May 2022

Israel: Cybersecurity

Quardia / Essentials collection / istockphoto.com

1. GOVERNING TEXTS

1.1. Legislation

Israel's cybersecurity related legislation comprises several laws and regulations covering various aspects of the cybersecurity sphere, as further detailed below.

The primary Israeli law governing data protection is the Protection of Privacy Law, 5741-1981 ('the Law'), enacted in 1981. The Law applies to any entity that manages or possesses a 'database', including both private and public entities. A 'database' is defined in the Law as a collection of personal data maintained in electronic form, excluding:

- a collection of personal data maintained for personal use rather than for business purposes; and

- a collection that includes only names, addresses, and contact information, and which by itself does not create any characterisation that invades the privacy of the persons whose information is included therein.

The Law requires certain databases to be registered with the Registrar of Databases, which operates within the Privacy Protection Authority ('PPA'), as further detailed in section 3.3. In addition, according to the Law, certain organisations are required to appoint an information security officer. The Protection Of Privacy Regulations (Data Security) 5777-2017 ('the Data Security Regulations') is an omnibus set of rules promulgated by the Israeli Parliament ('Knesset') in March 2017, effective as of May 2018. These regulations require Israeli organisations, companies, and public agencies that own, manage, or maintain a database containing personal data, to implement prescriptive security measures, with the objective to prevent cybersecurity incidents. These include, for example, physical security measures, access control measures, cyber risk assessments, and periodic penetration test.

On 5 January 2022, the Israeli Government ('the Government') published a new Privacy Protection Bill (Amendment No. 14), 5722-2022 ('Amendment 14'), amending the Protection of Privacy Law, 5741-1981 (only available in Hebrew here). As of May 2022, the Amendment 14 is in the first stages of legislation in the Knesset, after it was approved in the first reading. If enacted, this would be the most comprehensive amendment to the Law since 1996. Amendment 14 seeks to amend the definitions of the Law's key terms, thereby expanding the scope of the Law, and to downscale the antiquated obligation to register database. These are two significant and far-reaching amendments. Amendment 14 also seeks to grant draconian enforcement powers to the PPA. These amendments are bound to impact every organisation in Israel.

The Israeli Computers Law, 5755-1995 (only available in Hebrew here) ('the Computers Law') is mostly a penal statute, specifying certain computer-related conduct comprising criminal offenses punishable by imprisonment:

- Section 2 of the Computers Law penalises any intermeddling with the ordinary operation of a computer or with its use (i.e. denial of service attacks).
- Section 4 of the Computers Law penalises unlawful intrusion into computer material (i.e. hacking and unauthorised access).
- Section 5 of the Computers Law penalises intrusion into computer material committed in furtherance of another predicate felony.
- Section 6 of the Computers Law penalises the programming of computer software, or its modification, made for the purpose of unlawfully performing any one of six enumerated acts. These acts comprise, among others, interfering with the ordinary operation of a computer, impacting the integrity of computerised content, facilitating unlawful intrusion into computers or invading a person's privacy. Section 6 of the Computers Law also deals with the act of trafficking in or installing such computer programs.

The Regulation of Security in Public Bodies Law, 5758-1998 (only available in Hebrew here) ('the Security of Public Bodies Law'), authorises the Israeli Security Agency ('ISA') and the National Cyber Directorate ('NCD') to issue binding directives to organisations operating critical infrastructures on matters related to information security and cybersecurity, and inspect such organisations' compliance with those directives. Organisations subject to this regime include telecommunications and internet providers, transportation carriers, the Tel Aviv Stock Exchange ('the Stock Exchange'), the Israeli internet Association ('the Israeli ccTLD Registry'), utility companies, and others.

The Defense Export Control Law, 5766-2007, and its regulations, govern the State's control of the export of defence equipment, the transfer of defence know-how, and the offering of defence-related services, for reasons of national security, foreign relations, international obligations, and other vital interests of the State of Israel.

In 2018, the Government published a proposal for a Cyber Defense and National Cyber Directorate Bill ('the Bill'). The Bill proposes to grant far-reaching and unprecedented powers to the NCD, such as compelling organisations to produce any information or document required to handle cyber-attacks and authority to issue instructions to organisations, including instructions to carry out acts on the organisation's computerised material, for the purpose of handling cyberattacks. Despite several drafts circulated since the first publication, as of May 2022, the bill had not yet been enacted into law.

1.2. Regulatory authority

The PPA within the Israeli Ministry of Justice ('MoJ') (formerly known as the Israeli Law, Information and Technology Authority), is the Israeli privacy regulator. The PPA is responsible for enforcing the Law and has investigative powers in relation to violations of the Law and the Data Security Regulations, including on issues relating to the cybersecurity of databases containing personal data.

Banks and credit card companies are subject to the cybersecurity requirements laid down by the Banking Supervision Department ('the Supervision Department') within the Bank of Israel ('BoI'). The Supervision Department is responsible, among other issues, for enforcing the data breach rules relating to cybersecurity incidents for banks and credit card companies.

The Capital Market, Insurance and Savings Authority ('the Capital Market Authority') operates within the Israeli Ministry of Finance ('MoF').

The Capital Market Authority is responsible for enforcing the data breach rules relating to cybersecurity incidents at these organisations.

In 2015, the Government established a National Cybersecurity Authority ('the Cybersecurity Authority'), and in 2018 merged that same with the National Cyber headquarters who was tasked with national capabilities in cyberspace. The resulting merger is the National Cybersecurity Directorate. The executive decision on the establishment of the Cybersecurity Authority prescribes its primary roles as follows:

- to manage, control, and carry out the overall, nationwide operational efforts to protect cyberspace;
- to operate a national, economy-wide Computer Emergency Response Team;
- to strengthen and reinforce the economy's resilience, through preparatory measures and regularisation;
- to design and implement a national cyber-defence doctrine; and
- to perform such duties as the Prime Minister may determine, consistent with the Cybersecurity Authority's designated mission.

