Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2024

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

Israel: Law & Practice

Haim Ravia and Dotan Hammer
Pearl Cohen Zedek Latzer Baratz

ISRAEL

Law and Practice

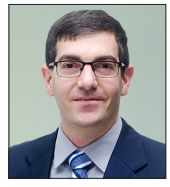
Contributed by:
Haim Ravia and Dotan Hammer
Pearl Cohen Zedek Latzer Baratz

Contents

Pearl Cohen Zedek Latzer Baratz (Pearl Cohen) 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 that respond to the growing complexities of information and data privacy regulations. At times, data protection and privacy matters entail court or administrative proceedings. Pearl Cohen's cyber, 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 cyber, privacy and copyright group. Haim deals extensively with data protection and privacy, cyber and internet law, copyrights, electronic signatures and open-source software.



Dotan Hammer is a partner in Pearl Cohen's cyber, privacy and copyright group and heads the firm's global privacy practice. 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, Dotan now uses his technological background to counsel clients in these emerging areas.

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

1. Basic National Regime

1.1 Laws

Fundamental Israeli laws applicable to cybersecurity include the Israeli Computers Law, the Protection of Privacy Law, the Penal Law, the Defence Export Control Law, the Regulation of Security in Public Bodies Law, and the (proposed) amendment to the General Security Service Law.

The PPL

The primary Israeli law governing data protection is the Protection of Privacy Law, 5741-1981 (PPL). The PPL applies to any entity that manages or possesses a database, including private and public entities. A "database" is defined as a collection of information. "Information" is data on the personality, personal status, intimate affairs, health condition, economic status, vocational qualifications, opinions or beliefs of a person that is 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 invade the privacy of the persons whose information is included therein.

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**.

Data Security Regulations

The Protection of Privacy Regulations (Data Security), 5777-2017 (the "Data Security Regulations"), are an omnibus set of rules promulgated by the Israeli Parliament in 2017, and effective as of 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 the regulations promulgated thereunder, the Israeli Protection of Privacy Authority (PPA) may take the measures detailed in **1.3 Administration and Enforcement Process**.

The Israeli Computers Law

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

The Regulation of Security in Public Bodies Law, 5758-1998, 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 Israeli country code top-level domain (ccTLD) registries, utility companies and others.

The Israeli Defence Export Control Law

The Israeli Defence 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.

General Security Service Law Amendment

In December 2023, the Israeli government published a proposal to amend the General Security Service Law, 5672-2002, which governs the authority and operation of the ISA. The proposal, which has yet to be enacted, introduces a significant expansion of the ISA's powers, particularly in the areas of intelligence collection and surveillance. The proposal establishes a legal basis for the use of advanced surveillance tools enabling the ISA to covertly access and collect data from various databases in Israel. It is designed to address scenarios in which obtaining information through ordinary investigative methods would undermine the clandestine nature of intelligence operations.

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 PPA, within the 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 notifi-

cation obligation took effect in 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. The Supervision Department conducts audits 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 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. The Capital Markets Authority also conducts audits 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 information and documents;
- 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 Offences Law, 1985. Fines range from ILS2,000 to ILS25,000, depending on the nature of violation and the characteristics of the database owner (individual/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 to regulated entities.

The Financial Data Services Law, 5782-2021, entered into effect in 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 extensive enforcement and investigative powers to the Israel Securities Authority (the national securities regulator) over financial bodies that violate the law, such as retention of financial information for longer than permitted by 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 Israel.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

In February 2023, the Banking Supervision Department amended the requirements regarding data breach notifications detailed at 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 of a cyber-incident, 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 data 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, doing so is not a legal requirement. The NCD operates the Computer Emergency Response Centre (CERT) for cyber-incident management, which can be reached voluntarily, as further detailed in **7.2 Voluntary Information Sharing Opportunities**.

1.6 System Characteristics

Cybersecurity enforcement by the regulators in Israel is generally less aggressive than that of regulators in the EU and the USA.

