Legal 500
Country Comparative Guides 2025

Israel

Data Protection & Cybersecurity

Contributor

AYR – Amar Reiter Jeanne Shochatovitch & Co

Eyal Roy Sage

Co-founding partner, head of Law & Tech | eyals@ayr.co.il

Shir Shoshany-Katz

Partner | shirs@ayr.co.il

Lior Talmud

Associate | liort@ayr.co.il

Or Rotter Haphiloni

Associate | orr@ayr.co.il

Yuval Achituv

Associate | yuvala@ayr.co.il

Shir Shapira-Perez

Associate | shirsh@ayr.co.il

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Israel.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Israel: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The primary legislation governing privacy, data protection and cybersecurity (in the context of personal data) in Israel is the Privacy Protection Law of 1981. This statute sets out the general provisions regarding the protection of privacy (not just in the context of processing) and personal data processing, both in the public and private sectors.

The data protection regulator is the Privacy Protection Authority, a semi-independent body equipped with broad enforcement powers to ensure compliance with the law.

The statute is supported by several sets of regulations. A key set is the Privacy Protection Regulations (Information Security), 2017, which establish specific data security requirements for the computerized processing of personal information.

The Privacy Protection Regulations (Transfer of Data to Databases Abroad), 2001 govern the export of personal data from Israel.

Additionally, the Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 2023 regulate the use of personal data originating from the European Economic Area. These regulations provide enhanced data minimization and transparency obligations, along with additional data subject rights such as the right to be forgotten, bringing Israeli law closer to the GDPR. These regulations were specifically promulgated to close gaps in Israeli law identified by the EU Commission.

Sector-specific provisions also apply to regulated entities, such as banks and insurance companies, imposing further obligations related to the protection of personal data on entities subject to their regulation.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

Amendment 13 to the Privacy Protection Law will come into effect on August 14, 2025. This is a broad and significant reform that introduces modern and updated definitions for key concepts in the law, such as “personal data”, “processing”, “processor”, “controller” and others. Beyond that, the most notable change is the introduction of extensive enforcement powers for the regulator and significant monetary sanctions.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

Until Amendment 13 enters into force, there is a duty to register most “databases” in the registry of the “Registrar of Databases", who heads to Protection of Privacy Authority. The Authority may suspend the use of a database if it is not properly registered. However, Amendment 13 significantly narrows the scope of the registration obligation, so that most private entities will no longer be required to register their databases. However, controllers of sensitive personal data about more than 100,000 data subjects will be subject to a notification obligation to the regulator.

Registration will continue to apply to public bodies and data brokers. There is no requirement to obtain a certification or a license to be allowed to process personal data, although no processing is allowed in a registrable database which the Registrar refused to register. Breach of the registration obligations can carry administrative and even criminal sanctions.

4. How do the data protection laws in your jurisdiction define “personal data,” “personal information,” “personally identifiable information" or any equivalent term in such

legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

Amendment 13 to the Privacy Protection Law establishes that the term "personal data" is defined as "Data relating to an identified individual or to an identifiable individual; for the purpose of this definition, 'an identifiable individual' means someone who can be identified with reasonable effort, directly or indirectly, including by means of an identifying detail, such as a name, identity number, biometric identifier, location data, online identifier, or one or more details concerning their physical, health, economic, social, or cultural status."

In addition, Amendment 13 defines the term "particularly sensitive data" to include 12 categories such as data regarding sexual orientation, medical information, biometric identifiers, ethnic origin, criminal record, financial activity, and political opinion or religious belief.

In addition, Amendment 13 defines the term "controller" similarly to the GDPR, as the entity who, alone or with others, determines the purposes of processing the data. Israeli law addresses the concept of a "processor" through the definition of the term "holder", which refers to a third party that processes data on behalf of the controller.

