Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Israel: Law & Pracrice
Haim Ravia and Dotan Hammer
Pearl Cohen Zedek Latzer Baratz

practiceguides.chambers.com

ISRAEL

Law and Practice

Contributed by:
Haim Ravia and Dotan Hammer
Pearl Cohen Zedek Latzer Baratz see p.25

Contents

1. Basic National Regime

1.1 Laws

Israeli laws applicable to cybersecurity include the Israeli Computers Law, the Protection of Privacy Law, the Copyright Law, the Penal Law, the Defense Export Control Law, the Regulation of Security in Public Bodies Law, and the (proposed, but not yet enacted) Cyber Defense Bill. Further details are provided below.

The primary Israeli law governing data protection is the Protection of Privacy Law, 5741-1981 (the PPL), enacted in 1981. The PPL 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 information 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.

"Information" is defined as data on the personality, personal status, intimate affairs, health condition, economic status, vocational qualifications, opinions or beliefs of a person.

The PPL requires that certain databases be formally registered with the Registrar of Databases, as further detailed in **3.3 Legal Requirements and Specific Required Security Practices**.

The Protection of Privacy Regulations (Data Security) 5777-2017 ("Data Security Regulations") are an omnibus set of rules promulgated by the Israeli Parliament (Knesset) in March 2017, and 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, the main objective of which is the prevention of cybersecurity incidents as further described in **3.3 Legal Requirements and Specific Required Security Practices**.

Where there is a violation of the provisions of the PPL or any of the regulations promulgated thereunder, the PPA may take the measures detailed in **1.3 Administration and Enforcement Process**.

The Israeli Computers Law, 5755-1995 is a statute that combines penal and tort provision. It specifies certain computer-related misconduct that comprises criminal offences punishable by imprisonment and in some cases also gives rise to actionable tort claims.

The criminalised acts include:

- interference with the ordinary operation of a computer;
- adversely impacting the integrity of computerised content;
- transmitting or storing fraudulent or misleading computerised information;
- unlawful intrusion into computers or computerised material; and
- developing, offering or distributing software capable of performing any of the above acts, or an act of invasion of privacy or unlawful wiretapping.

The Regulation of Security in Public Bodies Law, 5758-1998, authorises the Israeli Security Agency 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 Israeli Internet Association ("Israeli ccTLD Registry"), utility companies and others.

The Israeli 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 Israeli government published a proposal for a Cyber Defense and National Cyber Directorate Bill. That bill had proposed 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 cyber-attacks. That bill did not materialise into law, but the government reintroduced a revised version of the bill in March 2021. The revised version, now named the Powers for Strengthening Cyber Defense (Provisional Measure) Bill (the "Cyber Defense Bill"), would require that the NCD obtain a court order authorising it to instruct organisations to carry out acts on the organisations' computer systems. The court order would be obtainable only after the NCD has liaised with the organisation, explained the need and the rationale for the acts sought and gave the organisation a reasonable opportunity to address the cyber-attack in question by itself. Stakeholders opposing the new Cyber Defense Bill indicate that, among other issues, the Cyber Defense Bill's arrangements do not properly inter-operate with the existing regulatory landscape in Israel. The Cyber Defense Bill also did not materialise into law.

Data breach notification and incident response requirements are codified in a number of laws and binding directives and vary depending on the organisation that suffered from the incident (bank, company, etc) as further described in **3.3 Legal Requirements and Specific Required Security Practices**.

1.2 Regulators

The Privacy Protection Authority (PPA), within the Israeli Ministry of Justice, is the Israeli privacy regulator. The PPA is responsible for enforcing the PPL and has investigative powers in relation to violations of the PPL and the Data Security Regulations, including on issues relating to the cybersecurity of databases containing personal data. The PPA engages both in proactive investigation of data breaches and in responsive investigation amid complaints. Since the data breach notification obligation took effect in May 2018, most data security incidents are detected and reported by information security researchers and "white hat hackers".

The Banking Supervision Department within the Bank of Israel is responsible for enforcing the data breach rules relating to cybersecurity incidents at banks and credit card companies, among other things. The Supervision Department conducts audits at banks, and initiates investigations upon information provided to it by banking institutions, or on its own accord.

The Capital Markets, Insurance and Savings Authority operates within the Israeli Ministry of Finance. It is responsible for enforcing the data breach rules relating to cybersecurity incidents at insurance companies, financial institutions and financial data service providers. Following the security incident of the insurance company Shirbit (as further explained in **8.2 Significant Audits, Investigations or Penalties**), which was reported to the Capital Markets Authority, the deputy commissioner of the Capital Markets Authority said that, in light of the rapidly evolving cyberthreats, supervision of financial entities will be increased. The Capital Markets Authority also conducts audits at covered entities, and initiates investigations upon information provided to it by covered entities, or on its own accord.

The NCD's activities are specified in **2.3 Over-Arching Cybersecurity Agency**.

1.3 Administration and Enforcement Process

Should a violation of the PPL occur or be suspected, the PPA will consider the circumstances, the severity and the nature of the violation. It will:

- initiate administrative enforcement proceedings; or
- in egregious cases, initiate a criminal investigation, in co-operation with the cyber prosecution unit at the State Attorney's Office.

