Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cyber Security

Israel

AYR - Amar Reiter Jeanne Shochatovitch & Co.

chambersandpartners.com

2018

ISRAEL

LAW AND PRACTICE: p.3

Contributed by AYR - Amar Reiter Jeanne Shochatovitch & Co.

The 'Law & Practice' sections provide easily accessible information on navigating the legal system when conducting business in the jurisdiction. Leading lawyers explain local law and practice at key transactional stages and for crucial aspects of doing business.

Law and Practice

Contributed by AYR - Amar Reiter Jeanne Shochatovitch & Co.

CONTENTS

1. Basic National Legal Regime **p.4**
1.1 Laws p.4
1.2 Regulators p.5
1.3 Administration Process p.5
1.4 System Characteristics p.5
1.5 Key Developments p.6
1.6 Significant Pending Changes, Hot Topics and Issues p.6

2. Fundamental Laws **p.6**
2.1 Omnibus Laws and General Requirements p.6
2.2 Sectoral Issues p.7
2.3 Online Marketing p.8
2.4 Workplace Privacy p.8
2.5 Enforcement and Litigation p.8

3. Law Enforcement and National Security Access and Surveillance **p.9**
3.1 Laws and Standards for Access to Data for Serious Crimes p.9
3.2 Laws and Standards for Access to Data for National Security Purposes p.9
3.3 Invoking a Foreign Government p.9
3.4 Key Privacy Issues, Conflicts and Public Debates p.9

4. International Considerations **p.9**
4.1 Restrictions on International Data Issues p.9
4.2 Mechanisms That Apply to International Data Transfers p.10
4.3 Data Localisation Requirements p.10
4.4 Sharing Technical Details p.10

5. Emerging Digital and Technology Issues **p.10**
5.1 Addressing Current Issues in Law p.10

6. Cybersecurity and Data Breaches **p.10**
6.1 Key Laws and Regulators p.10
6.2 Key Frameworks p.11
6.3 Legal Requirements p.11
6.4 Key Multinational Relationships p.11
6.5 Key Affirmative Security Requirements p.11
6.6 Data Breach Reporting and Notification p.11
6.7 Cyberthreat Information Sharing Arrangements p.12
6.8 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation p.12

AYR - Amar Reiter Jeanne Shochatovitch & Co.'s data protection team has four dedicated lawyers and is one of Israeli's largest. AYR has a distinctly strong technology practice which serves key international and domestic clients in the IT, telecoms, media, banking, insurance, transportation, and retail, as well as numerous start-ups in Israel's burgeoning innovation scene. The firm's focus on technology is manifest in many of its other practices, including IP and antitrust/competition practices (where lawyers have unique experience in advising on the interface between IP, technology, and competition), its commercial transactions practice, its real estate and planning practices (experienced in serving the telecommunications industry), and the litigation practice with its dedicated department for defending class action claims (which currently handles some of Israel's most significant privacy-related class actions).

Author



Eyal Roy Sage is head of department at the firm. He specialises in data protection, technology, antitrust/competition, telecommunications and media and intellectual property.

1. Basic National Legal Regime

1.1 Laws

The Israeli legal system has continental, American and common-law influences. It has no written constitution, but does have "Basic Laws" which enshrine constitutional values and rights.

From a privacy perspective, section 7 in the Basic Law: Human Dignity and Liberty is most relevant. This states that: "(a) All persons have the right to privacy and to intimacy; (b) there shall be no entry into the private domain of a person without that person's consent; (c) no search shall be conducted in the private domain or on the body of a person, nor in the body or effects of a person; (d) there shall be no violation of the secrecy of the communications, writings, or records of a person".

This broad and absolute right is qualified by a "limitation clause", allowing limitations on the basic right if they befit the values of Israel, are for a proper purpose and proportionate.

The Privacy Protection Law ("PPL"), enacted in 1981, is at the centre of Israeli data protection law. It has two key parts, one of which deals with general privacy protection (irrespective of data processing), and one which deals specifically with databases. Israeli jurisprudence has extended the first part's general privacy protections to the second part, so that data subjects' rights are protected by the first part as well, including its principles of purpose limitation and informed consent, but consent may be implied.