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

The core principles of privacy protection in Israel include: the principle of legality, the purpose limitation principle, the obligation to maintain accurate and up-to-date data, the right of access and rectification for data subjects, and data security. Additionally, the processing of personal data is subject to the principles of proportionality and data minimization.

Unlike the GDPR, Israeli law does not establish a concept of legal bases for processing. As a general rule, personal data may be processed if authorized by law, or with the informed explicit or implied consent of the data subject. Arguably, some processing can take place on the basis of notification alone. Moreover, Israeli law provides defences which could be construed to cover GDPR legal bases such as public interest and legitimate interest.

Israeli law also imposes a transparency requirement regarding the processing of personal data. This is reflected in a provision that specifies which details must be provided to the data subject prior to data collection or processing. Furthermore, the principle of data minimization is reflected in documents issued by the Privacy Protection Authority and can be inferred from regulation 2 in the Privacy Protection Regulations (Information Security), 2017, that requires an annual review in order to check whether the data stored in the database exceeds what is required for the database purposes.

6. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Consent and legal authority are the only bases recognized by the regulator, so consent is typically sought in most circumstances. Consent may be implied, but generally, the more sensitive the personal data or the further the processing purpose deviates from the original purpose for which the data was provided, the stronger the form of consent required (i.e., opt-in). In such cases, separate consent—not embedded within general terms and conditions—is preferable. Conversely, for less sensitive processing, lighter forms of consent may suffice. Consent must always be informed.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Israeli data protection law does not prohibit or restrict the processing of any specific category of data. However, the more sensitive the data, the greater the need to

implement enhanced safeguards—such as increased transparency and consent, stronger data security measures, and other appropriate precautions. Prior to the entry into force of Amendment 13 the processing of any category of sensitive data mandated the registration of the database, irrespective of the number of data subjects. Once Amendment 13 enters into force, databases with sensitive data on 100,000 data subjects or more would require notification to the regulator.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Several defences allow the processing of personal data even when such processing is without consent and entails a breach of privacy as defined by law. These defences apply in criminal or civil proceedings, and with the enactment of Amendment 13 to the Privacy Protection Law, they will also apply to administrative proceedings. Defences apply, for example, in cases where the data controller/ processor has a "legitimate personal interest", if they are under a legal, moral, social, or professional obligation to perform the processing, or if there is a public interest in performing this processing. In all cases, processing must be proportionate.

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

Data Protection Impact Assessments are not legally required, although the Privacy Protection Authority strongly recommends conducting such exercises and has published various documents on the subject.

However, Regulation 5(c) of the Privacy Protection Regulations (Information Security), 2017 mandates periodic security risk assessments where the regulations apply the highest security level, which is generally where there are 100,000 data subjects or more or where an organization has 100 employees or more, and sensitive data is processed.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

No.

11. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Yes, under the Privacy Protection Regulations (Information Security), 2017 it is mandatory to prepare a "Database Definition Document" which contains information about processing activities. The Privacy Protection Authority has published a standard template for this document, and an updated version is expected to be released soon in line with Amendment 13 to the law.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

Yes, the Privacy Protection Regulations (Information Security), 2017 require an annual review to determine whether information stored in information systems is no longer needed for the purposes it was collected. There are also regulations concerning the transfer of data to Israel from countries in the European Economic Area – the Privacy Protection Regulations (Instructions for Data Transferred from the European Economic Area), 2023 apply to data transferred from the EEA to Israel (and to all data processed in the same "database" with it, even if not emanating from the EEA) and require not only such an annual review, but also the establishment of an organizational, technical or other timely deletion mechanism. While the Privacy Protection Regulations (Information Security), 2017 do not explicitly require deletion of excess data, the Regulator opined that retaining it creates data security risks which may be a breach of the law.