1.3. Regulatory authority guidance

Over the past several years, the PPA has issued guidance to various market sectors concerning compliance with the Law. The guidelines reflect the Israeli privacy regulator's position on interpretation of the Law and clarify the PPA's position on various matters.

In particular, the following guidelines have been issued by the PPA:

- a statement regarding the transfer of personal information from Israel to the United States following the ruling of the Court of Justice of the European Union ('CJEU') in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) ('the Schrems II Case') (only available in Hebrew here);
- guidelines regarding the appointment of a Chief Privacy Officer in organisations, and their functions and responsibilities (only available in Hebrew here);
- Guidance on Student Privacy in Educational Institutions in the Digital Age (only available in Hebrew here);
- guidance on the use of CCTV and storage of CCTV footage (only available in Hebrew here);
- guidelines covering use of CCTV in workplaces (only available in Hebrew here);
- guidance on the outsourcing of data processing operations (only available in Hebrew here);
- guidance on requirements for user authentication when providing remote access to personal data (only available in Hebrew here);
- guidance on restrictions of financial institutions' use of information concerning attachment orders for sequestration issued against their clients' financial property (only available in Hebrew here);
- Guideline No. 2/2012 on Applicability of the Provisions of the Law on Screening Procedures for Admissions to Work and Sorting Institutes Activities (only available in Hebrew here);

- Clarification for Sorting Institutes Regarding the Right of Reference for Examiners for Work (only available in Hebrew here);
- guidance on the allocation of responsibility for databases between health insurers and primary health care providers (only available in Hebrew here);
- guidance on direct mailing and direct mailing services (only available in Hebrew here);
- guidance on collection of data from minors;
- draft guidance concerning privacy in the workplace (only available in Hebrew here);
- draft guidelines on the transfer and sharing of personal information in the context of mergers or acquisitions (only available in Hebrew here);
- guidance on the use of drones (only available in Hebrew here);
- guidance for municipalities on privacy aspects of smart cities (only available in Hebrew here);
- recommendations on data protection issues relating to the use of drones (only available in Hebrew here);
- clarifications on political parties' responsibility to protect personal data when using third-party applications during an election campaign (only available in Hebrew here);
- review of digital monitoring tools used around the globe amid the Coronavirus pandemic and proposed operational models for such tools (only available in Hebrew here);
- guidance on workplace privacy amid the Coronavirus pandemic (only available in Hebrew here; summary of an earlier version of this guidance, in English, is available here);
- general Q&As on privacy amid the coronavirus pandemic (only available in Hebrew here);
- guidance on schoolchildren privacy amid the Coronavirus pandemic (only available in Hebrew here);
- background review of the data protection impact of social ranking solutions (only available in Hebrew here);
- draft guidance on data minimisation (only available in Hebrew here);
- guidance on the protection of privacy in epidemiological investigations (only available in Hebrew here);
- guidance on the protection of privacy in public transportation in a digital environment (only available in Hebrew here);
- guidance on privacy aspects of payment applications and validation of use of public transport services (only available in Hebrew here);
- guidance on privacy in advanced means of payment for transferring money and payments at businesses (only available in Hebrew here);
- guidance on the appointment of a Chief Privacy Officers in organisations and their functions (only available in Hebrew here); and
- draft guidance on students' privacy in educational institutions (only available in Hebrew here).

In addition, the following guidelines have been issued by the Supervision Department:

- circular on cyber-defence management at banking corporations and credit card companies (only available to download in Hebrew here) ('the Circular on Cyber-defence Management');
- guidelines to banks and credit card companies regarding their use of cloud computing services (only available to download in Hebrew here) ('the Guidelines on Cloud Computing');
- circular requiring banks and credit card companies to manage and monitor the cybersecurity risks associated with service providers who are involved in processing sensitive business or personal data (only available to download in Hebrew here) ('the Circular on Cybersecurity Risks');
- circular on management of operational risks (only available in Hebrew here) ('the Circular on Operational Risks');
- circular on business continuity management (only available to download in Hebrew here) ('the Circular on Business Continuity Management'); and
- circular on digital banking services (only available to download in Hebrew here) ('the Circular on Digital Banking Services').

One of the Circular on Cyber-defence Management's operative sections requires that banking corporations and credit card companies appoint a cyber-defence manager and define the board of directors' responsibilities in this realm. The Circular on Cyber-Defence Management also specifies that banking corporations are expected to regularly identify and evaluate cyberthreats and risks and details the requirements for an effective process for doing so. Furthermore, the Circular on Cyber-defence Management points out that banking corporations ought to continuously examine the effectiveness of the various cyber-defence controls that they have established, using tools such as vulnerability reviews and controlled-intrusion tests.

The Guidelines on Cloud Computing specify how banks and credit card companies should manage the risks involved in using cloud services for data processing. The Guidelines on Cloud Computing provide, among other things, that banks and credit card companies may only use cloud services if the data is stored and processed in Israel, or through a cloud service provider that adequately protects personal data pursuant to EU data protection legislation. In May 2022, a draft amendment of the Guidelines on Cloud Computing was published which aims to permit banks and credit card companies to move their core systems to cloud computing and carry out ongoing material activities in the cloud.

The Circular on Cybersecurity Risks requires banking corporations to audit the service providers they use, impose data security obligations on the providers, and ensure that the providers comply with those obligations.

The Circular on Operational Risks requires banking corporations, (in addition to the requirements in the Guidelines on Cloud Computing), to identify, monitor, and manage technological risks by:

- implementing the same principle of managing operational risks by corporate governance and monitoring to ensure that the technology risks are aligned with the banking corporation's agenda;
- establishing policies and procedures for risk assessment; and
- auditing and monitoring procedures to mitigate technology risks.