The first clause of the PPL prohibits the infringement of privacy without consent. It then goes on to give examples of infringement of privacy, which include spying or trailing a person in a manner likely to harass, or disclosing information about a person's private affairs for a purpose other than that for which it was given.

New data security regulations, due to enter into force in May 2018, introduce detailed data security obligations in relation to data processing, as well as a new breach notification requirement.

Regulations dating back to 2001 limit data exports and usefully note the basic principles of Israeli data processing:

- information must be collected and processed in a lawful and fair manner;
- information must be kept, used and transferred only for the same purpose for which it was received;
- information must be accurate and up-to-date;
- data subjects have the right to review the information and demand its correction; and
- there is an obligation to implement due measures to protect the databases.

Numerous guidelines fill the gap between the PPL's dated provisions and modern data processing realities, covering such matters as outsourcing and security cameras.

Cybersecurity is mostly governed by the Regulation of Security in Public Entities Law, 1998, which gives the General Security Services ("GSS") and the National Cyber Security Authority the right to issue orders regarding security, including cybersecurity, to covered entities.

The PPL also contains definitions of "information" and "sensitive information". There is no definition of personal data based on the possibility, or likelihood, of an individual being identified. Instead, the PPL specifies that "information" means "data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs' of a person". Whilst on the face of it the PPL is very narrow in scope, courts have taken a very wide view of what constitutes personal information. The Supreme Court also found that the capacity of computerised databases to store, match and transfer large volumes of information, which could be used to compile blacklists against the interests of data subjects, requires a broad interpretation of the term "information". For example, in a landmark 1988 case, the Supreme Court held that the term "information" covers such details as a person's address and telephone number, bank account number, national ID number and, many years before Facebook existed, a person's "list of friends". In effect, this narrowed the gap between PPL and continental definitions of personal data. Other cases, guidelines, and regulations have further expanded the definition of "information", resulting in most identified or identifiable personal information being covered by the PPL.

1.2 Regulators

The recently renamed Privacy Protection Authority ("PPA", previously the Israel Law, Information and Technology Authority) is a unit in the Ministry of Justice that encompasses several statutory regulators related to the data processing, such as the Registrar of Databases (the main data processing regulator) and the Registrar of Certificate Authorities.

The Registrar of Databases in the PPA registers databases (most commercially used databases are registrable, and the registrar has a right to require registration of otherwise not registrable databases), and enforces the other provisions of the PPL, including those dealing with data security and direct marketing. The PPA's refusal to register a database (or to order its deletion) in effect means that processing the affected data is prohibited.

The PPA has criminal and administrative investigative and enforcement powers. Its investigators have the power to enter business premises where data processing takes place without a warrant, and have other auxiliary powers, such as the power to require the production of documents. The PPA also has the power to issue guidelines.

The Law for the Regulation of Security in Public Entities, 1998, grants the General Security Service ("GSS") (with respect to telecommunications operators) and the National Cyber Security Authority (with respect to certain other structurally important entities, including private companies), the right to instruct covered entities to take such cybersecurity defensive action as the regulator may order. The regulatory powers include the right to audit.

Cybersecurity in regulated industries is also handled by their sectoral regulators, such as the Supervisor of Banks.

Investigations are instigated at regulators' discretion. It is likely that investigative activity will increase after May 2018, when the new data security regulations enter into force.

1.3 Administration Process

A normal supervision process starts when the PPA learns of a possible breach of the law, or the PPA is interested in looking into an activity or a sector, such as the Internet of Things ("IoT"). The PPA normally sends document requests, which are mandatory, although it also has the right to audit and to seize documents, including unannounced. No warrant is needed if the audit or seizure takes place on business premises, although if the PPA needs to penetrate computers without consent, a warrant is required. The PPA has an investigatory arm which has a forensic lab at its disposal.

General administrative law requires the PPA to give supervised entities a right of audience before making a final decision, which may then be appealed to an administrative court. Criminal enforcement takes place in normal criminal courts.