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

Amendment 13 to the law introduces a mechanism for submitting a pre-ruling request to the Privacy Protection Authority.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

Yes, Amendment 13 establishes a requirement to appoint a Data Protection Officer (DPO) similar to the GDPR. The DPO is responsible for preparing a continuous monitoring program to ensure compliance with the law, verifying its implementation, reporting on it, and proposing remedies for any deficiencies. The DPO must also ensure the existence of a data security procedure within the Database Definition Document, oversee the handling of data subjects' requests, serve as a professional authority and knowledge center within the organization, and advise the organization's management. In addition, the DPO must prepare a training program, supervise its execution, and serve as the point of contact with the Privacy Protection Authority.

Certain entities are required to appoint an Information Security Officer, including banks, insurance companies, public bodies, and larger processors. The Information Security Officer is responsible for the security of personal data in databases held by the organization. The Privacy Protection Regulations (Information Security), 2017 list further duties of the Information Security Officers and a prohibition on a conflict of interests and also applies to CISOs appointed voluntarily.

15. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

The Privacy Protection Regulations (Information Security), 2017 mandate employee training to be conducted both prior to assuming a position and on a periodic basis (at least once every two years).

16. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Yes. Notice is required when collecting personal information directly from data subjects, and if the Privacy Protection Regulations (Instructions for Data Transferred from the European Economic Area), 2023 apply, also when data is collected indirectly. Data subjects must be informed whether they are legally required to provide personal information or doing so is voluntary, the consequences of not providing the information, the purposes for which the information will be used, to whom the information will be transferred and for what purposes, the name of the data controller and how to contact it, as well as the individual's right to access and correct their information.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

The primary obligations under Israeli law apply to data controllers (for example, the duty to inform is generally interpreted as applying to the controller and not to the processor). However, under the Privacy Protection Regulations (Information Security), 2017, the obligations imposed on controllers also apply to processors, with the necessary adjustments.

18. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

Monitoring, automated decision-making and profiling are subject to the same framework as any other processing. However, data subjects always have a right to opt out of direct marketing based on profiling, and sale or transfer of profiled personal data requires opt-in consent.

Moreover, the regulator and Attorney-General have opined that profiling which is not tied to the original purpose for which personal data was collected also requires opt-in consent.

Israel has no specific provisions on cookies and similar tracking technologies, but general data protection law applies and there are several pending class actions alleging that the use of cookies requires opt-in consent.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How

are these terms or any similar terms defined?

The Privacy Protection Law gives data subjects a right to opt out of "Direct Mailing", which is defined as "contacting a person personally, based on his belonging to a group of the population that is determined by one or more characteristics of persons whose names are included in a database".

However, direct mailing services, which are defined as "providing Direct Mailing services to others by way of transferring lists, labels or data by any means" are opt-in.

There are no specific provisions about behavioural advertising. However, a person's behaviour in private entails heightened data security requirements pursuant to the Privacy Protection Regulations (Information Security), 2017.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

Direct mailing services are defined as "providing Direct Mailing services to others by way of transferring lists, labels or data by any means". The definition applies irrespective of any consideration. Such services require opt-in consent.

Amendment 13 also refers to databases the main purpose of which is "the collection of personal data for transfer to another by way of business or for consideration, including Direct Mailing Services". Such databases must be registered.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

The Consumer Protection Law, 1981 imposes restrictions on human marketing phone calls (these are only permitted with explicit consent and only if the recipient is not listed in the "Do Not Call" registry).

In addition, The Communications (Telecommunications and Broadcasting) Law, 1982 regulates the sending of advertising text messages and emails, and requires explicit consent for such communications unless specific conditions are met that allow sending on the basis of prior relationship and an opt-out option.

This Communications Law also sets formal requirements regarding the format and presentation of advertisements sent through these means.

As for direct marketing, as mentioned above, Israeli privacy law allows it on an opt-out basis and includes both formatting requirements for such mailings and a right to be removed from distribution lists.

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

The Protection of Privacy Law defines "biometric identifier" as "biometric data which is used for the identification of a person or for authenticating his identity, or biometric means from which such data can be extracted". The term "biometric" is defined as a "a unique personal, physiological or behavioural characteristic, which is capable of computerised measurement."