As part of the administrative enforcement proceedings, the PPA may:

- demand the correction of the deficiencies;
- prohibit the use of data by suspending or revoking the registration of the database; and
- impose administrative fines.

Administrative fines are imposed in accordance with the Administrative Offenses Law, 1985. Fines range from ILS2,000 to ILS25,000, depending on the nature of violation and the characteristics of the database owner (an individual or a legal entity). Continuous violations can carry an additional fine of 10% of the originally imposed fine, for each day in which the violation continues past the "cease and desist" date determined by the PPA.

The Banking Supervision Department and the Capital Markets Authority operate at the administrative level. They investigate incidents and may issue directives and administrative fines.

The Financial Data Services Law, 5782-2021, entered into effect in April 2022. It grants new enforcement and investigative powers in relation to the provision of financial data services (ie, the collection, transfer, and online use of financial data). The law specifies privacy protection and cybersecurity obligations regarding consumers' financial information. It grants expansive enforcement and investigative powers to the Securities Authority over financial bodies that violate the law, such as retention of financial information for longer than permitted by the law, or use of information for purposes other than those for which it was collected.

1.4 Multilateral and Subnational Issues

The matter of regulation and enforcement at multilateral or subnational level is not applicable in this jurisdiction.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

In 2018 and 2021, the Israeli government published proposals for a Cyber Defense Bill, as explained further in **1.1 Laws**.

In December 2020, the Banking Supervision Department at the Bank of Israel amended the requirements regarding data breach notifications and added the New Reporting Directive No 880, Reporting Technological Failure Incidents and Cyber Incidents. The Directive outlines the scope of information that must be provided to the Supervision Department at each phase, as further detailed in **2.5 Financial or Other Sectoral Regulators**.

The Financial Data Services Law includes a notification obligation to the Securities Authority (in addition to the PPA) regarding any severe security incident (as defined under **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**) at a financial data service provider.

Insurance companies and financial institutions are required to report any cybersecurity incidents and data breaches to the Capital Markets Authority.

An organisation experiencing a data breach may turn to the NCD or the Police's National Cyber Unit for assistance in handling and investigating the incident and its origin; however, this is not a requirement by law.

1.6 System Characteristics

The enforcement by the regulators in Israel is less aggressive than the enforcement of regulators in the EU and the USA.

According to the PPA's annual report for 2021, the PPA conducted a total of 216 supervisory cases and 60 follow-ups. A list of enforcement actions is available on the Privacy Protection Authority's website and a summary is included in its biennial report.

In addition, 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 Israeli Model

At a high level, the Israeli privacy regime is slightly more similar to the EU omnibus model. Substantively, the Israeli framework comprises of rules governing traditional notions of privacy, alongside an outdated set of rules governing data protection (with the exception of the rules for data security measures, which are fairly recent and modern).

Recently, the PPA has been pushing to overhaul Israel's privacy regime to modernise it to more closely resemble the EU's General Data Protection Regulation (GDPR). In late January 2022, the Knesset's plenum approved in first reading a new bill to amend the PPL. The bill's enactment was ultimately discontinued when early elections were called in 2022. Among other issues, the bill aimed to amend some of the PPL's definitions to bring them closer to the GDPR. For example, the bill proposed to change the term "database owner" to "database controller" and "sensitive information" to "especially sensitive information", the definition of which is akin to the GDPR's "special categories of data".

Owing to the definitional limitations in the PPL currently in effect, the PPA published in 2022 an opinion document advocating for a broad interpretation of the terms "information" and "knowledge of a person's private affairs" in the PPL.

1.7 Key Developments

The proposed amendment to the PPL, which passed first reading in late January 2022, aims

to grant the PPA much-needed rigorous supervisory and enforcement powers, including a much broader authority to impose penalties.

As mentioned in **1.6 System Characteristics**, this is the most recent attempt to overhaul the PPA, and it resumed in late 2021 but was discontinued again in 2022. The new bill encompasses five main amendments, as described in **1.8 Significant Pending Changes, Hot Topics and Issues**. The Shirbit data breach incident, disclosed in late 2020, attracted significant public attention and regulatory scrutiny, as further detailed in **8.2 Significant Audits, Investigations or Penalties**.

There have been a few reports of significant "black hat hackers" (or state-sponsored) data breach incidents against public agencies and commercial companies in Israel. In 2020, Iran launched a cyber-attack against Israel's water supply infrastructure, attempting to increase the levels of chlorine in six water facilities that supply fresh drinking water to Israeli homes. The attack was reportedly unsuccessful in causing any operational impact.

In October 2021, a series of Israeli targets were attacked, most likely orchestrated by Iranian hacker groups. The attacks crippled systems of one major hospital and blocked the access to multiple sites hosted on the servers of one Israeli hosting company. The hackers also leaked some of the personal information obtained from the attacks, including the information of users of one dating website and of patients of a major chain of medical institutes. In November 2021, Israeli internet providers were issued an order requiring them to block the access to any website containing the leaked information.

A significant development impacting the financial sector is the enactment of the Financial Data Services Law in November 2021. As mentioned in **1.3 Administration and Enforcement Process**, the law regulates financial data services. It requires financial bodies interested in providing financial data services to obtain a designated licence from the Israeli Securities Authority. Subject to the consumer's consent, licensed financial bodies can receive and transmit consumers' financial data to and from other financial bodies, via a designated online system.

