Information Security Considerations (Israel)

by Yuval Horn, Orly Sternfeld, Maya Weiss-Donin, and Shira Brami, Horn & Co., Law Offices, with Practical Law Data Privacy Advisor

Law stated as at 22 May 2019 • Israel

A Practice Note describing the laws, regulations, enforcement practices, and local resources to consider when developing, implementing, and maintaining an information security program in Israel or as applied to data originating from Israel. This Note also addresses the Protection of Privacy Law, 5741-1981, the Protection of Privacy Regulations (Data Security), 5777-2017, sector-specific obligations, and cybersecurity industry standards, including those from the Israel National Cyber Directorate (INCD). The Israel-specific guidance in this Note may be used with the generally applicable resources listed in the Global Information Security Toolkit.

Contents

Information security programs protect the confidentiality, integrity, and availability of data and information technology (IT) assets. However, differences in local data security laws, practices, and standards create challenges for global companies, and failure to comply with them can result in enforcement action and litigation. This Note explains the Israeli laws, regulations, enforcement practices, and local resources to consider when developing, implementing, and maintaining an information security program in Israel or as applied to personal data originating from Israel. The Israel-specific guidance in this Note may be used with the generally applicable resources listed in the Global Information Security Toolkit.

Information Security Laws and Regulations

Several Israel laws regulate information security and set related standards, including:

- The Basic Law: Human Dignity and Liberty, 5752-1992 (unofficial translation), which has constitutional value in the Israeli legal system and provides individuals with a right to privacy and intimacy.

- The Protection of Privacy Law, 5741-1981 (unofficial translation) (PPL) and Protection of Privacy Regulations (Data Security), 5777-2017 (unofficial translation) (Security Regulations), implemented under Section 36 of the PPL, which protect personal information.
- Sector-specific laws and regulations that impose further obligations for areas that typically carry specific information security risks, including financial services and health (see Sector-Specific Laws and Regulations).
- The Regulation of Security in Public Bodies Law, 5758-1998, which protects the critical computer systems of various public, government, and private bodies (see Critical Computer Systems Protection).

Protection of Privacy Law and Security Regulations

The PPL protects personal information and imposes data security obligations on:

- Database owners and managers, which the related Security Regulations also usually refer to as database controllers. This Note uses the term database controller collectively unless context requires otherwise.
- Certain organizations, including banks and insurance-related companies (Section 17B, PPL).
- Public entities, including:
  - government departments, state institutions, local authorities, and others carrying out public functions; and
  - Minister of Justice designees if Knesset-approved orders prescribe the categories and data items the designee handles.

- (Section 23, PPL.)

For more information on the PPL's general requirements, see Country Q&A, Data protection in Israel: overview.

The PPL uses general terms to refer to personal information, defining:

- Information as data regarding a person's:
  - personality;
  - personal status;
  - intimate affairs;
  - state of health;
  - economic position;
  - vocational qualifications; or
  - opinions and beliefs.
- Sensitive information as:
  - data on a person's personality, intimate affairs, state of health, economic position, or opinions and beliefs; or
  - information the Minister of Justice classifies as sensitive with Knesset approval.
- Database as a data collection impliedly containing personal information and intended for computer processing unless:
  - the collection is for personal, non-business purposes only; or
  - the database controller does not hold other databases and the collection includes only name, address, and communication method and does not infringe on individuals' privacy.

(Section 7, PPL.)

The Israeli Supreme Court interprets information broadly, despite the PPL's enumerated categories, according to the law's legislative purpose (CA 86/89 *State of Israel v. Bank Hapoalim BM* 24(2) PD 726 (1990)). For example, in *Database Registrar v. Ventura*, the Supreme Court held that information includes an individual's:

- Address.
- Telephone number.
- Bank account number.

- National identification number.

(CA 439/88 *Database Registrar v. Ventura* 48(3) PD 808 (1994).)

The PPL extends the definition of information to potentially encompass any data regarding individuals' private affairs when public entities collect or receive it (Section 23A, PPL).

The Minister of Justice lists several categories of public entities and the personal information they can receive, including:

- Hospitals.
- Health maintenance organizations.
- The Israeli Defense Force Disabled Veterans Organization.
- Other entities.

(Protection of Privacy Order (Determination of Public Entities), 5746-1986 (in Hebrew).)

Protecting Personal Information Under the PPL and Security Regulations

Database controllers are responsible for maintaining information security (Section 17, PPL). The Security Regulations prescribe specific information security measures for databases according to:

- The nature and sensitivity of the data that they store.
- The number of affected data subjects.
- The database controller's purposes for collecting and using the data.