Personal information which is a biometric identifier used or designed for use for the computerised identification or authentication of the identity of a person" is considered a personal information of special sensitivity.

Biometric data also requires enhanced security measures pursuant to the Privacy Protection Regulations (Information Security), 2017.

The use of biometrics in identity documents is governed by a specific statute, and government use of biometric applications is the subject of a 2012 government decision. The National Cyber Directorate encompasses a Supervisor of Biometric Applications, whose mandate specifically centers on biometric data and its regulation.

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

There are no laws addressing AI, but various government bodies have published policy papers. The Privacy Protection Authority is said to work on guidelines. A draft policy concerning the use of AI in the financial sector seems to suggest the use of personal information for training purposes requires consent.

24. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically

comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Privacy Protection Regulations (Transfer of Data to Databases Outside the Borders of the State), 2001 requires that personal data be exported only to jurisdictions offering adequate protection, or pursuant to several derogations. The Protection of Privacy Authority opined that jurisdictions complying with the General Data Protection Regulation (GDPR) are considered as affording an adequate level of protection under Israeli law. Derogations include, among other things, exports with the data subject's consent, to data importers in a signatory country of Treaty 108 or when the data importer was bound by an agreement to apply the same requirements as required under the Israeli law to the personal data that is transferred. Exports to the EU and jurisdictions deemed adequate by the EU are also allowed.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

Israeli data protection laws impose specific data security obligations on controllers and processors, primarily through the Privacy Protection Regulations (Information Security), 2017. These regulations set out mandatory security measures based on the sensitivity of the database and the nature of the organization.

Depending on the sensitivity of the information, the amount of data and the size of the organization, measures include organizational mechanisms such as policies and employee training, detailed access control policies which must be reviewed periodically, the use of encryption in transit, incident management procedures, including reporting obligations, protections for physical and logical infrastructure, regular backups of logs, and periodic audits and risk assessments.

In addition, the Israeli Privacy Protection Authority publishes guidelines to assist with compliance, and the National Cyber Directorate periodically issues recommendations and best practices for Information security.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Pursuant to Section 11 of the Privacy Protection Regulations (Information Security), 2017, controllers and processors must document security incidents and must report "severe security incidents" to the Privacy Protection Authority. Security incidents are defined as unauthorized use or harm to data integrity. Incidents are considered severe if they affect a high-security level database or a substantial part of a medium-security level database.

A security incident occurs in a high-security level database if there is unauthorized use of the data, use exceeding authorization, or a compromise of data integrity. In the case of a medium-security-level database, a security incident occurs if a substantial part of the database is used without authorization, used in excess of authorization, or if the integrity of a substantial part of the data is compromised.

The Privacy Protection Authority may, in consultation with the National Cyber Directorate, order the controller to notify affected data subjects.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

Under Section 13 of the Privacy Protection Law, individuals may access personal data held about them, subject to certain exceptions such as harm to health, legal privilege, or national security.

Section 14 grants data subjects the right to request the rectification of inaccurate, incomplete, or outdated data. If the request is accepted, the data must be updated and relevant recipients notified; if rejected, the individual must be informed accordingly. Data subject also have a right to delete inaccurate information about them if the controller refuses to rectify it.

Additionally, Israeli law provides a limited right of erasure, for example in cases where the personal data is used for direct marketing. These rights are generally exercised through a written request to the data controller.

Under the Privacy Protection Regulations (Instructions for Data Transferred from the European Economic Area), 2023, which apply to data transferred from the EEA to Israel (and to all data processed in the same "database" with it, even if not emanating from the EEA), data controllers are required — subject to certain exceptions — to erase or anonymize personal data that is no longer necessary for the purposes for which it was collected, received, or stored.