Because the relationship between the financial bodies and their data sources involves the transfer of voluminous personal information, the law specifies detailed provisions regarding the manner of collection, use, storage and transfer of financial information, as well as provisions regarding cybersecurity and security incident handling. The law adopts the PPL's principles such as consent, choice, purpose limitation and data minimisation, and in some cases even extends their scope. For example, the Financial Data Services Law gives data subjects a broader right to correct data. According to the law, the financial body must investigate any reported "flaw" in the consumer's financial data – a broad term which also includes a cybersecurity malfunction leading to unauthorised access to or unauthorised disclosure of the data, regardless of who submitted the report. In comparison, the right to correct data under the PPL is only exercisable by the data subjects themselves, and only where the data was found to be incorrect, incomplete, unclear or outdated. The law's provisions came into effect starting April 2022.

For more details regarding enforcement and publicly disclosed developments, please see **8.1 Regulatory Enforcement or Litigation**.

1.8 Significant Pending Changes, Hot Topics and Issues

One of the pending changes is the bill to amend the PPL, although this bill is now suspended. The bill included the following five key amendments.

Amendments to PPL's Definitions

The bill proposed to amend the definition of "personal information", which currently only covers certain types of personal information. The proposal would extend it to "any information about an individual, who is directly or indirectly identified or identifiable by reasonable measures". It also proposed to rewrite the definition of "sensitive information" as "especially sensitive information", and expand its scope to include genetic information, biometric identifiers, and criminal records. Importantly, the term "holder" would change to resemble "processor" under the GDPR, and be defined as anyone with "authorisation to use the information stored in the database to provide services" to the database owner.

Limitations to the Database Registration Obligation

The bill proposed to minimise the scope of the obsolete duty to register databases. The obligation would only apply to:

- databases that include information about 100,000 individuals or more, and this information was not collected directly from the data subjects, on their behalf or with their consent;
- databases that are owned by a public authority;
- databases whose main objective is to deliver the information to others; and
- databases that include especially sensitive information about 500,000 individuals or more.

However, it is unclear whether such amendment would downscale the registration obligation because the bill would expand the definition of "personal information" indefinitely, thereby also expanding the definition of "database" and, in turn, the scope of databases subject to compulsory registration.

Lawful Management

The bill proposed to add a provision prohibiting the management or possession of a database whose information was created, received, accumulated, or collected in violation of the law or any other legal provisions. This would introduce a severe limitation on processing information. This is seemingly consistent with the GDPR's legal bases for processing, but does not conform with Israeli law which only recognises two legal bases:

- a data subject's express or implied consent; or
- a legal obligation to process the data.

Use Limitation

The current version of the PPL codifies the principle of purpose-limitation by banning the use of information about an individual's private affairs for any purpose other than the purpose for which it was collected. The bill proposed to significantly expand this prohibition to not only apply to information, but to "knowledge about an individual's private affairs" as well. It would have gone so far as to prohibit controllers and processors from allowing others to use information about an individual's private affairs as well. In addition, the bill suggested prohibiting individuals from using or holding such information or knowledge without the permission of the database owner.

Enforcement Powers

The bill proposed a wide extension of the PPA's enforcement powers, which the PPA has been claiming to lack for years. Among other things, the bill expanded the PPA's investigative and supervisory powers to include the power to investigate offences, seize materials, detain a person for investigative purposes, and more. In addition, it granted the PPA authority to impose fines in increasing amounts, relative to the number of data subjects whose information is stored in the database. The proposed baseline fines are ILS800,000, which can be multiplied up to four times.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

The Data Security Regulations apply to all Israeli organisations, companies and public agencies that own, manage, maintain or service a database containing personal data. The Data Security Regulations create four tiers of data security obligations, 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 (ie, special categories of data) and the number of people with access credentials.

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 telecoms and internet providers, transportation carriers, the Stock Exchange, the Israeli ccTLD Registry, utility companies and others.

2.2 Regulators

The PPA is responsible for enforcing the data security regulations, and the PPL generally, across all Israeli organisations, companies and public agencies.

The Banking Supervisor at the Bank of Israel is responsible for enforcing the data security and breach rules relating to incidents in banks and credit card companies.

The Supervisor of Capital Markets, Insurance and Savings within the Israeli Ministry of Finance is responsible for enforcing the data security and data breach rules relating to incidents at insurance companies.

The Securities Authority is responsible for enforcing the data security and data breach rules relating to incidents at financial bodies providing financial data services or acting as financial data sources under the Financial Data Services Law.

The NCD must, among other things, manage, control and carry out the overall nationwide operational efforts to protect cyberspace as further described in **2.3 Over-Arching Cybersecurity Agency**.

2.3 Over-Arching Cybersecurity Agency

In 2015, the government established a National Cybersecurity Authority, and in 2018 merged it with the National Cyber Headquarters, which was tasked with national-level capabilities in cyberspace. The agency resulting from that merger is the NCD. The executive decision on the establishment of the Cybersecurity Authority, which since then has been absorbed into the NCD, prescribes the 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 (CERT);
- 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 its designated mission.

2.4 Data Protection Authorities or Privacy Regulators

The PPA is the Israeli privacy regulator. The PPA is responsible for enforcing the PPL, and has investigative powers in relation to violations of the PPL and the Data Security Regulations, as further described in **1.2 Regulators**.