Administrative sanctions include modest fines, orders to cease processing and to destroy data and findings, which the agency publishes on its website and which may, and do, result in class actions.

1.4 System Characteristics

Although Israel's main data processing law dates to 1981, in 2009 it was found by the EU's Article 29 Working Party to give an adequate level of protection, a finding that was formalised by a European Commission Decision in January 2011. In the PPA's 2016 annual report the agency promised to close any gaps with the General Data Protection Regulation ("GDPR").

Not only are the PPL's general principles similar to those expressed in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, PPA guidelines appear to follow EU law closely. For example, the PPL's modest access rights provisions have been interpreted by the PPA to encompass virtually identical rights to the GDPR's. GDPR provisions and PPA 2010 guidelines on outsourcing share many similar provisions.

On the other hand, the PPA is constrained by the very modest administrative fines it can impose – ILS25,000 (approximately USD7,000). Because criminal proceedings are reserved for the most egregious abuses, the PPA has very limited deterrents. In the many cases not warranting an or-

der to delete data – the ultimate administrative measure – the only real deterrent is the possibility of class action resulting from the publishing of the findings of an investigation.

1.5 Key Developments

The PPA issued two significant guidelines. The first deals with the right of access, expanding the right to almost all data held on an individual (including recorded calls) and giving a right to receive such data electronically, expanding on the PPL's modest requirement giving data subjects the right to review personal data physically in defined categories "in the locality where the database is located". The second deals with profiled direct marketing, which, due to peculiarities of the PPL, the PPA uses as a vehicle to impose a right similar to the right to be forgotten (very limited in the PPL) on any controllers who use their data for marketing.

Several major new civil suits seeking certification as class actions were filed, dealing with such diverse matters as processing location data for anonymisation and statistical purposes and for profiling.

In April 2017, the National Cyber Security Authority published its cyber-defence methodology guidelines. While these are only recommendations, it is likely that the methodology will become the yardstick against which the conduct of organisations will be measured when their liability for security breaches is evaluated. Moreover, the methodology is set to become binding on listed companies under an instruction of the Israel Securities Authority.

1.6 Significant Pending Changes, Hot Topics and Issues

An overhaul of the PPL, enacted in 1981 and only modestly amended since, is long overdue. The PPA is making a significant effort to close any gaps by issuing guidelines; these guidelines sometimes appear to significantly deviate from the PPL.

In February 2018, the government tabled a bill that, if enacted, would significantly increase the PPA's powers to impose administrative fines, which could reach ILS 3,200,000 (approximately USD 900,000) (double the amount for repeat offenders) per incident. The bill would also criminalise breach of the purpose limitation principle, and impose criminal liability on company officers.

In May 2018, sweeping new data security regulations will enter into force, replacing the outdated 1986 regulations.

The EU Commission is reportedly reviewing Israel's adequacy status.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The PPL sets out various registration, purpose-limitation, transparency and security requirements, as well as individual rights of access and rectification. These requirements are linked to the size and nature of the information stored, to how the information was collected (directly or indirectly), whether the database is held by the public or private sector, or used for direct marketing.

Most databases are registrable; the registration record must list any processors. Processors acting for more than five controllers must file an annual report listing the database numbers which they process. Security and confidentiality obligations applicable to all databases include a professional duty of secrecy for those having access to a database.

There is no requirement to appoint a privacy or data protection officer as such. The functions recognised in the PPL are those of a "manager" of a database, and a "data security manager". All registrable databases must have a "manager". The manager is responsible for the "confidentiality" and data security of the data in the database. The database manager must also hold a management position in the controller.

A data security manager must be appointed by processors serving more than five controllers, public bodies, banks, financial institutions and rating agencies.

The new data security regulations require controllers and processors to put in place a detailed data security procedure. Banks, financial institutions and other regulated entities are subject to additional requirements set by their regulator and under the Law for the Regulation of Security in Public Entities, 1998.

There is no obligation to adopt a privacy policy (as opposed to a data security procedure). However, such policies are commonly used to inform data subjects as part of obtaining consent or establishing another basis for processing.

