Chambers

GLOBAL PRACTICE GUIDES

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

Cybersecurity

Israel
Haim Ravia, Dotan Hammer and Ariel Amir
Pearl Cohen Zedek Latzer Baratz

practiceguides.chambers.com

2021

ISRAEL

Law and Practice

Contributed by:
Haim Ravia, Dotan Hammer and Ariel Amir
Pearl Cohen Zedek Latzer Baratz see p.13

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**.

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, whose main objective is the prevention of cybersecurity incidents as further described in **3.3 Legal Requirements**.

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 comprise, among others:

- 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;
- 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 materalise into law, but the government reintroduced a revised version of the bill in March 2021. The revised version, now named "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 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.

Data breach notification and incident response requirements are codified in a number of laws and vary depending on the

organisation that suffered from the incident (bank, company, etc) as further described in **3.3 Legal Requirements**.

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". Moreover, the PPA has issued periodic reports indicating a negligible number of breaches notified to the PPA. This suggests that many breaches were unnotified.

The Banking Supervision Department within the Bank of Israel is responsible, among other issues, for enforcing the data breach rules relating to cybersecurity incidents at banks and credit card companies. 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 and financial institutions. 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 deputy commissioner reported that over 20 penetration tests had recently been carried out on 20 different entities to check compliance with the Capital Market Authority's guidelines. 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: (i) initiate administrative enforcement proceedings; or (ii) 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 nature 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.

1.4 Multilateral and Subnational Issues

The matter is not applicable in this jurisdiction.

1.5 Information Sharing Organisations

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**.

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

1.6 System Characteristics

Enforcement

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

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

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 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). For example, the Memorandum of the Protection of Privacy Law (Amendment) (Definitions and Reduction of the Duty to Register), 5724-2020 recently proposed amendments to the PPL, suggesting the adoption of legal terms and definitions found in the GDPR. However, no progress has been made to date in adopting this draft bill into law.

1.7 Key Developments

A proposed amendment to the PPL, which was submitted to the Israeli parliament (the *Knesset*) in 2018 and passed first reading, aimed to grant the PPA much-needed rigorous supervisory and enforcement powers, including a much broader authority to impose penalties. The proposal, despite passing first parliamentary reading, was not significantly promoted since.

As mentioned in **1.6 System Characteristics**, amendments were recently proposed to the PPL, but no progress was made to date in adopting them into law.

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 commercial companies in Israel. One of them was reported in the media, when 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.

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 hot topics to be tackled this year that garnered much public attention in late 2020 was the data security incident at the insurance company Shirbit, as further detailed in **8.2 Significant Audits, Investigations or Penalties**.

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

The Cyber Defence Bill would have broad implications on operators of essential infrastructures, systems or services, including internet and communications service which are considered protectable vital interests. The Cyber Defense Bill would extend to organisations operating essential infrastructures, systems or services, and which are susceptible to activities designed to impair the use of a computer or computer material.

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 NCD is responsible, among other things, to manage, control and carry out the overall, nationwide operational efforts to protect cyberspace as further describes 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 was 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 cyberdefence doctrine; and
- to perform such duties as the Prime Minister may determine, consistent with its designated mission.

In 2018 and 2021, the government published proposals for cyber bills. More details are provided in **1.1 Laws**.

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, among other issues, 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 other financial institutions regarding privacy and cybersecurity, such as the ones detailed in **3.3 Legal Requirements**.

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.

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 who themselves are certified to either ISO 27001 or ISO 27799.

3.2 Consensus or Commonly Applied Framework

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

3.3 Legal Requirements

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

The Data Security Regulations 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 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 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 both of general cybersecurity risks that a company faces as well as of specific incidents having material adverse effects on the company.

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.

3.4 Key Multinational Relationships

The matter is 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, whose main objective is the prevention of incidents. See **3.3 Legal Requirements** 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

The matter is 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 telecom and internet providers, transportation carriers, the Tel Aviv Stock Exchange, the Israeli Internet Association, utility companies and others.

These directives were not publicly disclosed.

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**.

4.5 IoT, 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**.

5. Data Breach Reporting and Notification

5.1 Definition of Data Security Incident or Breach

Under the Data Security Regulations, a potentially reportable data security incident is a "severe security incident" defined as any of the following:

- (1) 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;
- (2) 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;
- exposure of sensitive information following a human error;
- theft or loss of computing equipment, removable media or a physical means of backup that contains sensitive information from an organisation's database;
- 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** 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.

5.7 Reporting Triggers

Under the Data Security Regulations, 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.

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 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's 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 "Risk of Harm" Thresholds or Standards

The common threshold 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" in which systems with sensitive information we 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.

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. We provide some examples 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's 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 pre-requisites 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.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

The data breach notification requirements to regulators, explained in the preceding questions, compel the sharing of certain cybersecurity information with regulators.

The Cyber Defense Bill, mentioned above, proposes to grant powers to the NCD, such as the ability to obtain a court order compelling organisations to take specific actions in response 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 Ministry 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 another instance, an employee of an Israeli offensive cybersecurity company misappropriated the company's offensive cybertools 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 recently completed its investigation of the 2020 data breach in the Elector app, used by two political parties during in February 2020 ahead of the general election. The breach compromised the full electoral register, leading to the unauthorised disclosure of the personal data of more than six million Israeli voters.

The PPA's investigation concluded that the company that develops and operates the app, and the two political parties that used the app, all violated the PPL and the Data Security Regulations in their failure to implement data security measures. The PPL will next determine what fine, if any, to impose on the three organisations.

In 2020, the PPA also launched another criminal investigation against two suspects regarding data protection violations at an undisclosed airline.

A senior flight attendant allegedly gave access credentials to another suspect, who in turn used them to access the airline's flight attendants' database and review the sensitive personal information about the airline's customers. This included information revealing the medical or health condition of customers.

The case was forwarded to the Cyber Department in the State Attorney's Office for review and decision on prosecution.

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.

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. We provide two examples 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.

Following Shirbit's data breach incident explained in the preceding questions, four lawsuits seeking class action certification were filed against Shirbit to date, seeking hundreds of millions of ILS in damages for the representative class.

9. Due Diligence

9.1 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.

9.2 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 will be addressed by the company's board of directors.

10. Other Cybersecurity Issues

10.1 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 & 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 the firm's internet, cyber & 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 & 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 brick-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.

Ariel Amir is an associate in the internet, cyber & copyright group at Pearl Cohen's Tel Aviv office. Ariel's practices include internet and cyber law and privacy and data protection. She counsels client on user agreements, digital (electronic) signatures, copyright issues, open-source matters and other aspects of the law relating to computers, the internet and information technology. Ariel completed her academic degrees (LLB and BA) at the Inter Disciplinary Center, later working as legal counsel and project manager at the Money Laundering Prohibition Authority of Israel.

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