The Circular on Business Continuity Management requires banking corporations to implement procedures for data backups and recovery and a data breach response and recovery policy, as well as procedures for remote access to the banking corporation's systems.

The Circular on Digital Banking Services requires banking corporations to perform an initial and periodic assessment of the risk for digital banking solutions used; and implement monitoring measures to mitigate the risks for customers such as monitoring of irregular activities, increasing customer awareness, and implementing proper procedures for customer identification. In addition, the Circular on Digital Banking Services instructs banks on the manner in which they can remotely identify and authenticate their clients' identities.

Moreover, the Capital Market Authority has issued the following guidelines:

- circular on Cyber Risk Management at Institutional Entities (only available in Hebrew here) ('the Circular on Cyber Risk Management'); and
- institutional entities circular on 'Instructions for Information Security Risk Management at Institutional Entities' (only available in Hebrew here) ('the Circular on Information security Risk Management').

The Circular on Cyber Risk Management, which entered into force on April 2017, applies to all institutional investors in Israel. Its declared objective is to provide 'principles regarding the protection of an institutional entity's assets for the purpose of ensuring the rights of stakeholders and policyholders, by safeguarding the confidentiality, integrity and availability of information assets, information systems, business processes and the proper functioning of the entity.'

According to the Circular on Cyber Risk Management, cybersecurity risk management includes actions for preventing, neutralising, investigating, and addressing cybersecurity threats and incidents to mitigate their effects and damage before, during, and after they occur. The Circular on Cyber Risk Management repealed the Circular on Information security Risk Management. The Capital Market Authority's cybersecurity requirements include, for instance, the obligation to approve, at least once a year, a corporate policy on cybersecurity risk management. Regulated entities must appoint a chief cybersecurity officer and conduct an annual

assessment of the suitability of defensive measures to the organisation's overall cybersecurity risks. The Capital Market Authority's guidelines also require financial institutions and insurance companies to run a security operation centre tasked with monitoring, detecting, and mitigating cybersecurity risks.

2. SCOPE OF APPLICATION

Personal scope

The Law and regulations apply to any natural person or legal entity that manages or possesses a database that includes 'Information', as defined below in section 3, including both private and public entities.

Territorial and extraterritorial scope

The Law, the regulations promulgated thereunder, Israeli case law, and the PPA's guidelines do not clarify whether the Law applies extraterritorially. Under statutory canons of interpretation, there is a rebuttable presumption that a law enacted by the Israeli parliament extends only territorially within Israel, i.e. to persons and companies located in Israel. There are plenty of other Israeli statutes that have express extraterritorial provisions; however, the Law and the regulations promulgated thereunder do not have such express extraterritorial provisions, and no provision of the Law or the regulations promulgated thereunder spell out that it applies to database owners outside Israel. Section 9(b)(1) of the Law provides that an application to register a database with the PPA must state 'the names of the owner of the database, the possessor of the database and the manager of the database, and their addresses in Israel', alluding to a possible statutory intent that the Law only extend to database owners located in Israel.

Material scope

The Law applies to any type of processing activity performed on 'Information' (personal information). 'Information' is any data concerning a person's personality, familial status, intimate affairs, health or medical condition, economic status, opinions, or beliefs.

3. DEFINITIONS

Information: Any data concerning a person's personality, familial status, intimate affairs, health or medical condition, economic status, opinions, or beliefs.

Database: A set of 'Information' as defined above, stored by magnetic or optic means, and intended for computerised processing, excluding:

- a set of Information for personal use that is not for business purposes; or
- a set that includes only the name, address, and contact information, which in itself does not characterise the data subject in a way that would invade their privacy, provided that the owner of that the set

or the corporate body under their control does not own an additional set.

Database holder: A person who permanently possesses a database and is permitted to use it. This definition is aimed at those who provide processing services for the benefit of the database owner.

Information security: Protection of the integrity of information, or protection of information from being exposed, used, or copied, without lawful permission.

Information Security Officer: A person with appropriate training, who is:

- answerable to the database owner or anyone acting on their behalf;
- responsible for the database's information security, including the establishment of data security procedures and their implementation; and
- performing any other security tasks assigned by the database owner.

Data security procedure: A document summarising all information security obligations regarding a database, including:

- instructions concerning physical protection of the database systems and their surroundings;
- access authorisations to the database and the database systems;
- description of the means intended to protect the database systems and the manner of their operation;
- instructions to authorised users of the database and database systems, regarding the protection of data stored in the database;
- risks to which the data in the database is exposed in the course of the ongoing activities;
- manner of dealing with information security incidents; and
- instructions concerning the management and usage of portable devices.

Data subject: the person about whom information is stored in the database.

Database subject to high security level: A database administered primarily for making its information available to other parties; or a database that contains sensitive information (namely, information about a person's intimate affairs, medical, physical or mental health information, genetic or biometric data, political opinions, faith or religious beliefs, criminal history, telecom metadata, economic status, financial assets, debts and solvency, or consumption habits information indicative of one of the foregoing), provided that the database contains the information of at least 100,000 data subjects or to which more than 100 people have access privileges.

Database subject to medium security level: A database to which more than ten people have access privileges, provided that the Database:

- is maintained by a public agency;
- contains special categories of data unless the data subjects are only the employees or suppliers of the database owner; or
- is primarily administered for making its information available to other parties (e.g. direct marketing services).

Severe data security incident: Any of the following:

- in a database subject to high security level - an incident involving the use of data from the database without authorisation or in excess of authorisation, or where the integrity of the information was compromised; or
- in a database subject to medium security level – an incident involving the use of a material portion of the database without authorisation or in excess of authorisation, or where the integrity of a material portion of the database was compromised.