The simplest requirements apply to individually controlled databases, while an escalating set of security classifications and requirements further apply to organizations, including public and private entities, and their databases. Database controllers must secure databases according to the applicable security level (Regulation 19, Security Regulations). Some database controllers must also appoint a data security officer (see Data Security Officer).

Individually controlled databases:

- Include databases that:
  - an individual or individually owned corporation manages; and
  - only the individual and no more than two additional authorized users access and use.
- Exclude databases, treating them as if an organization controls them, if:
  - their main purpose is to collect and transfer data to a third party for business purposes, such as direct mailing;
  - they contain information on 10,000 or more individuals; or
  - the database controller has a professional duty of confidentiality by law or professional ethics principles regarding the data.

(Regulation 1, Security Regulations.)

For detailed security requirements that apply to individually controlled databases, see Individually Controlled Database Security Requirements.

Organizations' databases fall into three classifications with corresponding and increasingly stringent security requirements, which are:

- Basic security level databases, which are those databases that do not meet the criteria for any of the other classifications (see Basic Level Database Security Requirements).

- Medium security level databases, which are generally the most typical type for companies that collect and process personal information, according to various criteria (see Medium Level Database Security Requirements).
- High security level databases, which are medium level security databases that also:
  - contain information on 100,000 or more individuals; or
  - permit access and use for more than 100 authorized users.

- (See High Level Database Security Requirements.)

(Regulation 1, First Schedule, and Second Schedule, Security Regulations.)

Medium security level databases include databases if:

- Their main purpose is to collect and transfer data to a third party for business purposes, such as direct mailing.
- A public entity controls them.
- They contain information regarding an individual's:
  - intimate life, including conduct in the private domain;
  - health or mental condition;
  - genetic data defined under Section 35 of the Genetic Information Law, 5761-2000 (unofficial translation);
  - political opinions or religious beliefs;
  - criminal records;
  - contact information, such as name, identification or company number, address, or phone number, as defined under the Criminal Procedure (Enforcement Authorities – Telecommunications Data) Law, 5768-2007 (in Hebrew);
  - biometrics data;
  - financial information, including assets, debts, liabilities, and creditworthiness; or
  - consumption habits denoting these data or regarding the individual's personality, beliefs, or opinions.

A database that might otherwise qualify is **not** medium level if it:

- Supports no more than ten authorized users.
- Contains only employee or supplier facial photos that the database controller uses for business management purposes, such as identification badges.

(Regulation 1 and First Schedule, Security Regulations.)

The Privacy Protection Authority (PPA) Complete Guide to the Security Regulations (in Hebrew):

- Explains the Security Regulations' requirements.
- Sets out criteria for determining the appropriate database classification.
- Indicates which regulations apply to each security level.

Database controllers must register a database in the government's online registry (in Hebrew) if:

- The database contains:
  - information on 10,000 or more persons;
  - sensitive information; or
  - information not delivered by affected individuals, on their behalf, or with their consent, such as third-party collected data.
- The database belongs to a public body.
- They use the database for direct mailing services.
- The Registrar of Databases (Registrar) orders registration, even if the database is otherwise exempt.

(Section 8(c)-(e), PPL.)

Individually Controlled Database Security Requirements

Database controllers of individually controlled databases must:

- Create a Database Definitions Document that at minimum:
  - provides a general description of the database;
  - explains the database's use purposes;
  - lists any data elements contained in the medium security level criteria (see Protecting Personal Information Under the PPL and Security Regulations);
  - details any cross-border transfers, including the purpose and manner of transfer, destination country, recipient, and data uses outside Israel;
  - describes any data processor activities, such as third-party service providers;
  - explains the main database information security risks and how the controller manages them; and
  - names the database manager, database processor, and data security officer, if appointed.

- (Regulation 2(a), Security Regulations.)
- Update the Database Definitions Document whenever there is a significant change (Regulation 2(b), Security Regulations).
- Annually assess whether:
  - the Database Definitions Document requires any additional updates due to technology changes in the organization or security incidents; and
  - the data stored exceeds what is required for the database's purposes.

- (Regulation 2(b), (c), Security Regulations.)
- Maintain physical security measures suitable for:
  - the nature of the database's activities; and
  - the sensitivity of the information.

- (Regulation 6(a), Security Regulations.)
- Implement appropriate access control measures (Regulation 9(a), Security Regulations).
- Document any security incident involving a breach of data integrity or unauthorized data use (Regulations 11(a), Security Regulations).
- Control the use of mobile devices by:
  - limiting or denying their use according to data sensitivity and risks; and
  - using reasonable protective measures, such as encryption, when permitting them.