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Yes, Israeli data protection law provides individuals with a private right of action. Under Section 4 of the Privacy Protection Law, a violation of privacy is considered a civil tort, allowing individuals to bring personal claims in court. A common cause of action relates to the breach of the purpose limitation principle without consent. Class actions are available if the breach is in a consumer setting.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

Yes, individuals are entitled to monetary compensation under Israeli data protection law if their privacy has been violated. A violation of privacy is considered a civil tort under Section 4 of the Privacy Protection Law, enabling individuals to file personal claims in court. In addition, under Section 29A of the Privacy Protection Law, the court may award statutory damages of up to NIS 50,000 without the need to prove actual harm. This means that non-material harm, such as emotional distress or injury to feelings, may be sufficient for compensation. This applies to certain types of privacy violations such as unauthorized use or disclosure of personal information, or the publication of a person's photograph in a manner that may humiliate or degrade them. In such cases, non-material harm such as emotional distress or injury to dignity may be sufficient for awarding compensation.

In addition, under Section 15A(a), courts may award statutory damages of up to NIS 10,000 in specific cases—such as failure to register a database, denial of access rights, or failure to correct or delete inaccurate data.

In addition, under Section 30A(i) of the Communications Law (Telecommunications and Broadcasting), 1982, courts may award statutory damages of up to NIS 1,000 per message sent in violation of the anti-spam provisions — even without proof of harm.

In practice, Israeli courts often award statutory compensation ranging between NIS 50–100 per message, depending on the circumstances.

While the law does not require proof of material damage in these cases, Israeli courts have also recognized compensation for non-material harm, such as emotional distress.

Thus, both statutory damages without proof of harm and compensation for proven emotional injury are available under Israeli law.

30. How are data protection laws in your jurisdiction typically enforced?

The Privacy Protection Authority has broad investigative and enforcement powers. Following Amendment 13, which will enter into force on August 14th, 2025, the Privacy Protection Authority can appoint investigators with authority to question individuals, seize evidence, and request court warrants. The Authority can also impose significant administrative fines for violations, including unauthorized processing and failure to protect data. A formal process includes a warning, the right to respond, and a final decision. Repeat or ongoing violations lead to higher penalties. Some breaches can carry criminal penalties, including imprisonment.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

Under Amendment 13 of the Israeli Privacy Protection Law, the range of administrative fines that may be imposed for data protection violations spans from 15,000 NIS for minor breaches (such as denying access to personal data), to 150,000–300,000 NIS for more severe infractions (such as unlawful data processing or operating unregistered databases). Additionally, certain violations are subject to per-person-based fines—ranging from NIS 2 to 8 per individual, depending on the sensitivity of the data and the nature of the breach. These amounts may be doubled in cases involving databases containing information on over 1,000,000 individuals or in

instances of repeated or ongoing violations, making the potential total sanction reach millions. There is a cap of 5% of the domestic annual revenue.

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

No.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, enforcement decisions by the Israeli Privacy Protection Authority are subject to appeal. According to Amendment 13 of the Privacy Protection Law, the recipient of a notice of intent to impose a monetary sanction has the right to present their arguments, either in writing or orally, within 45 days. If the authority subsequently imposes a monetary sanction, there is a right of appeal to the Magistrate's Court within 45 days of receiving the payment demand. The court has the authority to uphold, modify, or cancel the decision, or to return the matter to the head of the authority with specific instructions. Additionally, if an appeal is filed, the violation is not considered a breach until the court issues a ruling.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

In recent years, there has been an increase in sector-wide audits. A significant increase in enforcement activity is expected with the entry into force of Amendment 13 of the Privacy Protection Law, given the significant new powers the regulator will have.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

Yes. The Privacy Protection Regulations (Information Security), 2017 require organisations that process personal data to implement specific security measures. These requirements apply in accordance with the sensitivity of the data held in the database. Amendment 13 defines the term “particularly sensitive data” to include 12 categories such as data regarding sexual orientation, medical information, biometric identifiers, ethnic origin, criminal record, financial activity, and political opinion or religious belief.