In July 2020, the MoJ published a draft bill proposing to amend some of the provisions of the Law, including some of its basic definitions. For example, the definition of 'Information' is suggested to be amended to follow the path of the General Data Protection Regulation (Regulation (EU) (2016/679) ('GDPR'). The definition of a database 'Holder' is suggested to be amended to include anyone who has access to a database for the provision of services to the database owner, similar to the definition of a 'processor' under the GDPR. The draft bill also suggests to adopt the GDPR's definition for 'processing' which would include disclosure, transfer, storage, review, organisation, rectification, and completion of personal data.

In addition, in May 2021 the PPA published an opinion on the definition of the term 'Information' (only available in Hebrew here), which was highly criticised for trying to re-write the statute's definitions. In its opinion, the PPA argues that telecom metadata, geolocation information and email address are all examples of 'Information' because they are personally identifiable, even though the antiquated statutory definition for the term does not included these data elements.

4. IMPLEMENTATION OF AN INFORMATION MANAGEMENT SYSTEM/FRAMEWORK

4.1. Cybersecurity training and awareness

The Data Security Regulations require that the database owner conduct training sessions for authorised users, before they gain first-time access to a database or before changing the scope of a their authorisation.

The training should regard to the authorised users' obligations under the Law and the Regulations.

In addition, in a database subject to medium or high security levels, the database owner is required, once every two years, to conduct training to authorised users regarding the database definitions document, data security procedure, and the requirements of the Law and the Data Security Regulations, as is relevant for their roles. This training should also be held for newly authorised users as soon as possible after they are onboarded.

4.2. Cybersecurity risk assessments

The Data Security Regulations require that the owner of a database subject to high security level conduct an information security risk assessment every 18 months. In addition, the owner of a database subject to high security level is required to conduct, at least once every 18 months, penetration tests to the database systems, in order to test their vulnerability.

4.3. Vendor management

The Data Security Regulations and the guidance on the outsourcing of data processing operations set out the guidelines for the engagement of a database owner with any vendor who is an external service provider.

The database owner is required to assess, prior to engaging with the vendor, the risks involved in the engagement.

If the database owner decides to enter into an agreement with the vendor, such agreement must include the following information security provisions:

- a specification of the data the vendor may process and the permitted purposes for processing;
- a specification of the database systems that the vendor may access;
- the type of processing or activities the vendor may perform;
- the agreement duration, the manner of returning the data to the database owner or its disposal, and the manner of reporting accordingly to the database controller;
- a specification of the implementation of the vendor's data security obligations, and additional data security instructions determined by the database owner, if any;
- the vendor's duty to bind its authorised users to protect the information's confidentiality, to use the data only according to the agreement, and to implement appropriate data security measures;
- the vendor's duty to notify the database owner in case of a security incident, and report, at least annually, on how it implements its information security obligations; and
- where a database owner authorised the vendor to provide the service through another subcontractor, the agreement between the vendor and subcontractor must flow-down all of the above matters.

The obligations set out in the agreement with the vendor shall also be expressly mentioned in the data security procedure.

In addition, the database owner is required to take measures to monitor and supervise the vendor's compliance with the provisions of the agreement and the Data Security Regulations.

4.4. Accountability/record keeping

Periodic audits

The Data Security Regulations require that the owner of a database subject to medium or high security levels conduct an internal or external audit at least once every two years.

In the audit report, the auditor will report on the owner's adherence to the data security procedure and to the Regulations, identify shortcomings and recommend the necessary measures to remedy the situation. The database owner will review the audit reports and assess the need to update the database definitions document or the data security procedure accordingly.

Documentation of security incidents

The Data Security Regulations require that a database owner document every event that raises concerns of a breach of the database's integrity, unauthorised use thereof, or deviation from authorisation. The documentation should be based, to the greatest extent possible, on automated records.

The database owner is also required to establish instructions for handling different security incidents, according to the security incident's severity and the information's sensitivity level, including all necessary measures to be immediately taken at the event of a security incident.

In addition, the owner of a database subject to the medium security level is required to hold a discussion regarding data security incidents, at least once a year, and at least quarterly in a database subject to high security level. These owners also are required to assess the need to update the data security procedure.

In case of a severe data security incident, the database owner is required to immediately notify the PPA of the incident and the measures taken in response.

5. DATA SECURITY

The Data Security Regulations create four tiers of databases, each subject to an escalating degree of information security requirements and security measures:

- Tier One comprises databases maintained by individuals (e.g. by a sole proprietor or a corporation with a single shareholder, or a database to which no more than three people have access credentials);
- Tier Two comprises databases subject to the basic level of data security (i.e. those that do not fall within any other category, including many employee and human resources ('HR') databases);
- Tier Three comprises databases subject to intermediate data security (i.e. those to which more than ten people have access credentials or whose purpose includes making information available to other parties); and
- Tier Four comprises databases subject to the highest level of data security (i.e. those whose purpose includes making information available to other parties, or database to which either more than 100 people have access credentials or the number of data subjects therein is at least 100,000).

The Data Security Regulations also require organisations to monitor and document any event that raises suspicion of compromised data integrity or unauthorised use of data. In addition, any organisation that is subject to the Data Security Regulations is required to oversee and supervise its vendors' data security compliance on an annual basis.

Additionally, organisations that hold certain 'sensitive information' are required, under the Data Security Regulations, to implement an automated audit mechanism to monitor any attempt to access information systems that contain personal data. Sensitive information covers information regarding an individuals' private affairs, including:

- individuals' behaviour in the private domain;
- health or mental condition;
- political opinions or religious beliefs;
- criminal history;
- telecommunication meta data;
- biometric data;
- financial information regarding individual's assets, debts and economic liabilities; and
- consumption habits of an individual which may be indicative of the above-mentioned types of data.