- (Regulation 12, Security Regulations.)
- Manage and operate the database system according to commonly accepted standards, including:
  - segmenting the database from other systems;
  - regularly updating the database system; and
  - not using unsupported vendor components unless appropriate security measures are available.

- (Regulation 13, Security Regulations.)
- Install appropriate safeguards against unauthorized penetration or malicious software (malware) before connecting the database system to the internet or another public network (Regulation 14(a), Security Regulations).
- Ensure that data transfers over the internet or other public networks use commonly accepted encryption methods (Regulation 14(b), Security Regulations).
- Install identity verification measures for remotely accessible databases (Regulation 14(c), Security Regulations).

Basic Level Database Security Requirements

Database controllers of basic security level databases must:

- Meet the security requirements applicable to individually controlled databases (see Individually Controlled Database Security Requirements).
- Implement and annually assess the need to update a written data security procedure that at minimum includes:
  - physical security measures to protect database sites and their surroundings;
  - role-based access authorizations to the database and database systems;
  - intended safeguards and implementation plans;
  - security training for authorized users;
  - known information security risks and how the database controller identifies and manages them, including encryption measures;
  - incident response planning according to incident severity and information sensitivity; and
  - instructions on managing and using mobile devices.

- (Regulations 4(a)-(e) and 11(b), Security Regulations.)
- Maintain a document of the database's current structure and systems inventory, available only to authorized users who require access to perform their roles, that includes:
  - infrastructure and hardware elements, communication types, and data security components;
  - any software the database controller uses to operate, administer, and maintain the database, support its activities, and monitor and secure it;
  - communication software and interfaces;
  - a network diagram, including system component interfaces and physical locations; and
  - the document's most recent revision history.

- (Regulation 5(a), Security Regulations.)
- Implement reasonable personnel screening measures for authorized users according to data sensitivity and access levels (Regulation 7(a), Security Regulations).
- Train authorized users on their obligations under the PPL, the Security Regulations, and the database controller's procedure before granting access or changing the scope of access (Regulation 7(b), Security Regulations).
- Implement role-based access according to authorized users' roles in the organization (Regulation 8(a), Security Regulations).
- Maintain a current list of roles, role-based authorizations, and authorized users performing those roles and retain that list for 24 months (Regulations 8(b) and 17(a), Security Regulations).
- Perform pre-engagement due diligence to assess information security risks before entering into agreements with external service providers that access the database (Regulation 15(a)(1), Security Regulations).
- Expressly agree with external service providers, considering identified data security risks, to:
  - restrict the data the provider can access and process, the types of processing, and the purposes for processing;
  - limit the agreement's duration and define mechanisms for returning or destroying personal information on completion, including certification of the actions taken;
  - require safeguards consistent with the Security Regulations and database controller standards;
  - obligate the providers' authorized users to sign a confidentiality agreement, including commitments to follow the overall agreement and support established safeguards;
  - require the provider to execute similar terms with any downstream service providers;
  - notify the database controller of any security incidents; and
  - report to the database controller at least annually on its compliance with the agreement.

- (Regulation 15(a)(2), Security Regulations.)
- Include service provider oversight and management in its written procedure and retain that procedure for 24 months (Regulations 15(a)(3), (4) and 17(a), Security Regulations).

Database controllers of multiple same security level databases may prepare a single written data security procedure, structure and systems inventory, and agreement with external service providers for those databases (Regulations 4(f), 5(e), and 15(b), Security Regulations).

Medium Level Database Security Requirements

Database controllers of medium security level databases must:

- Meet the security requirements applicable to:
  - individually controlled databases (see Individually Controlled Database Security Requirements); and
  - basic security level databases (see Basic Level Database Security Requirements).
- Include in their written procedure:
  - identification and verification measures for managing authorized users' access to the database and database systems, including password requirements and how they handle automated disconnections and authentication failures;
  - how they monitor database use; and
  - instructions for conducting periodic security audits, performing data backups, and managing database development activities.

- (Regulations 4(d) and 9(b)(2), Security Regulations.)
- Monitor and document access to and equipment movement in their facilities, retaining and backing up records for 24 months (Regulations 6(b) and 17, Security Regulations).
- Provide training on the Database Definitions Document, the written procedure, and their data security obligations under the PPL and Security Regulations to:
  - existing authorized users at least once every two years; and
  - newly authorized users as soon as possible.