Regarding privacy by design and privacy impact assessment, the PPA published position papers on privacy by design and data privacy impact assessments, but there is no general rule requiring mandating the adoption of either. However, the PPA suggested the adoption of a DPIA could help organisations avoid enforcement action.

Data subjects have a right of access and a right to have erroneous data about them corrected. A right to expunge exists only if the controller refuses to correct erroneous data.

The PPL does not directly address anonymisation, de-identification and pseudonymisation, but the PPA has opined

that anonymisation is a substitute to deletion because the PPL does not apply to properly anonymised data. Several class action claims raise questions related to anonymisation, including whether anonymisation in and of itself complies with the purpose limitation principle.

A breach of privacy is a tort, and the normal heads of damage apply, including pecuniary and non-pecuniary damages. An amendment to the PPL addresses the difficulty in proving harm by providing for statutory damages, but this provision does not apply to class actions.

It appears that under unjust enrichment theories, revenues received due to processing in breach of privacy may be disgorged. This could significantly affect big data monetisation.

2.2 Sectoral Issues

The PPL defines "sensitive data" as data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person. Case law, PPA guidelines and the new data security regulations have broadened these categories. For example, a person's "conduct in private", mental state, genetic data, criminal record, communications data (including location data), biometric data and consumer habits from which any of the above may be inferred all raise the security level of a database. PPA guidelines indicate that employee screening reports and security camera footage are all considered sensitive.

Financial Data

Under the Credit Data Service Law, 2002 (and its successor law, the Credit Data Law, which will enter into force in October 2018), only licensed agencies may engage in credit rating. Under the new Credit Data Law, only the Bank of Israel will be allowed to collect and share credit history. The new Credit Data Law limits the statistical model used for rating, which must not take account of gender, age, sexual orientation, race, religion, country of origin, nationality, place of residence, marital status, or health.

A PPA guideline prohibits financial institutions from using data they receive from courts about foreclosures against their clients for any purposes other than foreclosure; this limitation prohibits use of the data for credit risk assessment.

Health Data

In addition to the PPL's provisions on sensitive data, the Patient Rights Law, 1996, limits disclosure of medical data to the following:

- the patient has given consent;
- there is a legal obligation to disclose the data;
- the disclosure is to another health service provider for the purpose of medical care;
- the ethics committee has granted permission where there is a concern that disclosing the data to the patient might seriously harm his or her health or mental condition;
- the ethics committee has allowed the disclosure, after hearing the patient, because it is essential to protect the public or a third party;
- the data is disclosed to the health provider who provides care to the patient;
- the data is provided for archiving pursuant to law; and
- for research purposes, provided the data is not identified.

Health data held by financial institutions, such as insurance companies, is also subject to regulation by the sectoral regulator.

Communications Data

While the PPL does not directly address communications data, the new data security regulations do cover such data. In addition, enforcement agencies' access to communications data is regulated by the Criminal Procedure Law (Enforcement Powers – Communications Data), 2007. In most cases such access requires a court order.

In terms of the internet, there is no obligation to adopt a privacy policy. However, such policies are commonly used to inform data subjects (as required by the PPL's transparency principle), or as part of obtaining consent. There is no equivalent in Israel to the EU's "cookie law". General data processing rules apply to the processing of location and demographic data relating to an identified, or identifiable, individual. Data subjects should be informed of the processing, and, to the extent practicable and subject to the controller's legitimate interests and other overriding requirements, have a right to opt out of the processing of data not directly related to operations – this is a result of data subjects' right to be removed from databases used for direct marketing, which is basically any advertising based on profiling.

There is no specific privacy regulation of social media, search engines, or large online platforms, although the PPA recently opined that antitrust principles could affect how privacy law is applied to large online platforms.

The Supreme Court found there is no general right to be forgotten under Israeli law. However, there does exist a right to have one's data erased from the databases used for "direct marketing" (in essence, profiled marketing) unless the data serves other legitimate purposes, such the performance of a contract (and even then, the data may no longer be used for marketing).

There is also no provision for data portability in Israeli law. However, PPA guidelines require controllers to provide data subject access rights in electronic form where possible.