According to the PPA's latest annual report for 2022, the PPA conducted a total of 317 supervisory cases related to cyber-incidents and 400 sectorial inspections. A list of enforcement actions for each calendar year is available on the Privacy Protection Authority's website.

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 PPL is aimed at empowering the PPA with the authority to impose penalties.

The Israeli Model

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

The PPA has been pushing to overhaul/modernise Israel's privacy regime such that it more closely resembles the EU's GDPR. In 2022, the Knesset (the Israeli legislature) approved in a first reading a new bill to amend the PPL. The bill's enactment was ultimately discontinued when early elections were called in 2022. In April 2023, the government committee for legislation voted to continue the legislation. Among other issues, the bill aimed to amend some of the PPL's definitions to bring them closer to those employed by the GDPR.

1.7 Key Developments

The Israel-Gaza War

As the Israel-Gaza war unfolded in October 2023, the government promulgated emergency, wartime regulations to address severe cybersecurity incidents in the digital services and hosting sector: the Emergency Regulations (Iron Swords) (Addressing Severe Cyber-Attacks in the Digital Services and Hosting Services Sector), 2023. The regulations authorise the NCD, the Cyberthreats Division of the ISA, and the Chief of Security at the Defence Establishment in Israel, to issue directives to digital services and hosting providers in Israel in the case of a severe cybersecurity incident where a genuine threat to national security or public safety arises.

As the war continued, Israel has seen a significant increase in the scope and severity of cyber-attacks against civilian targets. These emergency regulations were substituted in December 2023 with the enactment of a provisional law for a period of seven months: Addressing Severe Cyber-Attacks in the Digital Services and Hosting Services Sector (Interim Measure – Iron Swords) Law, 2023. The directives that the authorised agencies may issue to digital services and hosting providers include action necessary to identify a cyber-attack, defend against it, or prevent it, in furtherance of the overarching objective of protecting the public interest and mitigating the adverse effects of the attack.

Israeli Data Protection "Adequacy"

in May 2023, The Israeli government published new privacy regulations (Privacy Protection Regulations (Provisions Regarding Information Transferred to Israel from the European Economic Area), 2023) that apply primarily to personal data that originates from the European Economic Area (EEA). The new regulations were adopted to support the efforts of the EU Commission to renew its recognition of Israel as an adequate country whose level of protection of personal data is equivalent to that of the EU. The regulations deal with data deletion, data minimisation, data accuracy, transparency, and more. The regulations first took effect on August 2023, regarding personal data received from the EEA as of that date onward. Beginning in May 2024, the regulations will also apply to personal data received from the EEA before August 2023. Beginning in January 2025, the regulations will also apply to all other non-EEA personal data stored in the same database with personal data of EEA origin.

in January 2024, the European Commission renewed its decision regarding the adequacy of Israel's data protection regime, recognising that it offers a level of data protection essentially equivalent to the laws in the EU. This continued recognition allows the free flow of personal data from the EU to Israel. Consequently, organisations in Israel can continue to receive personal data that is subject to the GDPR without the need for any special contractual, legal, technological, or administrative steps to legitimise the transfer.

1.8 Significant Pending Changes, Hot Topics and Issues

In April 2023, the governmental committee for legislation voted to continue the legislative process for Amendment 14 of the PPL, which was introduced in 2022 and had passed the first reading at the Knesset. The committee's decision allows the Knesset to continue its deliberations on the bill from the point they were discontinued when the previous Knesset was dissolved for elections. As of February 2024, the bill continues to pass through the legislative process. The bill proposes an expansion of the enforcement powers vested in the PPA (including a much broader

authority to impose penalties), an update to key definitions in the law, and a down-scaled obligation to register databases.

The proposed amendment to the General Security Service Law, 5672-2002 (further explained in **1.1 Laws**) introduces a significant expansion of the ISA's powers, particularly in the areas of intelligence collection and surveillance, including the use of advanced surveillance tools enabling the ISA to covertly access and collect data from various databases in Israel. The legislative process for this proposed amendment is expected to continue in 2024.