- (Regulation 7(c), Security Regulations.)
- Identify authorized users by physical means, to the extent feasible, such as a keycard (Regulation 9(b)(1), Security Regulations).
- Monitor database system access using automated logging that captures, at minimum:
  - user identity;
  - the date and time of any access attempt;
  - access type and scope; and
  - whether access was granted or denied.

- (Regulation 10(a), Security Regulations.)
- Manage their automated logging by:
  - informing authorized users of their logging activities;
  - if possible, not allowing logging to be deactivated or modified;
  - detecting and alerting on any attempts at deactivation or modification;
  - establishing an ongoing procedure to monitor and report on logging results and steps taken; and
  - retaining logging records for at least 24 months.

- (Regulations 10(b)-(e) and 17(a), Security Regulations.)
- Hold internal discussions about data security incidents at least annually and update their written procedure, as applicable (Regulation 11(c), Security Regulations).
- Notify authorities immediately of severe security incidents (Regulation 11(d), Security Regulations; see Cyber Incident Response and Data Breach Notification).
- Use physical means in the authorized users' exclusive control, such as multifactor authentication methods, to verify their identity for remotely accessing databases (Regulation 14(c), Security Regulations).
- Maintain procedures for routine data backup and restoration (Regulation 18(a), Security Regulations).
- Conduct an internal or external audit using a third-party data security auditor at least once every 24 months (Regulation 16(a), Security Regulations).

High Level Database Security Requirements

Database controllers of high security level databases must:

- Meet the security requirements applicable to:
  - individually controlled databases (see Individually Controlled Database Security Requirements);
  - basic security level databases (see Basic Level Database Security Requirements); and
  - medium security level databases (see Medium Level Database Security Requirements).
- Conduct at least once every 18 months and act on the findings of:
  - a data security risk assessment; and
  - an internal and external penetration test.

- (Regulation 5(c), (d), Security Regulations.)
- Hold internal discussions about data security incidents at least quarterly and update their written procedure, as applicable (Regulation 11(c), Security Regulations).
- Retain copies of data backups and procedures to ensure the organization's ability to restore the database if loss or destruction occurs (Regulation 18(b), Security Regulations).

Database controllers of multiple high security level databases may conduct a single risk assessment or penetration test for those databases (Regulation 5(e), Security Regulations).

Data Destruction Under the PPL and Security Regulations

The PPL and Security Regulations do not explicitly address general data destruction requirements for database controllers. Controllers should maintain a consistent data retention and disposal schedule to limit their cybersecurity risks by minimizing the amount of data they must secure.

Sector-Specific Laws and Regulations

Israel imposes additional information security requirements in some sectors, such as concerning:

- Financial services (see Banks, Credit Data, and Insurance Companies).
- Healthcare (see Health Data).
- Biometrics (see Biometrics Data).

Banks

The Bank of Israel has issued several directives regarding data security for banking corporations. These directives generally apply to any:

- Banking corporation, defined by the Banking (Licensing) Law, 5741-1981 (unofficial translation) (Banking Law).
- Organization under a banking corporation's direct or indirect control (Sections 11(a)(3a), (3b) and 11(b), Banking Law).

Proper Conduct of Banking Business Directive 361 on Cyber Defense Management (03/15) (unofficial translation) (Directive 361) sets out various specific cyber defense management obligations, including requiring banks to:

- Create an effective cyber risk management framework (Section 14, Directive 361).
- Set and approve a corporate-wide cyber defense strategy, risk management framework, and defense policy and receive reports on significant cyber incidents (Section 15, Directive 361).
- Appoint a qualified senior executive as a chief cyber defense officer to fulfill specified duties (Section 17, Directive 361).

- Conduct yearly assessments of cyber risks and controls that:
  - identify risks;
  - assess the control environment's effectiveness; and
  - determine residual risks.

- (Section 35, Directive 361.)
- Establish a dynamic proactive cyber defense program by:
  - mapping their environment;
  - researching threats and making predictions;
  - developing rapid response capabilities; and
  - retaining evidence from cyber incidents.

- (Section 55, Directive 361.)