2.5 Financial or Other Sectoral Regulators

The Supervision Department at the Bank of Israel is responsible for enforcing cybersecurity and the data breach rules relating to cybersecurity incidents at banks and credit card companies, among other issues. 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 **3.3 Legal Requirements and Specific Required Security Practices**.

The Capital Markets, Insurance and Savings Authority operates within the Israeli Ministry of Finance, and is responsible for enforcing the data security and data breach rules relating to cybersecurity incidents at insurance companies and financial institutions.

The Securities Authority is responsible for enforcing the data security and data breach rules relating to incidents at financial bodies providing financial data services or acting as financial data sources under the Financial Data Services Law. It also oversees public companies in their obligations to disclose material cybersecurity risks as further described in **10.2 Public Disclosure**.

2.6 Other Relevant Regulators and Agencies

All relevant regulators and agencies have already been covered.

3. Key Frameworks

3.1 De Jure or De Facto Standards

The PPA has issued guidance discussing the relation between the Data Security Regulations and ISO 27001. According to this guidance, organisations certified to ISO 27001 will have to additionally comply with a small subset of the full Data Security Regulations, so long as they also demonstrate that they actually follow the controls and requirements of ISO 27001.

In 2015, The Israeli Ministry of Health (MoH) issued a data security circular alerting all medical institutions (clinics, the Health Maintenance Organisation 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 that are certified to either ISO 27001 or ISO 27799.

3.2 Consensus or Commonly Applied Framework

Specific references to "reasonable security" were repealed with the entry into force of the prescriptive Data Security Regulations in 2018. The preceding regulations required database owners to establish reasonable security measures.

3.3 Legal Requirements and Specific Required Security Practices

Security Measures

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 (eg, 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 (ie, 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 (ie, 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 (ie, 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 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 to 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 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.

The Data Security Regulations introduce additional requirements applicable to databases subject to the intermediate level of security:

- 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 even further requirements applicable to databases subject to the highest level of security:

- 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.

In addition, 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.

In August 2022, the PPA tightened the policy regarding information security incidents and now requires that an immediate report be given to it upon discovery, or when there is concern about the existence of a serious information security incident, as well as the steps taken following the incident. Until 2022, the PPA had indicated that the time frame for reporting the incident in such a case is within 24 hours of the discovery of the security incident, and in any case no later than 72 hours from that date.

In certain circumstances, the PPA may order the organisation, after consultation with the Head of the National Cybersecurity Authority (now replaced by 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".

Banks are required to report any cybersecurity incidents and data breaches pursuant to regulatory guidelines by the Supervision Department. In December 2020, the Supervision Department amended the requirements regarding data breach notification and added the New Reporting Directive No 880, Reporting Technological Failure Incidents and Cyber Incidents. Now, banks and credit card companies are required to report to the Supervision Department by phone within two hours following the discovery of the incident. Thereafter, an initial report will be given in writing within eight hours. Later on, reports will be submitted daily or if a critical development has unfolded.

Insurance companies are required to report any cybersecurity incidents and data breaches pursuant to regulatory guidelines by the Capital Markets Authority.

The Israeli Securities Authority also published a position paper emphasising a publicly traded company's duties of disclosure, as further described in **10.2 Public Disclosure**.

Registration with Regulatory Authority

The PPL 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.

Appointment of an Information Security Officer

Under the PPL, certain organisations are required to appoint an information security officer. These organisations include public entities, service providers who process five or more databases of personal data by commission for other organisations (ie, as processors) 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 Israeli PPA published a paper on the advisable appointment of data privacy officers in Israeli organisations, regardless of whether they are required to do so by law. The PPA explained that it views the voluntary appointment as a recommended best practice for organisations whose operations involve processing personal data. The paper states that an

appointed data privacy officer is required to have in-depth knowledge of data protection laws and a sufficient understanding in the field of information technologies and information security. The paper recommends that the data privacy officer be involved in the organisation's data protection-related matters from the outset, that it serve as the key liaison with the PPA on all matters involving the regulator, and that the data privacy officer need not be a member of the organisation's senior management so long as they report to senior management.

The Data Security Regulations requires risk assessments and penetration tests at least once every 18 months for databases subject to the high level of security to conduct. The results of such assessments should be discussed and any required amendments or changes should be implemented.

Database owners are required to examine the security risks associated with engagements with service providers who are given access to the database, prior to such engagement. Under the Data Security Regulations, an agreement with the service provider should address the following matters:

- the purposes for which the service provider is authorised to access or process the personal data;
- the categories of personal data to which the service provider will have access during the engagement;
- the types of processing activities that the service provider is allowed to perform;
- the duration of the engagement, and instructions for returning the personal data to the database owner or destroying it, upon the termination or expiration of the engagement;
- how compliance with the above instructions is to be reported to the database owner;
- information security obligations imposed on the service provider pursuant to the Data Security Regulations, as well as additional instructions by the database owner with respect to the information security measures that the service provider must undertake;
- service provider's obligation to have its authorised personnel sign an undertaking to maintain the confidentiality of personal data, to use personal data only pursuant to the provisions of the agreement between the service provider and the database owner, and to comply with the security measures set forth in the agreement between the service provider and the database owner;
- provisions regarding the transfer of data to sub-processors acting on behalf of the service provider, including a provision stating that any transfer of data shall be subject to a signed written agreement which flows-down similar provisions;
- an obligation to provide the database owner a report, at least once a year, on the performance of service provider's obligations pursuant to the Data Security Regulations and the applicable agreement;
- an obligation to notify the database owner whenever the service provider reasonably believes that there has been a security incident; and
- the database owner's right to audit service provider's compliance with the provisions of the Data Security Regulations and the applicable agreement.