In addition to defamation laws, the Israeli parliament is debating a bill designed to allow the removal (or, where the illegal content is out of reach, blocking by Internet Service Providers (ISPs) and search engines) of certain illegal material. As currently defined, material may ordered to be removed if its publication is illegal and likely to substantially endanger the safety of a person or the public, or the security of the state.

The PPA published a draft guideline which, if officially published, would require greater transparency of controllers processing data about minors, and would require parental consent for processing the data of minors under the age of 14. In addition, rarely enforced regulations promulgated under the Consumer Protection Law, 1981, prohibit businesses from collecting and using any personal data from minors, even on adults, without parental consent.

2.3 Online Marketing

Unsolicited commercial communications by email, text messages, "robo-calls" and facsimile are regulated by the Communications Law (Telecommunications and Broadcasts), 1982, irrespective of whether such communications are based on profiling of personal data (in which case they are also subject to the PPL), or not.

The Communications Law covers "advertisements" which are messages whose purpose is to encourage the purchase of a product or service or otherwise spending money, communicated in a commercial manner. The Communications Law permits sending covered advertisements only with explicit consent or if the recipient provided his or her contact details as part of a purchase of a product or service, or during negotiation for such purchase, the advertiser notified the recipient that his or her details will be used for advertising, gave the recipient an opportunity to refuse such advertisements, and the advertisement relates to a product or service that is similar to the original product or service provided by the advertiser. Covered advertising must display, in the subject, the word "advertisement". All messages must explain how such communications can be stopped, in a simple manner and using a means of communications similar to that used to disseminate the advertising. The notice rules are somewhat relaxed for SMS' format limitations.

Behavioural Advertising

Behavioural advertising would fall under the PPL's direct marketing rules, which generally apply to any profiled commercial communication. Personal data may be used for targeted marketing if the data was lawfully collected – that is, the data subject is informed of the various uses of his or her information (including marketing) when his or her personal information is collected (if collected from the data subject). Under PPA guidelines, if the targeted marketing is related to the controller's core service (that is, the main purpose for which the data was collected), by the controller, to current customers, then no opt-in consent is required. Explicit, opt-in consent is needed if marketing is targeted at former customers, if it is not directly related to the service for which the information was originally collected, or if data is to be transferred to third parties for their own marketing purposes (such transfers are subject to additional restrictions).

Data subjects have a right to be removed from a database used for direct marketing. In effect, in a database used for both marketing and operations, this means that all data not used for operational purposes should be deleted (unless such data may be retained for other purposes, such as for legal purposes – however, in any event, any processing for direct marketing should stop).

2.4 Workplace Privacy

Consent given by employees is considered "suspect" and will therefore not be accepted automatically as a freely given consent. The PPA has issued guidelines on the use of security cameras in the workplace which make clear that employees have a reasonable expectation of privacy in the workplace. Hidden cameras should be avoided, and employees should be informed of the location and purpose of cameras.

The National Labour Tribunal found that employees are entitled to some privacy in their work email communications, especially if some private use of email is allowed or tolerated. Employees should be notified of any monitoring of their email communications. Employers must not access email communications that are prima facie private without consent or a court order.

The principles set down by the National Labour Tribunal were incorporated into a collective bargaining agreement that cover most employees in Israel.

2.5 Enforcement and Litigation

Criminal convictions must meet the normal standard of "beyond reasonable doubt". Administrative proceedings are required to meet a much lower standard, that of administrative reasonableness, fairness, and proportionality. Private (civil), administrative and criminal enforcement are all available for breaches of privacy. Criminal offences carry a penalty of up to five years' imprisonment, but criminal enforcement is very rare and generally limited to egregious conduct, such as leaking data from sensitive databases and unauthorised access. Administrative fines are nominal.

A breach of privacy is a tort. The tort of breach of privacy carries statutory damages of up to ILS50,000 (but double this amount if the breach was "with intent to cause harm"). Statutory damages are not applicable in class action cases.