The Data Security Regulations require anyone who owns, manages, or maintains a database containing personal data to implement the following information security measures:

- draft a database specification document;
- map the database's computer systems;

- maintain physical and environmental security controls;
- develop various data security protocols;
- perform annual reviews of security protocols;
- establish access credentials and manage those credentials on the extent necessary for users to perform their work;
- employ workers in database-related positions only if they have an appropriate level of clearance in relation to the database's degree of sensitivity and provide them training with respect to information security;
- maintain and document information security incidents;
- restrict usage of portable devices;
- segregate the database related systems from other computer systems;
- implement telecommunication security for computer systems connected to the internet;
- engage with data processors only after performing a proper information security due-diligence and bind them to an information security agreement; and
- keep records, documents, and decisions to demonstrate compliance with the regulations.

The Data Security Regulations introduce additional requirements applicable to databases subject to the intermediate level of security. The following requirements apply in addition to the above requirements applicable under the basic level:

- access to the database's physical premises shall be monitored;
- equipment brought in or taken out of the database's physical premises shall also be monitored;
- an extended data security protocol shall cover, among other issues, user authentication measures applicable to the database, backup procedures, access controls and periodic audits;
- users with access privileges shall be authenticated with physical devices such as smart cards;
- a protocol shall be established for means of identification, frequency of password change, and response to errors in access control;
- an automated mechanism for monitoring access to the database shall be established;
- audit logs shall be maintained for at least two years;
- either an internal or external audit shall be performed at least once in 24 months; and
- a backup and recovery plan shall be established.

The Data Security Regulations introduce additional requirements applicable to databases subject to the highest level of security. The following requirements apply in addition to the requirements applicable to those under the basic and intermediate level:

- the database owner shall perform a risk assessment once every 18 months, using a qualified professional;
- the database's computer systems shall be subjected to penetration tests once in 18 months; and

- security incidents shall be reviewed at least once every calendar quarter, and an assessment shall be made of the need to update security protocols.

Israel does not have laws regarding data disposal other than the Data Security Regulations, which require an organisation outsourcing the processing of personal data to contractually obligate the service provider to destroy its copies of the data at the end of the engagement. They also require database owners to annually review their databases for excess data that ought to be discarded.

However, in March 2021, the PPA published a new draft policy on data minimisation. The draft policy is premised on the notion that the collection of personal information that is unnecessary for the purposes for which it has been collected may infringe the data subjects' right of privacy as well as violate applicable law. The draft policy defines 'Excess Information' as 'information about a person that is irrelevant or unnecessary to achieve the purpose for which the information was collected or storage of information that is no longer needed for the purposes determined initially upon the collection of information.'

The draft policy includes several recommendations and guidelines for those that collect personal information, including ensuring that only relevant information is collected; deleting excess information, at the request of the data subject, or when required by law; and compliance with the provisions of the information security regulations, which include an obligation to annually review whether a database has any excess information. The PPA recommends that this review be conducted several times throughout the year, to prevent the extended retention of unnecessary personal data.

According to the draft policy, if a database owner concludes that any of the information it retains is indeed excessive, but neglects to discard that data, the database owner may violate the Data Security Regulations and may be exposed to liability under a civil lawsuit.

6. NOTIFICATION OF CYBERSECURITY INCIDENTS

There are several provisions of Israeli law according to which certain organisations are required to report cybersecurity incidents.

Effective since May 2018, the Data Security Regulations establish a data breach notification requirement in Israel. Under the Data Security Regulations, owners of databases designated within an 'intermediate' or 'high' tier of security are required to notify data breaches to the PPA. The notification obligation for database at the intermediate level of security applies when the breach extends to any material portion of the database, while the notification obligation for database at the high level of security applies to any breach, regardless of its scope or materiality.

The notification must state the measures taken to mitigate the incident. In effect, the notification obligation depends on the database's security level, which in turn depends on the nature of the information stored in the database.

The intermediate level of security applies to public agencies, organisations that hold sensitive information, and data brokers. The high level of security applies to organisations that hold sensitive information and to data brokers, where the database extends to at least 100,000 data subjects or if more than 100 persons have access credentials to the database.

In certain circumstances, the PPA may order the organisation, after consultation with the Head of the NCD, to report the incident to all affected data subjects. Generally, if the breached data is not capable of identifying an individual, then the incident does not need to be reported, since it does not pertain to regulated 'personal data.'

In July 2019, following the first anniversary of the Data Security Regulations, the PPA published a report (only available in Hebrew here) ('the Report') summarising its enforcement activities relating to data breaches. According to the Report, the PPA carried out 146 instances of administrative enforcement action against organisations in relation to data breaches classified as 'severe.' However, the PPA was only notified about 103 of those breaches. The remaining 43 breaches were investigated after the regulator either received complaints about them, or proactively discovered them.

Banks and insurance companies are required to report any cybersecurity incidents and data breaches pursuant to regulatory guidelines by the Supervision Department. Insurance companies and financial institutions are required to report any cybersecurity incidents and data breaches to the Capital Market Authority. Circular 2/2021 on the Use of Cloud computing in the Israeli Healthcare System (only available in Hebrew here) ('Circular 2/2021'), released by the Ministry of Health of Israel ('MoH') requires that medical institutions report any malfunction or unplanned interruptions in essential services, including computer systems. Data security incidents are included in this broad definition.

The ISA also published a position paper emphasising a public company's duties of disclosure both of general cybersecurity risks that a company faces as well as of specific incidents having material adverse effects on the company (only available in Hebrew here).

7. REGISTRATION WITH AUTHORITY

The Law requires that certain databases be registered with the Registrar of Databases, which operates within the PPA. The Law's provisions governing database registration apply to owners of databases that meet any of the following criteria:

- contain data about more than 10,000 persons;

- contain sensitive data;
- contain data about persons where the data was not provided by such persons, was not provided on their behalf, or was not provided with their consent;
- belongs to certain government bodies; and
- is used for direct marketing.

However, the Registrar of Databases may require registration of a database that is otherwise exempt from registration, though this decision is appealable. The database registration system is database-driven and not owner-driven. Hence, if a database owner has several databases, it must register each database separately.