The database owner must also perform periodic audits to ensure the service provider's compliance with the above-mentioned obligations.

According to Directives 359A on the Proper Conduct of Banking Business (10/18), when banking corporations and other financial institutions wish to outsource their activities, they must fulfil the following.

- Conduct diligence reviews assessing the political, financial, legal and regulatory restrictions imposed on the service provider, and the possible implications of transferring data outside of Israel.
- Address the following matters, among others, in the outsourcing agreement:
  (a) the activities to be outsourced and an adequate service level agreement;
  (b) service provider's liability to the banking corporation;
  (c) service provider's audit practices, including in aspects of data security, privacy protection and business continuity;
  (d) banking corporation's right to receive information regarding the outsourced activities, to audit them and to report them to the Supervisor of Banks;
  (e) banking corporation's right to monitor and evaluate the service provider on an ongoing basis so that the banking corporation can take immediate corrective measures if necessary;
  (f) managing and monitoring service provider's access to proprietary information of the banking corporation or of its customers;
  (g) manner of discontinuation of the engagement;
  (h) indemnifying and compensating the banking corporation for claims caused by the service provider's negligence; and
  (i) immediate reporting to the banking corporation of any damage to or invasion of data of customers or of the banking corporation, and of any change that has a material effect on the continued delivery of service.

There are no general regulations regarding use of cloud computing or cloud services.

In September 2021, the Supervisor of Banks issued a directive outlining the guidelines for maintaining data security when using cloud computing. According to the directive, banking corporations should:

- not use cloud-computing services for core activities or core systems;
- not store, transfer, or process information that it defines as "sensitive" (eg, customer data) on a cloud outside the borders of the state of Israel, unless the cloud service provider maintains a level of protection that complies with the provisions of the GDPR;
- perform risk-mapping and risk-assessment for every material cloud computing implementation; and
- address in the agreement with a cloud service provider, among other things, the banking corporation's right to unilaterally terminate the agreement, to transfer or delete its data from the service provider's systems, and to perform inspections and audits of the service provider.

A February 2022 preliminary opinion by the Ethics Committee of the Israeli Bar bans lawyers and law firms from using the services of free third-party tools for the management, storage and transfer of clients' information (eg, Gmail, Dropbox, etc). The Israeli Bar considers those tools to be insufficiently secure. The preliminary opinion clarified that lawyers who use such tools will be deemed in breach of the confidentiality obligation they are subject to by virtue of the Bar

Association Rules (Professional Ethics), 5746-1986.

3.4 Key Multinational Relationships

Multinational relationships are not relevant in this jurisdiction.

4. Key Affirmative Security Requirements

4.1 Personal Data

The Data Security Regulations require any Israeli organisation that owns, manages or maintains a database containing personal data to implement prescriptive security measures; the main objective of these measures is the prevention of incidents. See **3.3 Legal Requirements and Specific Required Security Practices** for more information.

In addition, financial institutions and insurance companies are required to establish a security operation centre tasked with monitoring, detecting and mitigating cybersecurity risks.

4.2 Material Business Data and Material Non-public Information

Affirmative security requirements are not applicable in this jurisdiction.

4.3 Critical Infrastructure, Networks, Systems

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency and the NCD to issue binding directives to organisations operating critical infrastructures or essential services on matters related to information security and cybersecurity, and inspect such organisations' compliance with those directives. Organisations subject to this regime include telecoms and internet providers, transportation carriers, the Tel Aviv Stock Exchange, the Israeli Internet Association, utility companies and others.

These directives were not publicly disclosed. In late 2021 and throughout 2022, the Israeli Ministry of Health issued a number of binding circulars and guidelines on cybersecurity assessments and preparedness in health institutions.

4.4 Denial of Service Attacks

There are no specific references to denial-of-service attacks in Israeli primary or secondary legislation. The Data Security Regulations prescribe the data security measures that organisations must implement, as explained in **3.3 Legal Requirements and Specific Required Security Practices**.

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

There are no specific references to IoT, supply chain or other systems in Israeli primary or secondary legislation. The Data Security Regulations prescribe the data security measures that organisations must implement, as explained in **3.3 Legal Requirements and Specific Required Security Practices**.

4.6 Ransomware

Ransomware attacks are likely to be considered as breach incidents that must be notified to the relevant regulator, as further described in **5. Data Breach and Cybersecurity Event Reporting and Notification**.

Anti-money laundering laws in Israel prohibit virtual currency service providers from transferring virtual currency to a recipient whose identify is not confirmed. The Terrorist Financing Prohibition Law bans transactions that enable, promote, aide, or finance terrorism. Finally, the Enemy Trade Ordinance prohibits transacting

with persons in enemy countries. Each of these can be a barrier to paying ransom in ransomware attacks.