The Supervisor of Banks adopted Proper Conduct of Banking Business Directive 357 on Information Technology Management (07/16) (unofficial translation) (Directive 357) to comply with e-banking principles published by the International Committee on Bank Supervision in July 2003. Directive 357 sets out general information technology requirements, including information security obligations requiring banks to:

- Adopt and enforce IT security, backup, continuity, and control protocols (Section 5, Directive 357).
- Document their current IT systems (Section 6(a), Directive 357).
- Log access, transactions, and queries (Section 6(b)(1), Directive 357).
- Conduct internal IT audits (Section 7(a), Directive 357).
- Perform IT system risk assessments and act on findings (Section 8, Directive 357).
- Establish unique personal identification for systems access (Section 12(a)(1), Directive 357).
- Consider encrypting data, especially for remotely accessible systems (Section 13, Directive 357).
- Maintain a backup and disaster recovery plan (Section 16(a)(1), Directive 357).
- Test all backup and recovery arrangements at least once every two years (Section 16(b), Directive 357).
- Execute written outsourcing contracts with specified terms and conditions related to information security and emergency situations (Section 18, Directive 357).

Credit Data

Under the Credit Data Law, 5776-2016 (unofficial translation) (Credit Data Law), the Bank of Israel protects consumer credit data by setting certain obligations, such as those regarding:

- Centralizing credit data collected from credit providers and government authorities.
- Transferring credit data through credit bureaus only to customers and authorized lenders.
- Appointing a Supervisor of Privacy Protection and adhering to a risk-based information security approach (Sections 18, 23, and 60, Credit Data Law).

Insurance Companies

The Israeli Ministry of Finance Department of Capital Market, Insurance, and Savings Circular on Cyber Risk Management in Institutional Entities (Institutional Entities Circular 2016-9-14) (in Hebrew) (Institutional Entities Circular) applies to pension insurance fund managers.

The Circular sets out several information security obligations, including requiring pension insurance funds to:

- Adopt a corporate policy on cybersecurity risk management (Section 3(a)(1)(a), (b)(1), Institutional Entities Circular).
- Ensure their chief executive officer (CEO) establishes an appropriate organizational structure to manage cyber risks (Section 3(a)(2), Institutional Entities Circular).

- Appoint an experienced chief cyber defense officer to implement a cyber risk management policy (Section 3(a)(4), Institutional Entities Circular).
- Establish a cybersecurity steering committee that includes the CEO, chief IT officer, chief risk management officer, and chief cyber defense officer (Section 3(a)(3)(a), Institutional Entities Circular).
- Prepare, assess, and update a cyber risk management program (Section 4, Institutional Entities Circular).
- Include cybersecurity protection provisions in outsourcing agreements (Section 5(e)(1)(b)(1), Institutional Entities Circular).
- Address cybersecurity concerns related to hiring and training employees who access sensitive information (Section 5(g), Institutional Entities Circular).
- Hold an annual discussion on updating their cyber risk assessment and management program (Section 3(a)(1)(b), Institutional Entities Circular).

Health Data

Databases containing medical or genetic information or information regarding a person's mental condition receive specific security level classifications. For example, databases containing health data of:

- Less than 100,000 people are medium security level databases (see Medium Level Database Security Requirements).
- 100,000 or more people are high security level databases (see High Level Database Security Requirements).

(First and Second Schedule, Security Regulations.)

The Israel Ministry of Health has issued several circulars for healthcare institutions, including:

- Circular 18/2012 on Protection of information in computerized system in the health system (in Hebrew) (Circular 18/2012), which provides instructions to secure and protect health data.
- Circular 03/2015 on Protection of information in computerized systems in the health system (in Hebrew), which updates Circular 18/2012.
- Circular 1/2018 on Secondary Uses of Medical Data (in Hebrew) (Circular 1/2018), which addresses data protection regarding secondary uses of medical data and imposes data security measures, including:
  - prohibiting the use of identifiable data for any purpose other than for which it was provided (Section 5.1, Circular 1/2018);
  - preferring de-identified data for secondary uses, even if Israeli law permits using identifiable data (Section 5.2, Circular 1/2018);
  - requiring healthcare organizations that currently use identifiable data for secondary purposes to present a solution plan for using de-identified data, where feasible (Section 5.5, Circular 1/2018);
  - obligating healthcare organizations to establish and manage user access control measures allowing only authorized users to access medical information (Section 8.2, Circular 1/2018); and
  - requiring those user access control measures to identify and authenticate authorized users and document any access to health information (Section 8.5, Circular 1/2018).

Biometrics Data

The Israeli government uses biometric data in residents' identification documents, such as identification cards and passports, to prevent falsification, identity theft, and misuse. The Inclusion of Biometric Identification Means and Biometric Identification Data in Identification Documents and in a Database Law, 5770-2009 (Biometric Database Law), governs the use of this data.

The Biometric Database Law:

- Establishes a government-maintained biometric database to retain residents' biometric data in a secure,

encrypted manner.
- Specifies the public bodies and persons authorized to access the database (Section 1, Biometric Database Law).
- Requires measures to protect biometric identifiers and other identification data from:
  - leakage or hacking; and
  - unauthorized transfer, disclosure, deletion, use, modification, or copying.

