DATA BREACH AND CYBERSECURITY

Security measures

Data breach notification

Government interception

GAMING

Legality and regulation

Cross-border gaming

OUTSOURCING

Key legal issues

Sector-specific issues

Contractual terms

Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

IP rights

TAXATION

Online sales

Server placement

Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

Contributors

Israel



Eyal Roy Sage

eyals@ayr.co.il

AYR - Amar Reiter Jeanne Shochatovitch & Co



Shlomi Bardugo

shlomib@ayr.co.il

AYR - Amar Reiter Jeanne Shochatovitch & Co

LEGAL AND REGULATORY FRAMEWORK

Government approach

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 that 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.

Law stated - 17 August 2022

Legislation

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

These are the Consumer Protection Law; Protection of Privacy Law ; Communications law (Telecommunications and broadcasts); Standard Contracts Law ; and their respective regulations and guidelines.

Law stated - 17 August 2022

Regulatory bodies

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

These are the Ministry of Communications; The Privacy Protection Authority; Consumer Protection and Fair-Trade Authority.

Law stated - 17 August 2022

Jurisdiction

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?

Recent Supreme Court case law 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, as were provisions forcing arbitration that 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.

Law stated - 17 August 2022

Establishing a business

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 foreign providers to register as a foreign company (or set up a local entity).

Law stated - 17 August 2022

CONTRACTING ON THE INTERNET

Contract formation

Is it possible to form and conclude 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.

Law stated - 17 August 2022

Applicable laws

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 contracts 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.

Law stated - 17 August 2022

Electronic signatures



LEXOLOGY

Getting The Deal Through

How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction?

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: (1) simple electronic signature (defined as electronic data or an electronic sign, that is attached to or associated with an electronic message); (2) 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 (3) 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 also is prima facie evidence that it was signed by the owner of the device.

Certification Authorities are licensed and supervised.

Law stated - 17 August 2022

Breach

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

No.

Law stated - 17 August 2022

FINANCIAL SERVICES

Regulation

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 and the Supervisor of Banks, and the Israel Securities Authorities. Each regulator issues rules on advertising and selling financial services.

Electronic money and digital assets

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 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 assets to include a crypto-currency, 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.

In respect of holding and using digital assets, now, there are no regulatory restrictions on the mere possession and use of digital currencies. That said, we will note that the banks in Israel are reluctant to allow their clients to deposit to their bank accounts FIAT money that is originated from the sale of digital currencies. This is due to the zero-risk appetite policy applied by the banks in terms of AML compliance.

Law stated - 17 August 2022

Digital and crypto wallets

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 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 assets to include a crypto-currency, 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.

Law stated - 17 August 2022

Electronic payment systems

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. 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 will be able to get access to an online system that allows receiving financial information about their clients (and with their consent) from different information sources and transfer to those information sources, additional information about the client in the same system.

Law stated - 17 August 2022

Online identity

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.

Law stated - 17 August 2022

DOMAIN NAMES AND URLS

Registration procedures

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

Registration of 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 a resident in the country.

Registering domain names designed to hinder access to a competitors' site can amount to an unfair business practice.

Law stated - 17 August 2022

IP ownership

Can domain names or URLs be the subject of trademarks 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 challenging a competitive use or registration of a similar domain name or URL, as 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.

Law stated - 17 August 2022

ADVERTISING

Regulation

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.

Law stated - 17 August 2022

Targeted advertising and online behavioural advertising

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

The Protection of Privacy Law (sections 17C-17I); 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 needs to be identified as such, and 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, but to the extent the information is personal information, privacy laws apply.

Law stated - 17 August 2022

Misleading advertising

Are there rules against misleading online advertising?

There are no specific rules on online advertising. Section 2 of the Consumer Protection Law prohibit 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.

Law stated - 17 August 2022

Restrictions

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

Not specifically. Advertising of unlicensed gambling and of prostitution is prohibited both online and offline.

Law stated - 17 August 2022

Hosting liability

What is the liability of content providers and parties that merely host the content, such as ISPs?
Can any other parties be liable?

Theoretically, liability for contributory copyright breach might arise against a party who merely hosts content, if it has actual knowledge of the infringement. 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 order can be given against ISPs and hosting providers.

Law stated - 17 August 2022

Email marketing

What regulations and guidance apply to email, SMS and other distance marketing?

Unsolicited email, SMS, fax 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 new law setting up a national do not call registry would prohibit cold calling to numbers on the registry.