5. Data Breach or Cybersecurity Event Reporting and Notification

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event

Under the Data Security Regulations, a potentially reportable data security incident is a "severe security incident", defined as 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 damage to the data integrity; and
- in a database subject to medium security level – an incident involving the use of substantial part of the database without authorisation or in excess of authorisation, or damage to the data integrity with respect to a substantial part of the database.

The PPA has also published a list of examples in which the obligation to notify the PPA arises:

- detected intrusion into the organisation's network in which there are reasonable grounds to suspect that an unauthorised person had physical or digital access to the organisation's database, making it possible to view, change or delete information contained in it;
- detection of an actual breach of sensitive information (to any extent) from the organisation's database, by external messaging or publication;
- temporary or permanent damage, deletion, disruption or prevention of access to the organisation's information, due to intentional physical damage to the database systems;
- theft or loss of computing equipment, removable media or a physical means of backup that contains sensitive information from an organisation's database; and
- detection of an attempt to access, modify or delete sensitive information in a database held or managed by an external party by virtue of an agreement.

5.2 Data Elements Covered

The data breach notification requirements apply to databases containing "information" as defined in the PPL: data on the personality, personal status, intimate affairs, health condition, economic status, vocational qualifications, opinions and beliefs of a person.

5.3 Systems Covered

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. See **3.3 Legal Requirements and Specific Required Security Practices** for information regarding the tiers.

5.4 Security Requirements for Medical Devices

The MoH has established a policy for cybersecurity in medical devices. 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, encryption of wireless transmission. The guidelines also prescribe the cyber-risk-management measures that healthcare provid-

ers must implement when purchasing, installing and using medical devices.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

There are no specific references to industrial control systems in Israeli primary or secondary legislation. The Security of Public Bodies Law applies to operators of critical infrastructures, but the security obligations that apply pursuant to that law are not publicly disclosed.

5.6 Security Requirements for IoT

There are no specific references to IoT in Israeli primary or secondary legislation.

5.7 Requirements for Secure Software Development

Under the Data Security Regulations, the notification obligation for a database at the intermediate level of security applies when the breach extends to any material portion of the database, while the notification obligation for a database at the high level of security applies to any breach, regardless of its scope or materiality. Where such a breach occurs in the systems of an entity that is either a financial data service provider or a financial data source under the Financial Data Services Law, the Securities Authority should be notified as well.

In certain circumstances, the PPA may order the organisation, after consultation with the Head of the National Cybersecurity Authority (now replaced by 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".

A preliminary opinion, published by the Ethics Committee of the Israeli Bar in February 2022, established an exceptional reporting obligation for law firms experiencing a data breach involving their clients' confidential information. Although the Data Security Regulations' state that the PPA will determine whether an affected organisation should notify data subjects, the Ethics Committee requires lawyers to notify their clients of any data breaches that might affect their information.

Medical institutions are required to report to the MoH about any malfunction or an unplanned interruption in the operation of a service that is essential to the proper functioning of the medical institution (including computer services). Banks are broadly required to report any cybersecurity incidents and data breaches to the Banking Supervision Department if they have a material impact on the bank's operations.

Insurance companies are broadly required to report any material cybersecurity incidents and data breaches to the Capital Markets Authority Department if they have a material impact on the insurance company's operations.

Public companies are required to submit an immediate report to the Stock Exchange through the stock exchange reporting system when the security incident constitutes a "company material event". Company material event means any event or matter that deviates from the ordinary business of the corporation "and which has or may have a material effect on the company".

5.8 Reporting Triggers

The common threshold that applies to notification is the "materiality" or "significance" test. For companies subject to the intermediate level of security under the Data Security Regulations,

this test examines whether a material part of the database was compromised.

For publicly traded companies or companies subject to oversight by the Banking Supervision Department, this test examines whether the incident has a material impact on the company, its operations, business continuity, customers, etc. For entities subject to oversight by the Banking Supervision the Capital Markets Authority, this test examines whether the incident is "significant" for systems with sensitive information which were compromised or suspended for more than three hours, or if there is an indication that sensitive information of the covered entities customers or employees was compromised or leaked.

5.9 "Risk of Harm" Thresholds or Standards

No information is available on "risk of harm" thresholds or standards.

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

Israeli legislation restricts the use of some practices and tools for network monitoring and cybersecurity defensive measures. Some examples are provided below.

Monitoring Emails, Web Access, and Internet Traffic

As a threshold matter, these measures could constitute unlawful invasion of privacy, unlawful wiretapping or unlawful intrusion into another person's computer if they are performed without the informed consent of the person being monitored.

For example, in the context of employee monitoring, Israeli case law in the 2011 Isakov case held that an employer monitoring employees' email accounts assigned to them by the employer is permissible if the employer also establishes a policy that these email accounts are to be used only for work-related purposes and not for personal correspondence, and provided that certain other conditions are met. These other conditions include the prior, affirmative, informed and written consent by the employee to a policy establishing such employer monitoring, and further provided that the measures used for monitoring are proportionate and aimed only at legitimate business purposes.

See **6.2 Intersection of Cybersecurity and Privacy or Data Protection** for more information.

Beacons

Use of beacons could arguably amount to unlawful intrusion into computer material, but could be defensible under the affirmative defences of necessity or self-defence.