In addition, sectoral obligations apply to regulated industries, including the financial sector, transportation, telecommunications, critical infrastructure, and other key sectors. Furthermore, certain organisations are subject to specific, detailed, and confidential instructions issued by the Internal Security Service or the Israel National Cyber Directorate.

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

There are no general requirements. However, the Privacy Protection Regulations (Information Security), 2017 impose certain organizational obligations on the use of processors, and many sector regulators impose specific supply chain requirements. For example, the Bank of Israel has issued specific and highly detailed directives on supply chain management. The Capital Market, Insurance and Savings Authority has also issued binding guidelines.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

Yes. The Privacy Protection Regulations (Information Security), 2017 require both controllers and processors to notify the Protection of Privacy Authority without undue delay (and no later than 72 hours) of any ‘serious security incident'. While there is no automatic requirement to inform affected individuals (although doing so may be advisable for damage mitigation purposes), the Registrar of Databases can, in consultation with the head of the National Cyber Defence Authority, require that data subjects be notified.

The above applies to databases that are subject to the high and medium security levels in the regulation. In addition to the general law, specific obligations from sectoral regulators require supervised bodies to notify of incidents (e.g., the Bank of Israel, Capital Market Authority, Insurance and Savings Authority, Israel Securities Authority).

Israel does not impose a general legal obligation on organizations to share cybersecurity-related information. However, sector-specific regulations promote such sharing in practice.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

The Israeli Protection of Privacy Law requires the appointment of a Chief Information Security Officer (CISO) for both controllers and processors when, among other things:

- The organization owns or controls five or more databases that are subject to registration or notification under Section 8A of the Privacy Protection Law.
- The organization is a public body, as defined in Section 23 of the Privacy Protection Law.
- The organization is a bank, insurance company, or a credit rating or assessment company.

The Privacy Protection Regulations (Information Security), 2017 require that the CISO report to a senior manager, prepare a security policy, develop and implement a continuous monitoring plan, report on its findings, be provided with the necessary resources to fulfil his duties, and avoid any potential conflicts of interest. This requirement applies also where a CISO has been appointed voluntarily or by virtue of other regulations. Several sector-specific regulations require the appointment of a CISO, including in the banking and insurance industries.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

Yes, sector-specific regulators in Israel have issued sectoral cybersecurity guidelines. For example, such guidelines have been issued by the Bank of Israel, the Capital Market, Insurance and Savings Authority, the Israel Securities Authority, the Ministry of Health, and the Ministry of Communications.

40. What impact do international cybersecurity standards have on local laws and regulations?

Yes, to some extent. While the Privacy Protection Regulations (Information Security), 2017 set out the core legal requirements for database security in Israel, the ISO 27001 and PCI-DSS certifications are common. This indicates that although not mandated by law, international cybersecurity standards are widely used in practice, particularly in regulated industries such as finance, telecommunications, transportation, and critical infrastructure.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Other than pursuant to the Privacy Protection Regulations (Information Security), 2017 and as regards incidents affection personal data, there is no general obligation to report cybersecurity incidents. However, several sectors are subject to specific obligations, including the banking, insurance, telecommunications and healthcare sector.

For example, in Proper Banking Management Directive No. 364, an information security event is defined as an event where information security was compromised or had the potential to be compromised, including a cyberattack. Banking corporations are required to report technological failure events and information security incidents to the banking supervisor when there is potential for significant negative impact on critical and sensitive information assets, and the report is also made to senior management and the board of directors.

In the financial sector, the Capital Market Authority circulars require regulated entities to immediately report significant cyber incidents or technological failures, especially when there is an impact on functional continuity or exposure of sensitive information. The circulars include detailed instructions regarding the reporting method, appointment of a cyber officer, conducting periodic drills, and implementing control and recovery mechanisms.