The Law sets forth the basic format of a database registration, requiring that an application to register a database include the following information:

- the identities and addresses of the owner and, if applicable, the holder (i.e. processor) of the data;
- the purposes of the database;
- the types of data contained in the database; and
- the information concerning data transfers abroad and the receipt of data from public bodies.

The database registration regime has been criticised as obsolete by numerous stakeholders, including the Israeli State Comptroller, the public commissions on the protection of privacy, and the PPA itself. A draft bill introduced in July 2020, proposes to revise the compulsory database registration regime, but it does not eliminate the registration duty. Instead, the bill attempts to limit the duty to require registration only for purportedly 'high risk' databases. Effectively, this amendment would preserve the registration requirement only for databases containing the information of 100,000 or more data subjects or more, and which also meeting certain other criteria. To date, no progress has been made with the draft bill.

8. APPOINTMENT OF A SECURITY OFFICER

Under the Law, certain organisations are required to appoint an information security officer responsible for information security of in their databases. These organisations include public entities, service providers who process five or more databases of personal data by commission for other organisations and organisations that are engaged in banking, insurance, and creditworthiness evaluation.

The Security of Public Bodies Law requires certain public organisation listed under Schedules 4 and 5 of the statute to appoint a person responsible for securing essential computer systems in those organisations.

To ensure the data security officer's independence, the Data Security Regulations require that the officer must be directly subordinate to the database manager, or to the manager of the entity that owns or holds the database. The Data Security Regulations prohibit the officer from being in a position that raises a conflict

of interests. Substantively, the Data Security Regulations require the officer to establish data security protocols and an ongoing plan to review compliance with the Data Security Regulations. The officer must present findings of its review to the database manager and to the officer's supervisor.

In January 2022, the PPA published for public comment a draft position paper on the advisability of appointing Chief Privacy Officers ('CPOs') in Israeli organisations (only available in Hebrew here). The paper explains that, although Israeli law does not mandate the appointment of a CPO (other than in the context of the BoI's central database regarding the creditworthiness of Israelis), the PPA views the voluntary appointment of a CPO as a recommended best practice for organisations whose operations involve the processing of personal data. The paper explains that, although the role may be performed by an in-house employee or an outside professional, for organisations whose core activities involve the processing of personal data or that process personal data on a large scale, appointing a senior, in-house executive is highly recommended. The position paper references the comparable CPO regimes under the GDPR, the Brazilian Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019), and the Health Insurance Portability and Accountability Act of 1996 in the US. The paper recommends that the CPO be responsible, among other matters, for the organisation's privacy policy; be involved in the lifecycle of the organisation's data processing activities to ensure that privacy and data protection principles are respected; conduct Data Protection Impact Assessments ('DPIAs'); and handle data subject complaints. The CPO also would be tasked with supervision and monitoring, education, training, and raising awareness. Those appointed should have independence in performing their role, be given adequate budgets and resources, and not be exposed to a potential conflict of interest. According to the position paper, threshold conditions for the appointment of the CPO include having an in-depth knowledge of the laws governing data protection in Israel and sufficient understanding in information technologies and information security.

9. SECTOR-SPECIFIC REQUIREMENTS

Financial Services

The Supervision Department is responsible for, among other issues, enforcing the data breach rules relating to cybersecurity incidents at banks and credit card companies. The Supervision Department has issued various regulatory requirements and guidelines for banks and other financial institutions regarding privacy and cybersecurity such as the ones detailed in section 1.3 above.

In addition, the PPA published a set of guidelines on financial institutions' compliance with the Data Security Regulations. These guidelines indicate which provisions of the Data Security Regulations apply to specific categories of covered entities in the financial sector:

- Guidelines on compliance with the Data Security Regulations for Stock Exchange members who are not banks but are subject to the Stock Exchange Market protocol (only available in Hebrew here);

- Guidelines on compliance with the Data Security Regulations for pension fund management companies and insurance companies subject to the Capital Market Authority (only available in Hebrew here); and
- Guideline on compliance with the Data Security Regulations for financial bodies supervised by the Supervision Department (only available in Hebrew here).

Health

In 2015, the General Manager of the MoH issued a data security circular alerting all medical institutions (clinics, health maintenance organisations, and hospitals) to the importance of cybersecurity and requiring them to certify to ISO 27799 on data security in healthcare related information systems. Certification to this standard is a prerequisite to obtaining or renewing the medical institution's permit. According to this circular, medical institutions may only use service providers who themselves are certified to either ISO 27001 or ISO 27799.

Circular 2/2021 requires medical institutions to report any malfunction or unplanned interruption in essential services, including computer systems. Data security incidents are included in this broad definition. An initial report must be filled within 24 hours. Circular 2/2021 does not set a time frame for full reporting.

The MoH also established a policy for cybersecurity in medical devices, which establishes the cybersecurity requirements for medical devices used in Israel. The guidelines are directed both to manufacturers and importers seeking to market medical devices in Israel, and to healthcare providers using medical devices in the treatment of patients. The guidelines describe a myriad of essential and non-essential cybersecurity controls. Essential controls include access restriction, disaster recovery and resilience, and encryption of wireless transmission. The guidelines also prescribe the cyber risk-management measures that healthcare providers must implement when purchasing, installing, and using medical devices.

In March 2022, the MoH published new draft guidelines regarding the digital management of medical records of patients. In particular, the draft guidelines discuss the scanning process for archiving medical information in a manner that assures the completeness, high-resolution, and availability of the medical information in the digital archive. The guidelines address, among others, the outsourcing of the process of scanning the medical information to private-sector service providers and the restrictions on changing or adding additional information to the original content.