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 Regulations create four tiers of data security obligation, 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 that operate various types of critical infrastructure, including telecoms and internet providers, transportation carriers, the Stock Exchange, the Israeli ccTLD registries, and utility companies. Further key laws are detailed in **1.1 Laws**.

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 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 later 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, which is the national security and technological agency responsible for defending Israel's national cyberspace and for advancing Israel's cyber capabilities. The NCD operates to strengthen the level of defence of organisations and citizens, to prevent and handle cyber-

attacks and to strengthen emergency response capabilities. The NCD's primary roles are:

- to lead efforts to defend national cyberspace by preventing, detecting, identifying and responding to cyber-attacks;
- to prepare and enable the private sector and general public to protect themselves from cyber-threats by adopting cybersecure technologies, publishing best practices, training personnel and increasing awareness;
- to establish and reinforce the cyber science-and-technology base by developing high quality human capital, supporting advanced academic research, engaging in deep technological R&D and fostering the cyber industry;
- to design and implement a national cyberdefence doctrine; and
- to promote Israel as a world leader in cyber, thus strengthening its defence, economic resilience and international standing.

2.4 Data Protection Authorities or Privacy Regulators

The PPA is the Israeli privacy regulator. It 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. The Supervision Department has issued various regulatory requirements and guidelines for banks and financial institutions regarding privacy and cybersecurity, as detailed in **3.3 Legal Requirements and Specific Required Security Practices** and **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**.

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 relationship between the Data Security Regulations and the ISO 27001 standard. 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 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 insti-

tutions 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 database, 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, 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 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 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.

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. Any organisation subject to the Regulations is required to oversee and supervise its vendors' data security compliance on an annual basis.

The 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 user authentication measures applicable to the database, back-up 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 every 24 months; and
- a back-up and recovery plan shall be established.

The Regulations introduce even further requirements applicable to databases subject to the highest level of security:

- the database owner shall perform a risk assessment at least once every 18 months, using a qualified professional;
- the database's computer systems shall be subjected to penetration tests at least once every 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 Regulations, owners of databases designated within an "intermediate" or "high" tier of security (ie, tier-three and tier-four as outlined above) 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 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 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 cybersecurity incidents and data breaches pursuant to regulatory guidelines by the Supervision Department. In 2023, the Supervision Department amended the requirements regarding data breach notification included in the Reporting Directive No 880, Reporting Technological Failure Incidents and Cyber Incidents. 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 PPL'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 credit-worthiness evaluation.

The Security of Public Bodies Law requires certain public organisation 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 Regulations prohibit the officer from being in a position that raises a conflict of interests. Substantively, the Regulations require the officer to establish data security protocols and an ongoing plan to review compliance with the Regulations. The officer must present findings of its review to the database manager and to the officer's supervisor.

In 2022, the 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 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 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;
- 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 Regulations, as well as additional instructions by the database owner with respect to the information security measures that the service provider must undertake;
- the 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 with the database owner, and to comply with the security measures set forth in the agreement;
- 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 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 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.

Banking and Finance

According to Directive 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 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.

Cybersecurity and Legal Ethics

A 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 cybersecurity 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 and Software

The Regulation of Security in Public Bodies Law authorises the ISA and the NCD to issue binding directives to organisations operating critical infrastructure 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 ccTLD registries, utility companies and others.

These directives were not publicly disclosed. The 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, software, 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**. For further information about the PPA's guidance on the use of IoT devices and "smart home" environments, please see **5.6 Security Requirements** for IoT.