Distance marketing by any means in subject to the disclosure and cooling off provisions of the Consumer Protection Law.

Law stated - 17 August 2022

ONLINE PUBLISHING

Content liability

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.

Law stated - 17 August 2022

ISP liability

Are internet service providers (ISPs) liable for content displayed on their sites? How can ISPs limit or exclude liability?

There are no specific statutory rules with regard to liability for content they merely host. ISPs would be liable for content they post themselves. As for content that is merely hosted by ISPs.

Theoretically, liability for contributory copyright breach might arise against a party who merely hosts content, if it has actual knowledge of the infringement. 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 order can be given against providers of internet connectivity and hosting providers.

Law stated - 17 August 2022

Shutdown and takedown

Can an online content provider or ISP shut down a web page containing defamatory material without court authorisation?

An online content provider or ISP 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 statutory law, but would seem to be a reasonable application of the general legal principles governing this question. Having said that, there is a difference between an internet site and an ISP: while an ISP is committed to neutrality and would generally refrain from shutting down a web page without a court order, an online content provider has the discretion to shut down a web page containing defamatory material based on sufficient evidence.

In 2019, the Copyright Law was amended to grant copyright holders the possibility to apply to the court for an order to instruct another person to provide the court with identifying details (such as IP address) of an alleged infringer who anonymously made available to the public infringing content, in order to enable the applicant to file a claim against such an infringer. According to the amendment, the court is given the discretion of whether to reveal the identity of the infringer, taking into account a variety of considerations. The court may also appoint an expert who will assist in clarifying the identity of the infringer.

The 2019 amendment also empowers courts to order ISPs and hosting providers to block access to infringing content or to sites with significant infringing content.

Law stated - 17 August 2022

INTELLECTUAL PROPERTY

Data and databases

Are data and databases protected by IP rights?

Some databases are protected by IP rights (under 'literary work'). According to section 4(b), '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.

Law stated - 17 August 2022

Third-party links and content

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

Yes.

Law stated - 17 August 2022

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 intellectual property laws (specifically, copyright), 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.

Law stated - 17 August 2022

Metaverse and online platforms

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

No.

Law stated - 17 August 2022

Exhaustion of rights and first-sale doctrine

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 in another territory. 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.

Law stated - 17 August 2022

Administrative enforcement

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.

Law stated - 17 August 2022

Civil remedies

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 the appointment of receivers with rights 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, orders for identifying anonymous infringers; and internet access blocking orders.

Law stated - 17 August 2022

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

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, ID numbers email suffix and more.

'Sensitive Information' is defined as: 'information on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person'. Databases that contain 'sensitive data' are subject to different registration requirements as well as to more information security standards.

Law stated - 17 August 2022

Registration and appointment of data protection officer

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?

Databases 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.

Law stated - 17 August 2022

Extraterritorial issues

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 extra-territorial provisions, although powers would extend to local branches and subsidiaries.

There is currently no requirement to appoint a local representative.

Law stated - 17 August 2022

Bases for processing

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 has two legal bases for data processing – consent, and legal empowerment or obligation.

However, consent in Israeli data protection law is quite a flexible concept. While it needs to be informed, it can be implicit (which means it need not be freely given), although in some cases, where processing is not necessary (for example, for the performance of a contract), express consent is required. Processing for direct mailing services (ie, profiled personal data used for marketing by third parties) requires opt-in consent. 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 General Data Protection Regulation (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.

Law stated - 17 August 2022

Data export and data sovereignty

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 which 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 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).

Government guidelines require government agencies to maintain certain types of sensitive data and operations to be kept in country, but there are exceptions.

Law stated - 17 August 2022

Sale of data to third parties

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 which have an obvious need for the data, such as for fulfilment or payment) can generally be done with implicit consent.

Law stated - 17 August 2022

Consumer redress

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 right to have data used only for direct (profiled) marketing to be deleted. These rights are not limited to citizens, but also apply on a foreign data subject's personal data that is being collected or processed in Israel.

Law stated - 17 August 2022

DOCUMENT DIGITISATION AND RETENTION

Digitisation

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.

Law stated - 17 August 2022

Retention

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.

Protection of Privacy Regulations (Information Security) contains two provisions on data retention: databases should not contain excess personal information (that is, personal information no longer needed for the purpose for which it was collected); and security logs should be kept for 24 months.

Law stated - 17 August 2022

DATA BREACH AND CYBERSECURITY

Security measures

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.
- Yes, the Protection of Privacy Regulations (Information Security) require organisations that 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.