Later that month, the MoH also published Circular 06/2022 for a Basic regulation for cyber protection in the health system in Israel (only available in Hebrew here) ('Circular 06/2022'). Circular 06/2022 derives from the guidelines of the Israeli National Cyber Directorate. It focuses specifically on the cybersecurity measures necessary for the organisation's cyber assets (i.e., personal and medical information stored in the organisation's databases), appropriate cybersecurity risk management, cyber attack preparedness and response, and

lastly, the appointment of cybersecurity supervisors in charge of the different aspects of implementing these principles and duties. Circular 06/2022 requires that health organisations (which are organisations who provide medical services to the public, such as affiliated entities of the MoH, hospitals, HMOs, and pharmacies) establish a corporate cybersecurity governance framework consisting, among others, of a cybersecurity officer appointed by the CEO, a cyber defense manager reporting directly to the cyber protection officer, technological professionals responsible for implementing cyber security principles at the technical level, and a privacy protection officer who more broadly will focus on data protection.

Telecommunications

Telecommunication providers are subject to the Regulation of Security in Public Bodies Law, 5758-1998 ('the Security of Public Bodies Law'), which authorises the ISA and the NCD to issue binding directives to organisations operating critical infrastructures on matters related to information security and cybersecurity, and inspect such organisations' compliance with those directives.

Telecom metadata retained by telecom providers in their course of business is made available, subject to certain judicial procedures, to investigative and intelligence agencies for the purpose of search and rescue, investigating or preventing crime, or seizing property, pursuant to the Criminal Procedure Law (Enforcement Powers – Communication Data), 5767-2007. Moreover, the Prime Minister is granted sweeping statutory powers to order that metadata and non-real time communications (traffic data at rest), which are retained by telecom providers, be surreptitiously made available to the Israeli Security Agency, pursuant to Section 11 of the General Security Service Law, 5762-2002.

Employment

The PPA's 2017 Guidelines on the use of surveillance camera in the workplace (only available in Hebrew here) ('the Workplace Surveillance Guidelines') underscore that employers may use surveillance cameras solely for legitimate purposes relevant to the workplace, and only to the extent required for such purposes. According to the Workplace Surveillance Guidelines, the use of surveillance cameras in the workplace is subject to a duty of reasonableness, proportionality, good faith, and fairness incumbent on the employer. Excessive use of surveillance cameras in the workplace, which is not proportionate, may put the employer at risk of administrative penalties and for criminal and civil liability. The Workplace Surveillance Guidelines require employers using surveillance cameras to take measures such as conducting a DPIA, developing and establishing a privacy policy regarding the manner and scope of using cameras and the purpose of placing them in the workplace, and limiting the use of cameras for specific, legitimate purposes. The Workplace Surveillance Guidelines must be published so that employees are notified. The Workplace Surveillance Guidelines also state that employer should not place cameras in areas in which employees have a reasonable expectation of privacy, such as at restrooms, dressing rooms, or private or shared workplace areas (provided such areas are not accessible to the public).

Israeli legislation does not specifically address the issue of employer monitoring and accessing employees' communications and files for cybersecurity purposes. The Labour Appeal no. 90/08 of *Tali Isakov Inbar v. The State of Israel, the Commissioner for Women Labor Law* (8 February 2011) of the Israeli National Labour Court expounded Israeli privacy law as applied to employers monitoring and accessing employees' communications and files. The decision sets forth the boundaries of permissible access to employee's email communications. The ruling also sets forth a stringent set of prerequisites and conditions for permissible access: such access must be for a legitimate purpose, proportional, and subject to the prior consent of the employees to a workplace privacy policy that transparently discloses the employer's envisioned activities of monitoring employees.

Additionally, in light of the spread of the COVID-19 pandemic the PPA has published a number of guidelines on the protection of privacy in workplaces:

- Guidelines for employers on protection of company data when working remotely (only available in Hebrew here);
- Guidelines for the protection of employees' privacy in workplaces in light of the COVID-19 pandemic (only available in Hebrew here); and
- Guidelines on privacy when entering workplaces and trade-commerce businesses in light of COVID-19 (only available in Hebrew here).

Education

There is no law or regulation specifically governing the privacy of students.

However, in September 2020, the PPA published a paper on the protection of students' privacy in distant education (only available in Hebrew here), during the COVID-19 pandemic, which includes recommendations for students and parents, as well as for educational institutions and local authorities. An updated paper on the same matter was published in January 2022 (only available in Hebrew here).

In addition, in November 2021, the PPA published for public comments draft guidance on students' privacy in educational institutions, for principals and managers of education departments in local authorities (only available in Hebrew here), which provides an overview of the main principles of students' privacy and recommendations for the protection of students' data in the digital age.

Insurance

Insurance companies are required to report to their supervisory authority (the Department of Capital Market, Insurance and Savings at the MoF) of any cybersecurity incidents and data breaches. The report shall be given pursuant to regulatory guidelines by the supervisory authority. In addition, the Law requires

that insurance companies (and other specific organisations) appoint an Information Security Officer, that would be responsible for information security of in their databases.

10. PENALTIES

The PPA is authorised to inspect and search database owners for the purpose of enforcement of the Law. It is also authorised to refuse to register a database if it has reason to believe the database is intended to be used for an illegal purpose. The PPA also has the authority to seek a court order to suspend a database's registration.

Registrar enforcement activities made public recently have dealt with data breaches associated with violations of the statutory duty to employ information security measures, violations of duties regarding direct mailing activities, the duty to report data breach incidents, and use of databases for purposes inconsistent with their registered purposes. These have resulted in declarations of fault and, in certain cases, fines.

The PPA invoked this authority for the first time in late 2020 when it mandated that Shirbit, an Israeli insurance company, proactively inform its data subjects of a significant data breach it had suffered in which a sizeable amount of personal data was compromised. Notably, the Regulations do not prescribe any sanctions for violating the breach notification requirement.