Class Actions
There are several pending class actions relating to the use of location-based data by mobile telephone operators for statistical purposes, a case alleging that Google collected location data without consent, that a navigation app is transferring data to Facebook without consent, and that a bank failed to implement adequate data security measures, resulting in a breach.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Laws empowering law enforcement agencies to access private information generally limit such access both specifically and under general constitutional principles.

Generally speaking, law enforcement access to data requires a court order. The Criminal Procedures Ordinance (Arrest and Search) (New Version), 1969, broadly empowers courts to issue orders to produce data (including content) if such data is needed for investigative purposes or legal proceedings. An order permitting a search in computers must specifically authorise this action and specify the conditions of the search and its purposes.

Under the Criminal Procedures Law (Enforcement Powers – Data Communications), 2007, which applies only to data held by licensed telecommunications operators, certain law enforcement agencies are entitled to access communications data (but not content) with a court order, except in exigent circumstances in relation to serious crimes (ie, those punishable by more than three years of imprisonment) or risk to life, in which case a subpoena by certain police officers suffices.

Under the Communications Law (Telecommunications and Broadcasting), 1982, the Prime Minister may – and often does – order licensed telecommunications operators to cooperate with the GSS (the Security Agency), Mossad (the Intelligence Agency), the national police force, the Israel Defence Force and the Prison Service in such matters as installation of equipment, giving access to data, etc, to exercise their legal powers.

Section 23B of the PPA allows law enforcement agencies to receive and transmit information between them if necessary in order to exercise their legal powers.

3.2 Laws and Standards for Access to Data for National Security Purposes

The General Security Service Law, 2002, empowers the GSS to access communications handled by licensed telecommunications operators. Powers – including sweeping data requests from ISPs (which exclude some content that is subject to wiretapping legislation which also applies to computer communications) – are subject to approval by the Prime Minister and to periodic reviews by the head of the service. Wiretapping (including of computer communications) requires a court order, although the Prime Minister or Minister of Defence may authorise warrantless wiretapping for purposes of national security for periods of up to three months.

3.3 Invoking a Foreign Government

Compliance with law is generally recognised as a legitimate basis to collect and disclose information, and nothing in the PPL suggest this is limited to Israeli law (the PPL merely mentions "a legal obligation" to provide data). However, as far as compliance with law as a basis for transfer abroad is concerned, that is limited to transfers that are "required under Israeli law" only.

3.4 Key Privacy Issues, Conflicts and Public Debates

Two key concerns are often mentioned. The first is the increasing government access to communications data under the Criminal Procedures Law (Enforcement Powers – Data Communications), 2007; see **3.1 Laws and Standards for Access to Data for Serious Crime**, above. The second is the national biometric database, which contains biometric data on all holders of newly issued national ID cards and passports. As of 2017, only biometric identification documents are issued.

4. International Considerations

4.1 Restrictions on International Data Issues

Generally, the Protection of Privacy Regulations (Exports of Data to Databases out of the Jurisdiction), 2001, allow exports of personal data only to jurisdictions whose laws give personal information the same level of protection available in Israel.

Key exceptions to the broad data export limitation include:

- exports with the informed, freely given consent of the data subject;
- exports to a processor who has agreed to comply with Israeli laws governing the processing of personal information; and
- exports to a jurisdiction which is a party to the European Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.

Another important exception concerns exports to a jurisdiction "which receives information from members of the

European Community, following the same terms for reception". Among other things, this exception allowed data exports to US companies that complied with the Safe Harbour framework. Although Israel is not a Member State of the EU, the CJEU Schrems decision dramatically affects data exports from Israel to the USA. The PPA has published a guidance note that regulation 2(8)(2) can no longer be relied upon for exports to the USA, and data controllers who wish to export data to entities in the USA "must consider whether they can base such exports on other exceptions". The PPA said it is considering whether Privacy Shield is applicable.

While the PPA's guidance suggests regulation 2(8)(2) no longer applies to any data exports to the USA, this is not necessarily so. For example, a US entity that complies with the so-called Model Clauses could arguable import personal data from Israel "following the same terms for reception" of personal data "from members of the European Community". This theory is untested, however; the fate of the Model Clauses in the EU remains to be seen.