Law stated - 17 August 2022

Data breach notification

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 without undue delay (and no later than 72 hours) 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, Israel Securities Authority).

Law stated - 17 August 2022

Government interception

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 telecommunications operators must give certain agencies access to communications data (not content) pursuant to the Criminal Procedures (Enforcement Powers – Data Communications) Law 2007. Subscriber information is generally available without a court order. 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.

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.

Communications Law (Telecommunications and Broadcasting) 1982. This law applies only to licensed telecommunications operators. It does not itself compel the disclosure of information, therefore, no warrant or subpoena is required; however, it does compel cooperation with certain enforcement and security agencies, who may then access information autonomously, within their legal mandates.

Finally, courts can issue intercept orders in cases involving serious crimes, and ministers can permit short-term intercepts in cases involving national security.

Law stated - 17 August 2022

GAMING

Legality and regulation

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. All prize-bearing games of chance (no matter how trivial the prize) require a licence from the Ministry of Finance, but only the national lottery received such a licence. There are some allowances for marketing campaigns involving raffles, and some exemptions for charitable and similar activities.

Law stated - 17 August 2022

Cross-border gaming

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.

Law stated - 17 August 2022

OUTSOURCING

Key legal issues

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.

Law stated - 17 August 2022

Sector-specific issues

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 generally requires risk assessment and a written contract covering key aspects of the outsourced service.

Law stated - 17 August 2022

Contractual terms

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 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, to use the data only according to the agreement and to implement the data security measures prescribed in the agreement;
- where a database controller permitted 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 of any security incidents.

Law stated - 17 August 2022

Employee rights

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 many cases employees are entitled to a severance package even if they quit.

Law stated - 17 August 2022

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

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?

Protection of Privacy Authority guidance is that data subjects be informed of automatic decision-making, especially based on artificial intelligence. The agency 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 artificial intelligence, machine learning, automated decision making or profiling.

Law stated - 17 August 2022

IP rights

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.

Law stated - 17 August 2022

TAXATION

Online sales

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 not different from offline services. In both cases, income derived from the provision of services in connection with digital assets is taxable income under the general rules of taxation. However, the government approach, in the past few years, is to approve a complete reform in the matter, and to impose a tax on such activities. Such reform, however, has yet to be approved.

Law stated - 17 August 2022

Server placement

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 main question that arises in this regard is whether the placing of servers in Israel constitutes a permanent establishment that would make income attributed to the permanent establishment taxable in Israel. Servers as such are likely not enough to create a permanent establishment, and the answer would depend on additional circumstances.

Law stated - 17 August 2022

Electronic invoicing

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.

Law stated - 17 August 2022

DISPUTE RESOLUTION

Venues

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

No.

Law stated - 17 August 2022

ADR

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.

Law stated - 17 August 2022

UPDATE AND TRENDS

Key trends and developments

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.

A national 'do not call' registry will begin operating in late 2022, and is expected to severely curtail cold calling. It would also apply to chatbots. This limitation will come on top of already strict rules applying to unsolicited emails and text messages.

An amendment to the Communications (Telecommunications and broadcasts) Law 1982, which required many telecommunications service providers to seek a licence is expected to enter into force in late 2022, replacing most licences with simple registration.

Israel is currently recognised as providing an adequate level of data protection thereby allowing free data flows from the EU to Israel. Israel's status is under review, and the government is considering stop-gap measures to address key EU concerns. If the adequacy status is removed, this could adversely affect digital operations involving in Israel.

The authors gratefully acknowledge the assistance of Yizhar Tal, Lior Talmud, Shir Shoshany-Katz, Or Rotter, Yuval Achituv and Niv Azran in writing this chapter.

Law stated - 17 August 2022

Jurisdictions

	Belgium	Astrea
	Chile	Magliona Abogados
	China	Buren NV
	Cyprus	Antoniou McCollum & Co LLC
	France	UGGC Avocats
	Germany	SKW Schwarz
	Gibraltar	Hassans
	Hungary	VJT & Partners
	India	AZB & Partners
	Israel	AYR - Amar Reiter Jeanne Shochatovitch & Co
	Italy	ICT Legal Consulting
	Japan	Anderson Mōri & Tomotsune
	Malaysia	Raja, Darryl & Loh
	South Korea	Barun Law LLC
	Taiwan	Lee and Li Attorneys at Law
	Turkey	Boden Law