A breach of the Law constitutes a strict liability criminal offence, punishable by one year of imprisonment, and also constitutes a civil tort. For example, under Section 31A(a)(6) of the Law, failure to appoint an information security officer where such is mandated by the Law is a strict liability offence punishable by up to one year in prison. The PPA is also authorised to impose administrative fines instead of criminal prosecution. There are currently no penalties imposable by the PPA for failing to comply with the data breach notification requirement in the Data Security Regulations. A proposed amendment to the Law is aimed to empower the PPA with authority to impose penalties.

The Computers Law specifies the maximum penalties for violation of the criminal offences governed by it. For example:

- intermeddling with the ordinary operation of a computer or interference with its use carries a maximum sentence of three years' imprisonment (Section 2 of the Computers Law);
- unlawful intrusion into computer material carries a maximum sentence of three years' imprisonment (Section 4 of the Computers Law);
- intrusion into computer material committed in furtherance of another predicate felony carries a maximum sentence of five years' imprisonment (Section 5 of the Computers Law); and
- programming or modifying a computer program for the purpose of unlawfully performing any of the acts enumerated in Section 6 of the Computers Law, is punishable by up to three years of imprison-

ment, whereas the act of trafficking in or installing such computer programs is punishable by up to five years' imprisonment.

In relation to civil proceedings, the most prominent civil action that may be brought against a legal entity in relation to a cybersecurity incident is a class action lawsuit in accordance with the Israeli Class Action Law, 5766-2006 (only avaliable in Hebrew here). In order for a court to certify a class action suit, the representative plaintiff must prove that:

- the action raises substantive questions of fact or law common to all members of the putative class that were affected by the incident, and that it is reasonably possible that such questions will be resolved in the class's favour;
- under the circumstances of the case, a class action is the efficient and fair method to dispose of the dispute;
- there are reasonable grounds to assume that the interests of all members of the class will be adequately represented and conducted; and
- there are reasonable grounds to assume that the interest of all members of the group will be represented and conducted in good faith.

In addition, any person or legal entity that suffered damages in relation to a cybersecurity incident may assert an individual civil action based on several applicable laws, for example, invasion of privacy under the Law or negligence in accordance with the Israeli Torts Ordinance.

11. OTHER AREAS OF INTEREST

Since the data breach notification requirement took effect in May 2018, most data security incidents are detected and reported by information security researchers and 'white hat hackers.'

Even under the new data breach notification regime, the negligible number of reported breaches suggest that many go unnotified. According to the PPA's 2019-2020 biennial report (only available in Hebrew here), it carried out 105 instances of administrative enforcement action against organisations in relation to data breaches classified as 'severe', out of 220 data security incident reports it received.

There have been reports of significant black-hat, hacker-driven data breach incidents against public agencies and commercial companies in Israel.

In late 2020, the website and servers of an Israeli insurance carrier were shut down and sensitive information about the company's employees and customers was compromised and offered for sale online. The sensitive information included national ID cards and insurance claims history with medical records. Following the incident, the PPA, for the first time, exercised its power under the Data Security Regulations to compel the insurance carrier to inform its customers of the breach, with recommendations on what they can do to

protect themselves. In November 2021, the Israeli Capital Markets, Insurance and Savings Authority fined the insurance carrier ILS 10.7 million (approx. $3.4M) following a lengthy investigation in which the insurance carrier was found to have mismanaged its cyber risks.

During the general election in Israel, held in March 2020, a data breach was discovered in the an app used by two political parties ahead of the election. The breach compromised the full electoral roll, leading to the unauthorised disclosure of the personal data of more than six million Israeli voters. A PPA investigation into the matter in 2021 concluded that the company that develops and operates the app, and the two political parties that used the app, all violated the Law and the Data Security Regulations in their failure to implement proper data security measures. Although the PPA determined that all three violated the Law, the PPA decided to impose a fine only on the app, and not the two political parties.

Network and information systems

The scope of the Security of Public Bodies Law extends only to the list of organisations expressly enumerated in the statutes' schedules. These are all organisations operating various types of critical infrastructure, including telecom and internet providers, transportation carriers, the Stock Exchange, the Israeli ccTLD Registry, utility companies, and others.

The Data Security Regulations apply to any Israeli organisation, company, and public agency that owns, manages, or maintains a database containing personal data. The Data Security Regulations create four tiers of databases, each subject to an escalating degree of information security requirements and security measures. The triggering criteria for each tier relates to the number of data subjects involved, the data's sensitivity (i.e. special categories of data), and the number of people with access credentials.

The Bill has broad implications for operators of essential infrastructures, systems, or services, including internet and communications service which are considered protectable vital interests. This Bill extends to organisations operating essential infrastructures, systems, or services, and which are susceptible to activities designed to impair the use of a computer or computer material.

Critical information infrastructure operators

The scope of the Security of Public Bodies Law extends only to the list of organisations expressly enumerated in the statute's Schedules 1, 2, 4, and 5.

Operator of essential services

The scope of the Security of Public Bodies Law extends to the list of organisations expressly enumerated in the statute's Schedules 1,2,4, and 5. These include, *inter alia*, communication service providers, chemicals and oil companies, transportation service providers, the BoI, Israel Electric Corporation, and various government bodies., etc.

The Bill would grant the NCD certain authority over any organisation (including the State, local authorities, businesses, and anyone providing public service) that deals in matters of essential public interest, such as:

- state security, public security, or public safety;
- human life;
- state economy;
- essential infrastructure, systems or services, including internet and communications services;
- organisations providing services on a significant scale;
- environmental or public health;
- significant assets of personal data; and
- other interests declared by the Prime Minister.

Digital service providers

There are no specific references to digital service providers as covered entities in Israeli primary or secondary legislation other than the Security of Public Bodies Law which list the Israeli ccTLD Registry and communication providers that are subject to the law, since they operate critical infrastructures.

Haim Ravia Partner, Chair of the Cyber, Privacy, and Copyright Practice Group
hravia@pearlcohen.com
Pearl Cohen Zedek Latzer, Tel Aviv