(Section 25(a), Biometric Database Law.)

Critical Computer Systems Protection

Israeli law does not formally define critical infrastructure or essential services.

However, the Regulation of Security in Public Bodies Law, 5758-1998, as amended (in Hebrew) (Security Law), establishes powers and responsibilities for critical computer systems in various public, government, and private bodies listed in the Security Law (Schedules 1 to 5, Security Law). The list includes:

- Utilities, including telecommunication providers.
- Financial services.
- Public transportation.
- Government agencies.

The Security Law directs regulatory authorities to issue binding cybersecurity directives applicable to listed groups.

Other Laws and Regulations

Israeli laws, regulations, and regulatory guidance protect other types of at-risk data, assets, and business interests.

Public Companies

There are no laws or regulations that specifically impose data security requirements on companies publicly traded on the Tel Aviv Stock Exchange.

In October 2018, the Israeli Securities Authority (ISA) issued Guideline 105-33 on disclosure regarding cybersecurity (in Hebrew) (Guideline 105-33). Guideline 105-33 recommends that publicly traded companies include cyber issues in their required disclosures.

The Securities Law, 5728-1968 (unofficial translation), and Securities (Details, Structure, and Form of Prospectus) Regulations, 5729-1969 (unofficial translation), generally require publicly traded companies to describe risk factors and exceptional events in their prospectuses, periodic reports, and annual reports.

Guideline 105-33 addresses cybersecurity regarding these obligations, noting that:

- Cyber risks are similar to any other risk (Section C(1)(a), Guideline 105-33).
- Publicly traded companies must:
  - disclose substantial cyber risks in their prospectuses and periodic reports and, in some circumstances, in their annual reports; and
  - indicate if they have adopted a correctly implemented, effective, and appropriate cybersecurity policy.

- (Sections C(1)(a), (2), Guideline 105-33.)

- Public companies should use various factors to determine whether a cyber risk or cyberattack is substantial or exceptional for disclosure purposes, such as:
  - the occurrence of previous cyberattacks, including their severity and frequency;
  - the probability of recurrence;
  - the company's ability to prevent and minimize its risk exposure;
  - aspects of the company's business and activities that create substantial cyber risks;
  - the resources required to maintain cyber defense;
  - the potential damage to the company's assets, intellectual property, reputation, and competitive advantages;
  - the attacker's identity and type;
  - the attack's circumstances and duration;
  - whether the company can fully detect and contain damages from the attack;
  - the scope and type of damage, including indirect consequences; and
  - the necessary actions taken during and after the attack to address the current and prevent future attacks.
- (Section C(1)(a), (b), Guideline 105-33.)

Trade Secrets

There are no Israeli laws or regulations that specifically set out the data security measures organizations must take to protect trade secrets.

However, Section 5 of Commercial Torts Law, 5759-1999 (unofficial translation), requires owners of commercial information to take reasonable security measures for information to be considered a trade secret. Owners can meet this standard even if the reasonable measures implemented prove to be inadequate in practice to protect the information (DC 2117/07 *Gamida MedEquip Ltd. v. Fisher Scientific Co. LLC* (2012)).

Business Contracts

Data security requirements may also arise under contractual duties. Organizations that fail to support sufficient data security measures may be liable for damages claims under Israeli contract law. Common obligation sources include:

- Outsourcing or other service provider agreements.
- Non-disclosure agreements.
- General contractual commitments to follow industry standards and practices, including implicit or unwritten expectations.

Industry Standards

ISO Standards

Israel has issued several guidelines and resolutions that support the ISO 2700x family of international information security standards. These guidelines and resolutions include:

- Guideline No. 03/2018 (in Hebrew), which declares that organizations certified under the ISO/IEC 27001:2013(E) standard and in full compliance with its terms meet the Security Regulations for applicable databases.
- Resolution No. 2443, which directs government agencies to follow the Israeli Standard ISO 27001, adopted from the ISO standard.
- Circulars 18/2012 and 3/15 (see Health Data and Biometrics Data), which:

- require healthcare institutions in Israel to receive certification under the ISO 27799 standard (Section 6.1, Circular 18/2012); and
- recommend that healthcare institutions engage with external services providers that comply with ISO 27799 or ISO 27001 standards (Section 7.1, Circular 18/2012 and Section 8.3, Circular 3/15).