Honeypots

Use of honeypots for detection purposes is likely permissible so long as it does not involve unlawful intrusion into the cyberthreat actors' computers or invasion of their privacy (although these may in turn be defensible under the affirmative defences of necessity or self-defence). Use of honeypots for counter-attacks would amount to unlawful intrusion into the cyberthreat actors' computers and other correlative offences.

Sinkholes

Use of sinkholes for deflection purposes is likely permissible so long as it does not involve unlawful intrusion into another person's computer, invasion of their privacy or interference with the ordinary functioning of their computer (although

these may in turn be defensible under the affirmative defences of necessity or self-defence).

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Cybersecurity measures that involve various forms of monitoring emails, web access, and internet traffic could arguably give rise to actionable invasion of privacy, wiretapping or unlawful intrusion into another person's computer, if they are performed without the informed consent of the person being monitored.

Although not focused on cybersecurity, the 2011 Isakov case of the Israeli National Labor Court expounded Israeli privacy law as applied to employers monitoring and accessing employees' email communications. As further explained in **6.1 Cybersecurity Defensive Measures**, the judgment 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.

In December 2022, the PPA published a document on the privacy aspects of monitoring remote workers. The document describes types of surveillance measures that may significantly exceed what is necessary and permitted by law, such as tools for scanning and monitoring websites that the employee visits, means for controlling webcams on the employee's computer or means for monitoring the employee's movement. Employers are required to comply with the principle of data minimisation and to refrain from the collection and storage of information that is not necessary for the purpose of legitimate surveillance. Employers are also obligated to examine, at least once a year, whether the information collected should be discarded.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

The data breach notification requirements to regulators compel the sharing of certain cybersecurity information with regulators.

The Cyber Defense Bill proposed to grant powers to the NCD, such as the ability to obtain a court order compelling organisations to take specific actions in response to or in preparation for a cyber-attack.

There is also no specifically codified exemption from liability to Israeli organisations that voluntarily share cybersecurity information with the government, although generally available affirmative defences could be invocable to insulate from, or at least downscale, such liability.

7.2 Voluntary Information Sharing Opportunities

The NCD operates the Operational Center for Cyber Incident Management 119, which can be reached voluntarily in any case where there is a concern about a cybersecurity incident (phishing, DDoS, scraping, etc).

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation

The Israeli Capital Markets, Insurance and Savings Authority (the "Authority") at the Israeli Min-

istry of Finance, together with the Israeli National Cyber Directorate, launched an investigation into the cyber-attack perpetrated against the Israeli insurance company Shirbit.

The company's website and servers were shut down and sensitive information about the company's employees and insureds was compromised and offered for sale online. The sensitive information includes national ID cards and insurance claims history with medical records.

Following the incidents, the PPA – for the first time – exercised its power under the Data Security Regulations to require Shirbit to inform its insureds of the breach, with recommendations on what they can do to safeguard themselves. In November 2021, the Authority fined Shirbit ILS10.7 million, following a long investigation in which it found that Shirbit did not properly manage its cyber-risks.

In another instance, an employee of an Israeli offensive cybersecurity company misappropriated the company's offensive cyber tools and attempted to sell them for tens of millions of dollars on the darknet. He was apprehended, indicted and convicted in a plea-bargain.

8.2 Significant Audits, Investigations or Penalties

The PPA completed an investigation into the illegal trafficking of personal data about insureds in Israel's three largest insurance carriers. The investigation revealed that an insurance agency had colluded with employees of insurance companies to mine sensitive data from the insurance carriers systems. The agency had paid ILS30 for each record of an insured that the insurance companies' employees retrieved for the agency. The state attorney's cyber-unit is considering criminal charges against the suspected offenders.

In December 2022, the PPA announced that it had imposed a fine of ILS320,000 on a data broker and enrichment company that had systematically and repeatedly violated the PPL, despite past commitments made to the PPA that it would cease and desist. The company was charged with several counts of PPL violations.

8.3 Applicable Legal Standards

Pursuant to the PPL, the PPA has broad authority to investigate any person and obtain any documents and information that relate to the operation and use of databases containing personal data. The PPA is also authorised to search for and seize evidence, including computerised material, located in any premises reasonably believed to be operating or using a database of personal data.

However, the PPA's authority to impose fines is much more limited. It only extends to a subset of violations of the PPL and the maximum imposable fines are relatively low, up to ILS25,000. Notably, the PPA is not presently authorised to impose fines for failures to implement the required data security measures. As a result of its limited powers to impose fines, the PPA often resorts to merely publishing "findings of fault", in order to publicly condemn violations.

These published "findings of fault" may motivate private actors to assert legal claims, including class actions lawsuits, against the wrongdoers.

8.4 Significant Private Litigation

Other than class action lawsuits, which are detailed in **8.5 Class Actions**, there have been very few notable lawsuits based on privacy, data protection or data security grounds.

One rare example is a recent petition filed by an attorney advocating for privacy protections, requesting that the court enjoin political parties and the company that operates the Elector app from using the app in the upcoming general election in Israel, amid the data breach that occurred through their use of the app in 2020. The petition was dismissed.

8.5 Class Actions

Class action lawsuits on privacy, data protection and data security are permitted and have been ongoing in court in recent years. However, the Israeli Class Actions Law limits class action lawsuits based on privacy, data protection or data security grounds, to only those arising out of a consumer's relationship with a business.