For all exports, the transferor must obtain a written undertaking from the recipient that the recipient will implement adequate measures to protect privacy, and that the personal information will not be transferred onward to any other person or jurisdiction. Therefore, controllers should agree to sub-processors in advance, and sub-processors must be subject to similar contractual obligations that apply to the original processor. However, some interpret this provision as limiting any use of sub-processors.

When a database is registered, the application must specify whether data is exported, where, and for what purposes. As it is the duty of the controller to keep registration current, any changes in export practices must also be notified.

None of the export restrictions mentioned above apply to transfers under the International Legal Assistance Law, 1998 (ie, MLATs). Outside the MLAT framework, the normal restrictions apply. As far as compliance with law as a basis for transfer, that is limited to transfers that are "required under Israeli law" only.

4.2 Mechanisms That Apply to International Data Transfers

See above, **4.1 Restrictions on International Data Issues**.

4.3 Data Localisation Requirements

An internal government procedure requires certain key government processing activities to remain in-country.

4.4 Sharing Technical Details

The use of encryption requires a licence from the Ministry of Defence, so information about encryption algorithms may be requested as part of the licensing process, although a detailed review process is generally reserved for non-commercial encryption.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Big data processing is the subject of several class actions which are partly based on the argument that mere anonymisation requires specific consent, when it is not part of the original purpose of processing. The PPA recently reviewed subscription TV set-top boxes as part of its growing interest in IoT. Key issues identified were consent (including of children), outsourcing, data exports, purpose limitation, and data security.

The processing of biometric data (including photographs, except when used to identify employees – eg, in name tags) elevates the level of security required under the new data security regulations.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

The new data security regulations promulgated pursuant to the PPL set four levels of protection for data processing, from the lowest for data processing by individuals, to the highest, where the data is sensitive and there is a large number of users. The two highest levels are subject to a new breach notification requirement.

In common with the PPL, many provisions of the new data security regulations are directly applicable to processors. The regulations require the mapping of data collection and processing processes, an indication of the purpose, the types of data, and whether there are transfers of data out of Israel. Importantly, the regulations require annual assessment of retention practices. Although they do not explicitly require that excessive data be destroyed, this is implied.

A data security procedure must be drawn up, covering such matters as physical, environmental and logical security requirements, including access restrictions, auditing, risk mitigation, authentication, employee screening, penetration testing and breach mitigation and handling procedures. All security events must be documented and reviewed. The regulations also cover outsourcing, backup and recovery processes, and audits.

The PPA may exempt certain entities from compliance with parts of the regulation – for example, if such entities are subject to sectoral regulations. So far, the PPA has exempted

banks from some provisions, considering the rigorous data security requirements of the Supervisor of Banks.

The PPL and the regulations promulgated pursuant to it apply to personal information and, accordingly, to data security of personal information only.

The Law for the Regulation of Security in Public Entities, 1998, grants the General Security Service ("GSS") (with respect to telecommunications operators) and the National Cyber Security Authority (with respect to certain other structurally important entities, including private companies), the right to instruct covered entities to take such security and cybersecurity defensive action as the regulators may order. The National Cyber Security Authority also operates the national CERT, has educational programmes, and has published comprehensive cyber-defence methodology guidelines.

Cybersecurity in regulated industries is also handled by their sectoral regulators. For example, banks are subject to the Supervisor of Banks' Proper Conduct of Banking Business Directive on Information Technology Management (Directive 357), on Cyber Defence Management (Directive 361) and on Cloud Computing (Directive 362), all of which contain provisions relevant to cybersecurity. Similar directives were issued by the Authority for Money Markets, Insurance and Savings, which regulates financial institutions, including insurance companies.

The National Cyber Security Authority published a comprehensive cyber-defence methodology. It is generally non-binding, but the Israel Securities Authority has ordered entities subject to its jurisdiction to comply with it.

6.2 Key Frameworks

The new data security regulation allows the PPA to recognise standards or other guidelines as providing an equivalent level of protection as required by the regulation. None such has been recognised to date.