4.6 Ransomware/Extortion

Ransomware and cyber-extortion attacks are likely to be considered as breach incidents that must be notified to the relevant regulator, as further described in **5. Data Breach or 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 or extortion 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;
- transfer of sensitive information from the organisation's database by an employee, to external locations, without permission or authorisation;
- theft or loss of computing equipment, removable media or a physical means of back-up that contains sensitive information from an organisation's database;
- exposure of sensitive information due to human error; 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 providers 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. In 2023 the

PPA issued guidance on the use of IoT devices and smart home environments, which includes the following recommendations:

- inform household members about possible recording by IoT devices;
- use IoT devices cautiously and turn them off when not in use;
- install antivirus software on IoT devices before connecting them to the network;
- review personal data held by smart home providers;
- avoid installing recording devices in private areas;
- limit the use of mobile IoT devices in sensitive areas;
- use strong, unique passwords for smart devices and update them regularly;
- select IoT products from companies that prioritise privacy;
- keep IoT devices updated for enhanced security; and
- minimise the use of remote-control features to protect privacy.

The PPA's recommendation for providers include:

- controlling employee access to data;
- implementing robust user identification measures;
- adopting "Privacy by Design" and "Privacy by Default" practices;
- clearly articulating the purposes of data collection;
- explaining AI operations to facilitate informed consent;
- using collected data solely for its intended and consented purposes; and
- enabling users to access, review, and delete their data.

5.7 Requirements for Secure Software Development

There are no specific references to secure software development in Israeli primary or secondary legislation.

5.8 Reporting Triggers

The common threshold that applies to notification is the "materiality" or "significance" test. For entities 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 Capital Markets Authority, this test examines whether the incident is "significant" for systems with sensitive information, and (i) which were compromised or suspended for more than three hours, or (ii) 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 (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 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.

Employee Email Monitoring

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.

Privacy and Remote Work

In 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.

in 2023, the PPA issued guidelines specifically addressing privacy risks in remote work monitoring. These guidelines highlight concerns such as unauthorised data collection, privacy intrusion, sensitive data exposure, and misuse of personal information. Employers are urged to consider the privacy impact on employees and their families, align monitoring methods with their intended purpose, and refrain from using data for unrelated purposes. Additionally, informing employees about monitoring practices and obtaining their consent are emphasised as critical steps, reinforcing the principle of data minimisation.

In addition, the PPA released a position paper on collecting employees' location data through apps and vehicle tracking, which focuses on the use of technology for performance monitoring by employers, stressing the importance of complying with privacy laws, balancing benefits against privacy rights, and resorting to such methods only when less invasive alternatives are unavailable.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

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

The proposed amendment to the General Security Service Law, 5672-2002, introduces a significant expansion of the ISA's powers, particularly in the areas of intelligence collection and surveillance, including the use of advanced surveillance tools enabling the ISA to covertly access and collect data from various databases in Israel. See **1.1 Laws** for further discussion.

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 down-scale, such liability.

In applicable cases, competent Israeli courts may order the disclosure of cybersecurity information as part of general disclosure proceedings in civil cases.

7.2 Voluntary Information Sharing Opportunities

The NCD operates the Computer Emergency Response Centre (CERT) for cyber-incident management, which can be reached voluntarily in any case where there is a concern about a cybersecurity incident (phishing, DDoS, scraping, etc). The CERT's data security analysts seek to identify threats, assess the damage posed by the threat and to provide a customised first response according to the level of severity, as well as guidance and tools.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation

According to the PPA's latest annual report for 2022, the PPA conducted a total of 317 supervisory cases related to cyber-incidents and 400 sectorial inspections in 2002. A list of enforcement actions for each calendar year is available on the PPA's website.

The PPA has also published several regulatory enforcement proceedings for cybersecurity incidents which took place in 2023, including:

- the unauthorised access to customer information on the Israel Electric Corporation's website;
- a security incident at the Israeli Public Broadcasting Corporation's access control network;
- exposure of sensitive student information by the American Jewish Joint Distribution Committee; and
- a security breach at Israel's Ministry of Transportation's website.

In August 2023, following a data breach at the "Mayanei Hayeshua" Medical Centre, the PPA issued guidelines warning against the misuse of leaked personal medical information. These guidelines prohibit copying, distributing, publishing, transferring, processing, or storing the information, noting that misuse could potentially constitute a criminal offence. The PPA emphasised that even using this information for artificial intelligence training is forbidden. Additionally, it provided advice for affected individuals, such as changing passwords, enabling two-step verification, and being cautious of suspicious communications, to prevent further exposure of sensitive information.