Additionally, Telecommunications Regulations (Telecommunications and Broadcasting) (Licensee's Reporting of a special event), 2020 require operators to report special events to the manager via SMS or other online communication means, and to provide initial and

final reports, accordingly, detailing the affected service, the number of affected subscribers, and the estimated time to resolve the event.

42. How are cybersecurity laws in your jurisdiction typically enforced?

The Privacy Protection Authority has investigative powers and enforces the law and its regulations through measures such as issuing orders to suspend the processing of databases or imposing fines. Starting from the entry into force of Amendment 13, the Authority's enforcement powers will be significantly expanded, and the monetary sanctions will be considerably higher. In addition, the courts also play a role in enforcing data protection laws, including through civil lawsuits that may be filed, including class actions. Sectoral regulators including the Banking Supervision Department (Bank of Israel), the Ministry of Communications, the Capital Market, Insurance and Savings Authority, the Israel Securities Authority, and the Privacy Protection Authority have wide reached powers to issue orders. Regulators may also impose significant fines and even suspend operating licences.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

The Protection of Privacy Authority has sweeping powers which include search and seizure, demand to provide documents and provide information, and order to stop processing. These powers extend to Privacy Protection Regulations (Information Security), 2017.

In addition, sectoral regulators—such as the Bank of Israel, the Capital Market Authority, the Insurance and Savings Authority, and the Israel Securities Authority—mandate that supervised entities implement cybersecurity measures, including report security incidents, and they have investigative powers.

The Public Bodies Security Arrangement Law, 1998, which also applies to economically significant private organizations makes such organizations subject to cybersecurity directives from the Israel National Cyber Directorate or the General Security Service (aka Shin Bet), depending on their sector or sensitivity.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

In Israel, there is currently no overarching cybersecurity legislation. Instead, cybersecurity-related obligations and sanctions are governed through sector-specific regulations and broader legislative frameworks. For example, under the Banking Ordinance, 1941, the Supervisor of Banks may impose monetary sanctions for violations of proper banking conduct. In addition, the Communications Law (Telecommunications and Broadcasting), 1982 allows the Ministry of Communications to impose administrative fines for breaches of license terms, including cybersecurity-related failures. Similarly, under the Supervision of Financial Services (Regulated Financial Services) Law, 2016, financial service providers may be subject to financial penalties for non-compliance with information security and cyber risk management obligations. Although regulatory circulars in these sectors impose detailed cyber-related duties, the actual range of sanctions stems from the general statutory powers to enforce compliance.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

No.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, enforcement decisions by the Israeli Privacy Protection Authority are subject to appeal. According to Amendment 13 to the Privacy Protection Law, an individual who receives a notice of intent to impose a monetary sanction has the right to present their arguments, either in writing or orally, within 45 days. If the authority subsequently imposes a monetary sanction, the individual may appeal the decision to the Magistrate's Court within 45 days of receiving the payment demand. The court has the authority to uphold, modify, or cancel the decision, or to return the matter to the head of the authority with specific instructions. Additionally, if an appeal is filed, the violation is not considered a breach until the court issues a ruling.

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your

jurisdiction?

In addition to increased data security enforcement pursuant to the Privacy Protection Regulations (Information Security), 2017, sectoral regulators have been revising their data security requirements. Among other things, the Bank of Israel has significantly broadened the scope of its supply chain security requirements, affecting wide swathes of suppliers of the banking sector.

Contributors

Eyal Roy Sage
Co-founding partner, head of Law & Tech
eyals@ayr.co.il

Shir Shoshany-Katz
Partner
shirs@ayr.co.il

Lior Talmud
Associate
liort@ayr.co.il

Or Rotter Haphiloni
Associate
orr@ayr.co.il

Yuval Achituv
Associate
yuvala@ayr.co.il

Shir Shapira-Perez
Associate
shirsh@ayr.co.il