6.3 Legal Requirements

The new data security regulations will require, as of May 2018, any processor of personal data (except by an individual, or a firm whose sole shareholder is an individual) to put in place a detailed data security procedure, which must be reviewed annually, and which should contain an incident response plan. Sectoral regulators have required such plans for some time.

The PPL only requires the appointment of a data security officer of processors serving more than five controllers, public entities, banks, insurance companies and credit-rating agencies, although if an entity appointed a data security officer voluntarily, he or she is also covered by the new data protection regulation.

The Bank of Israel must appoint a privacy officer to advise on privacy issues in relation to the central credit rating database that the Bank of Israel oversees. Involvement of the board of directors is only required in banks and financial institutions, and only with respect of data security and cyber-defence.

Databases subject to the highest protection level in the new data security regulations must undergo a risk assessment and penetration testing at least once every 18 months. Banks and financial institutions are subject to additional requirements set by their regulators.

In addition, the new data security regulations require controllers to survey risks, which include internal risks. These regulations also require controllers to train users about the PPL, and the controller's data security procedures before they are given access to data. Databases subject to the two highest protection levels require at least bi-annual training.

6.4 Key Multinational Relationships

In January 2011, the European Commission adopted a decision on the adequate protection of personal data by Israel with regard to automated processing of personal data (notified under document C(2011) 332). In its latest Annual Report, published in November 2017, the PPA said it will aim to close any gaps between Israeli law and the GDPR.

The PPA is a member of the International Conference of Data Protection and Privacy Commissioners, Global Privacy Enforcement Network (GPEN), OECD Working Party on Security and Privacy in the Digital Economy, the International Working Group on Telecommunications, and the Digital Clearing House.

6.5 Key Affirmative Security Requirements

Banks, financial institutions and telecoms operators, among others, must report significant incidents to their respective regulators. The Law for the Regulation of Security in Public Entities, 1998, empowers the GSS or the National Cyber Authority, as applicable, to set additional requirements, which are generally classified.

6.6 Data Breach Reporting and Notification

Breach notification arises upon a "serious security incident". Only security incidents in databases classified as subject to medium or high security levels are considered "serious".

In a database subject to the high security level, an incident is "serious" if there was an unauthorised use of the data, or a breach of data integrity. In a database subject to the medium security level, an incident is "serious" if there was an unau-

thorised use of the data, or a breach of data integrity, with respect to a "substantial" portion of the database.

A database is subject to medium security if it is used for direct marketing or for other transfers to third parties (data brokers), or contains certain types of sensitive data, including data on health, personal life, genetic data, political opinions or religious beliefs, criminal background, biometric data (except facial photos used solely for identification of employees), economic situation and consumer habits. If the database has more than 100 users (in any capacity, from users to administrators) or contains data about more than 100,000 data subjects, it becomes subject to the high security level.

Banks, financial institutions and telecoms operators, among others, must report significant incidents to their respective regulator. The Law for the Regulation of Security in Public Entities, 1998, empowers the GSS or the National Cyber Security Authority, as applicable, to set additional requirements, which are generally classified.

After reporting a serious security incident to the PPA, it may order notification to affected data subjects after consultation with the head of the National Cyber Security Authority, if such data subjects may be harmed by the incident.

AYR - Amar Reiter Jeanne Shochatovitch & Co.
Champion Tower
Levels 39-40
30 Sheshet HaYamim Rd.
Bnei Brak 5120261 Israel

Tel: +972.3.6019601
Fax: +972.3.6019602
Email: eyals@ayr.co.il
Web: www.ayr.co.il

6.7 Cyberthreat Information Sharing Arrangements

In July 2017 the Israel Antitrust Authority published a position paper about cyber-threat information exchange through the national CERT. According to the position paper, such information exchange is permitted, even among competitors, provided the information does not also relate to the firms' commercial activities.

6.8 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

The PPA issued several decisions finding breaches in such matters as failing to address known security vulnerabilities (leading to data breach), misuse of the national population registry, and use of publicly available information for direct marketing. The PPA criminally pursued a serious incident involving the national population registry. A minor data breach involving a bank resulted in a class action claim that is currently pending.