8.2 Significant Audits, Investigations or Penalties

The PPA has established a unit whose focus is broad, sectoral, and topical inspections at organisations that process personal data. The unit is tasked with detecting violations of the PPA and the Regulations, particularly systemic deficiencies, and increasing awareness across the Israeli economy. In 2023, the PPA completed an extensive sector specific audit of 31 hostels and retirement homes, which found low adherence to data security requirements.

The PPA places considerable regulatory attention on data breach incidents. Other PPA enforcement activities have involved violations of duties regarding direct mailing activities and use of databases for purposes inconsistent with their registered purpose, as further explained in **8.1 Regulatory Enforcement or Litigation**.

In August 2023, the PPA identified privacy risks on higher education websites, exposing student information. Key issues involve vulnerabilities, such as the "Listing Directory" in online systems, which allows public access to personal data. The recommended solutions published by the PPA include removing sensitive data from accessible areas, configuring servers to prevent data exposure, and strengthening authentication processes. Additionally, there is an emphasis on educating students and staff about data privacy and secure information handling.

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.

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. For example, some individual lawsuits have asserted violations of privacy principles resulting from social media publications of a person's details or photos (generally in addition to a slander lawsuit).

Another example is a recent regional labour court decision that held that placing CCTV cameras in the vicinity of an employee's work space may be considered as grounds for lawful resignation under Israeli labour laws.

8.5 Class Actions

Class action lawsuits on privacy, data protection and data security are permitted and have been ongoing in courts 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 (including banks, insurance companies and providers of financial services).

The vast majority of 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 September 2023, one of Israel's leading communications providers settled a motion for class action certification following its alleged use of its customers' location data without obtaining lawful consent. In addition to other remedies, the respondent agreed to compensate its customers with benefits worth about ILS3 million.

Another motion for class action certification was filed in 2020 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 and was eventually approved by the court only in March 2023 and included free benefits for the represented group, in addition to an ILS400,000 payment to a state fund.

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 (including such service providers' data security obligations towards the company), 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 the case of cybersecurity events that have occurred, and which are not part of the ordinary course of the business and which present a potentially material impact on the company. The document also demands that cyber-issues be addressed by the company's board of directors.

Following an in-depth audit of cyber-related reports by public companies, held by the Securities Authority in 2022, the Securities Authority has updated its position paper in January 2023, to further expand the adequate disclosure of cyber-risks, including strategy and resources allocated by a company. The document further requires companies to disclose any cyber and data security expertise of board members and the company's management.

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, Artificial Intelligence and Other Cybersecurity Issues

11.1 Further Considerations Regarding Cybersecurity Regulation

In December 2023, the Israeli Ministry of Innovation, Science, and Technology, in partnership with the Legal Counsel and Legislative Affairs Department of the Ministry of Justice, has released a regulatory policy document to guide government ministries and Israeli regulators on AI regulation and ethics.

The document highlights the vital role of responsible AI development in promoting growth, sustainable development, social welfare, and leadership in innovation. It stresses the need for a unified, government-wide regulatory policy on AI to achieve policy objectives, enhance the AI sector, protect fundamental rights and public interests, and minimise risks to technological innovation.

The guidelines aim to strike a balance between legal certainty, the protection of public rights and interests, and the promotion of technological innovation. The guidance for regulators includes:

- tailoring regulation to the risks posed by AI technology, as determined by regulators' risk management assessments;
- operating within sector-specific regulations and avoiding broad legislation in the AI field, considering the diverse applications of AI technology, the limited understanding of its implications, and the rapid pace of technological advancements;
- implementing a regulatory policy that aligns with global regulations and those adopted by international organisations; and
- developing regulation in phases and with flexibility according to technological advancements, using regulatory experiments, sandboxes, and neutral, adaptable tools not bound to any specific system.

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

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