Israel National Cyber Directorate Standards

The Israel National Cyber Directorate (INCD) Cyber Defense Methodology for an Organization (INCD Methodology) minimizes Israeli organizations' cyber risks by helping them:

- Recognize relevant risks.
- Formulate a defense response.
- Create a risk reduction program.

The INCD Methodology has two stages, including:

- Stage A, which uses a questionnaire to classify organizations in one of two categories according to their cyberattack risk exposure, which are:
  - low damage potential (Category A) organizations, whose potential damage from cyber incidents is not great; or
  - significant damage potential (Category B) organizations, whose potential damage from cyber incidents is great.
- Stage B, which provides information on constructing an appropriate work plan to address:
  - the information the organization needs to protect;
  - the required protection level; and
  - existing protection gaps.

In November 2018, the INCD issued:

- The National Cyber Concept for Crisis Preparedness and Management, which:
  - provides guidance on mapping vital cyber assets;
  - describes cyber states of alert and principles for changing the alert level; and
  - elaborates on cyber crisis preparedness, management, and response.
- Organizational Preparedness for a Cyber Crisis – Characterization & Requirements from Crisis Management Team and IR Team, which provides guidance on building a cyber crisis management team.

Developing, Implementing, and Maintaining an Information Security Program

Israeli laws generally obligate most organizations to support an information security program for one or more purposes, such as to:

- Protect the personal data that they collect and use (see Protection of Privacy Law and Security Regulations).
- Comply with applicable sector-specific laws (see Sector-Specific Laws and Regulations).
- Protect specified public, government, and private bodies' critical computer systems (see Critical Computer Systems Protection).
- Protect other forms of at-risk data, assets, and business interests (see Other Laws and Regulations).

Organizations should consider Israel's laws, including sector-specific requirements, and industry standards when implementing information security program elements, including:

- **Assigning accountability.** See Data Security Officer.
- **Identifying and assessing risks.** Database controllers at every security level must perform varying

degrees of risk assessment to reliably identify and maintain reasonable security measures.

- **Developing information security policies.** Controllers of basic, medium, and high security level databases must implement a written security procedure that includes user training, implying the need for a formal policy (Regulation 4, Security Regulations; see Basic Level Database Security Requirements). Robust information security policies can help organizations by:
  - establishing information security as a core value;
  - helping employees and others to understand information security risks and take appropriate actions to minimize them; and
  - providing clear strategies and rules for using and protecting the organization's information and other IT resources.
- **Training employees.** Controllers of basic, medium, and high security level databases must provide varying degrees of information security training to their authorized users (Regulations 4 and 7, Security Regulations; see Basic Level Database Security Requirements and Medium Level Database Security Requirements). Sector-specific laws often also require some form of employee training.
- **Evaluating program effectiveness and compliance.** Database controllers must periodically review their information security programs. Industry standards like the INCD Methodology also encourage internal risk analysis and work plan reviews.

For more details on building comprehensive information security programs, see Global Information Security Toolkit.

Data Security Officer

The people and entities that must appoint a qualified person to manage their information security are:

- Individuals or entities owning at least five registered databases.
- Public bodies.
- Banks.
- Insurance companies.
- Companies that rate or evaluate credit.

(Section 17B(a), PPL and Regulation 3, Security Regulations.)

A person convicted of an offense involving moral turpitude or violating the PPL cannot be a data security officer (Section 17B(c), PPL). No other qualifications are specified.

The data security officer, if required, must:

- Report directly to:
  - the database manager;
  - an active manager of the database controller or processor; or
  - another senior official who directly reports to the database manager.
- Prepare a data security procedure and have it approved by the database controller.
- Prepare and implement a plan to regularly monitor compliance with the Security Regulations and notify the database controller and manager of the findings.

(Regulation 3, Security Regulations.)

Organizations should consider applicable laws, industry standards, any sector-specific obligations, and their overall risks and business needs when choosing how to assign accountability for information security.

Cyber Incident Response and Data Breach Notification

A robust well-tested incident response plan can help database owners respond more effectively to cyber incidents and data breaches (for an example plan, see Standard Document, Global Cyber Incident Response Plan (IRP)).

Owners of medium and high security level databases must immediately notify the Registrar of a severe security incident. Data subjects do not have an automatic notification right under the PPL. The Registrar may order a database controller to notify a data subject who may suffer damage from a severe security incident (Regulation 11(d)(2), Security Regulations).

For details on responding to cyber incidents and providing data breach notification, including interacting with Israel's computer emergency response team (CERT) resources, see Practice Note, Cyber Incident Response and Data Breach Notification (Israel).