Virtually all class actions are disposed of by way of settlement, and class action lawsuits around privacy, data protection and data security are no different. However, the disposition of class action lawsuits is slow and lengthy, with some lawsuits pending for years. Two examples are provided below.

In 2020, a motion for class action certification was filed, seeking damages amid an alleged data breach involving medical information of tens of thousands of patients of healthcare providers in Israel. The lawsuit was filed against Israel's largest and third-largest health maintenance organisations as well as against two medical centres. It alleges that the breach was uncovered after a veterinarian who purchased used medical devices discovered that they still stored the medical history of patients. An expert opinion by a data security professional indicated that the information was not anonymised and was accessible to anyone operating these devices. The lawsuit alleges that as a result, medical records of approximately 78,882 people were exposed. The lawsuit seeks damages of ILS1.5 billion.

Another motion for class action certification was filed against the genealogy platform MyHeritage, seeking ILS100 million due to a data breach on the platform. A proposed settlement was filed for court approval in 2021. The proposal does not include payment of actual damages, but an offer to MyHeritage users to receive free access to a feature on the MyHeritage platform. The proposed settlement was formally opposed by a privacy advocacy association in Israel, and the court is expected to consider and decide on the proposed settlement in 2023.

Following Shirbit's data breach incident, four lawsuits seeking class action certification were filed against Shirbit, which were joined to one class action in July 2021. The representative class is seeking hundreds of millions of Israeli shekels in damages.

A motion for class action certification against Facebook, filed in October 2018, was dismissed in August 2022. The motion sought compensatory damages for Facebook users in Israel amid a data breach in the social network in 2018. The plaintiff claimed that the data breach constituted a breach of contract by Facebook under its terms of service, unfair dealing, breach of the covenant of good faith and violation of privacy – but all claims were dismissed.

9. Cybersecurity Governance, Assessment and Resiliency

9.1 Corporate Governance Requirements

The PPL compels the appointment of a Chief Information Security Officer in a number of instances, as further described in **3.3 Legal**

Requirements and Specific Required Security Practices. The Data Security Regulations impose requirements regarding risk assessments, security audits and penetration tests as further described in **3.3 Legal Requirements and Specific Required Security Practices**. The Israeli Securities Authority has opined that a publicly traded company has specific duties of disclosure as further described in **10.2 Public Disclosure**.

10. Due Diligence

10.1 Processes and Issues

When conducting diligence in corporate transactions, the issues most frequently investigated are the company's efforts to comply with the Israeli Data Security Regulations, its use of external service providers to process data, the measures it uses for privacy notice and consent when collecting information from data subjects, the registration of its databases with the PPA and its cross-border data transfer activities.

10.2 Public Disclosure

In October 2018, the Israeli Securities Authority published a position paper titled "Cyber-Related Disclosures". The paper opined that companies must adequately disclose cyber-risks in their quarterly reports and prospectuses, as part of their general duty to disclose risks that the company faces. The paper also extends to similar reports required to be issued to the market as a matter of course, in case of cybersecurity events that have occurred, and which are not the part of the ordinary course of the business and present a potentially material impact on the company.

The document aims to increase the transparency required of public companies, but its impact on private companies is minor. Companies whose securities are not publicly traded can still largely refrain from public disclosures. The document also demands that cyber-issues be addressed by the company's board of directors.

11. Insurance and Other Cybersecurity Issues

11.1 Further Considerations Regarding Cybersecurity Regulation

All relevant issues have already been covered in the preceding sections.

Pearl Cohen Zedek Latzer Baratz is an international law firm with offices in Israel, the USA and the UK, offering legal services across numerous practice areas. Pearl Cohen's cyber, data protection and privacy practice group in Israel comprises seasoned attorneys who leverage their nuanced understanding of new technologies and their experience in internet and cyber law to offer clients comprehensive legal services for the growing complexities of information and data privacy regulations. At times, data protection and privacy matters entail court or administrative proceedings. Pearl Cohen's data protection and privacy practice group has accumulated vast experience in representing clients before the Israeli Protection of Privacy Authority through investigative, supervisory and enforcement procedures, and before Israeli courts in privacy and data protection litigation. Pearl Cohen also represents clients in deliberations on bills in the Israeli Parliament's committees.

Authors

Haim Ravia is senior partner and chair of Pearl Cohen's internet, cyber and copyright group. Haim deals extensively with data protection and privacy, cyber and internet law, copyright, electronic signatures and open-source software.

Dotan Hammer is a partner in the internet, cyber and copyright group at Pearl Cohen. His practices primarily focus on cyber, data protection and privacy, where he counsels a wide array of clients – from technology-driven to bricks-and-mortar – on the ins and outs of data and cyber regulation in the USA, the EU and Israel. Having completed his academic degree in computer science at the age of 19, later working as a software developer and a technological project leader in the public sector in Israel, Dotan now uses his technological background to counsel clients in these emerging areas in law.

Pearl Cohen Zedek Latzer Baratz

Azrieli Sarona Tower – 53rd floor
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9000
Fax: +972 3 303 9001
Email: Tel-Aviv@PearlCohen.com
Web: www.PearlCohen.com; www.law.co.il

PEARL COHEN

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com