Cyber Information Sharing

Israel supports public-private partnerships for cybersecurity information sharing through:

- The INCD, which is responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational defense in cyberspace (see Israel National Cyber Directorate Standards).
- Israel's Computer Emergency Response Team (IL-CERT), a professional organization that addresses information security and cyber events.
- The Inter-University Computation Center, a non-profit established by Israel's universities that:
  - provides computing, digital information, and research services for Israeli universities, colleges, research institutions, and industrial companies; and
  - runs its own CERT, IUCC-CERT, to address networking and computer security incidences in Israel's academic network.
- The Cyber and Finance Continuity Center (FC3), a part of the Israeli Ministry of Finance. FC3's mission is to provide financial services and business continuity to the public and the government while protecting stability, financial leadership, and confidence.

Enforcement and Litigation

Regulatory Enforcement

Registrar of Databases

The Registrar:

- Heads the Minister of Justice's unit to supervise databases, their registration, and their information security.
- Appoints qualified inspectors.
- May:
  - require individuals to provide data or documents related to a database;
  - enter and search any place it has a reasonable belief is being operated illegally and seize property, though a court order is necessary to enter a residential property; and
  - delay, suspend, or cancel database registrations.

(Section 10, PPL.)

The Registrar may also exempt or enhance a database's data security obligations under the Security Regulations

if there are justified reasons (Section 20, Security Regulations).

Privacy Protection Authority

The PPA investigates and enforces administrative and criminal actions against organizations that violate the PPL and Security Regulations. Following an investigation, the PPA may:

- Require an organization to:
  - fix a violation under its supervision; or
  - cease using personal information by suspending or canceling its database registration.
- Initiate an administrative or criminal action depending on the nature and severity of the violation.
- Impose administrative fines on an organization for its unlawful use of a database.
- Refer potential criminal enforcement actions to the State Attorney's Cyber Unit, which specializes in the enforcement of computer and information offenses.

The PPL expressly imposes criminal sanctions for some violations. For example, any person who willfully infringes another's privacy by failing to register a database may be subject to up to five years imprisonment (Section 5, PPL). The PPL also applies strict liability and imprisonment for one year for several offenses, including to those who:

- Violate the database registration and use requirements under Section 8 of the PPL.
- Provide false information when registering a database under Section 9 of the PPL.

(Section 31A, PPL.)

The PPA publishes enforcement actions, listing the organization's name and violations on its website (in Hebrew). For example, in July 2018, the PPA:

- Investigated an organization after an information leakage incident allowed access to its servers and disclosure of personal information.
- Determined that the organization had not fulfilled its information security obligations under the PPL and related Security Regulations by failing to:
  - have a Database Definition Document or written data security procedure; and
  - take appropriate measures to ensure that only authorized users were using its database.
- Mandated corrective actions to implement the required security level by a specified deadline.

Private Actions

An act or omission that violates the PPL's database privacy provisions is a civil tort under the Israeli Civil Wrongs Ordinance [New Version] (Section 31B, PPL).

Israeli courts have recognized class actions brought by individuals suffering data breaches. For example, in:

- In 1634-05-11 *Ohad Pinchewski v. Sony Corp.* (2013), the District Court of Tel-Aviv-Jaffa approved a settlement between Sony Corporation, other companies, and a group of individuals whose sensitive information was exposed when a security failure led to the hacking of Sony's PlayStation Portable and PlayStation3 videogame consoles.
- In pending case 32672-02-17 *Avi Avraham Barak v. Facebook Inc.*, the claimants allege that Facebook published their pictures without consent and created a database of the pictures. The claimants have asked for a court order:
  - prohibiting publication of the pictures; and
  - requiring Facebook to delete any database.

Protecting Sensitive Information Security Records

Organizations should exercise caution and protect from unnecessary disclosure sensitive information security analyses, such as risk assessments and cyber incident investigations, where possible.

Israeli law provides a broad attorney-client legal privilege that includes information and documents exchanged between attorneys and clients seeking legal advice. Documents and information cannot be revealed or disclosed in any legal proceeding, investigation, or search unless the client waives privilege (Section 90 of the Israel Bar Association Law, 5721-1961, and Section 19 of the Bar Association Rules (Professional Ethics), 5746-1986).

Protected documents may potentially include those regarding risk assessments, security incidents, or investigative reports. The privilege applies in the context of seeking and receiving legal advice, making routinely conducted risk assessments or other business activity records more difficult to protect. However, attorneys generally cannot provide documents they receive from clients to third parties, regardless of their content, without client approval or a court order.

