Cyber Incident Response and Data Breach Notification (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 addressing legal requirements and considerations when handling data breaches, cyberattacks, or other information security incidents in Israel or drafting data breach response notifications regarding personal data originating from Israel. This Note discusses the Protection of Privacy Law, 5741-1981, Protection of Privacy Regulations (Data Security), 5777-2017, and guidance from the Privacy Protection Authority (PPA) and the Israeli National Cyber Directorate (INCD). The Israeli-specific guidance in this Note may be used with the generally applicable resources listed in Global Cyber Incident Response and Data Breach Notification Toolkit.

Contents

Data breaches, cyberattacks, and other information security incidents are increasingly common across sectors and affect a wide range of large and small organizations. In response, data breach notification laws, regulations, and best practices raise significant challenges for global companies. This Note explains the Israeli laws and regulations an organization must consider and the local resources available when handling breaches of personal data originating from Israel.

Cyber incidents occur when events raise concerns regarding the security, confidentiality, integrity, or availability of an information technology (IT) system, network, or data. Reporting and notification obligations vary according to a cyber incident's characteristics. For example:

- Data breach notification obligations may apply if the event exposes personal information to potential unauthorized access or use.
- Other cyber incident notification requirements may apply in some jurisdictions if the event affects critical infrastructure or regulated entities.

Some cyber incidents result from criminal activities. Victimized organizations should consider reporting cybercrime to applicable authorities.

The Israeli-specific guidance in this Note may be used with the generally applicable resources listed in Global Cyber Incident Response and Data Breach Notification Toolkit.

Data Breach Notification

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, require database owners, managers, and possessors to protect information that databases contain and, for that purpose, maintain information security (Section 17, PPL). The Security Regulations sometimes call these parties database controllers. This Note uses the term database controller collectively unless context requires otherwise.

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(d) PD 808 (1994).)

The PPL and Security Regulations characterize databases in four ways and apply escalating information security requirements 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.

For more information on database levels and required security measures, see Practice Note, Information Security Considerations (Israel): Personal Data Under the PPL and Security Regulations.

Triggering Events

Severe security incidents trigger notification requirements for database controllers of medium and high security level databases. A severe security incident is, for:

- High security level databases, an incident involving:
  - the use, disclosure, transfer, or delivery of data from the database without or exceeding authorization; or
  - damage to the data's integrity.
- Medium security level databases, an incident involving:
  - the use, disclosure, transfer, or delivery of a **substantial** part of the database without or exceeding authorization; or
  - damage to the integrity of a **substantial** part of the database.

(Section 3, PPL and Regulations 1 and 11(d)(1), Security Regulations.)

Privacy Protection Authority (PPA) guidance indicates that organizations can determine whether an incident involves a substantial part of a medium security level database by generally considering:

- The severity of the risks.
- The scope of the data at risk, such as the amount of affected information or the number of persons exposed.
- The quantity and kinds of systems that were damaged or used without authorization.
- The event's duration.

Notice to Authorities and Affected Individuals

Database controllers:

- Must generally notify the Registrar of Databases (Registrar) of a severe security incident and the response measures that they take within 24, but no later than 72, hours after discovery (see PPA: Reporting a severe security incident (in Hebrew)).
- Should submit notifications using email to ppa_SecurityEvents@justice.gov.il using the PPA's online form.

Data subjects do not have an automatic data breach notification right under the Security Regulations. The Registrar, after consulting with the head of the Israeli National Cyber Directorate (INCD), can order a database controller to notify data subjects who may suffer damage from a severe security incident (Regulation 11(d)(2), Security Regulations).

Other Cyber Incident Notification Requirements

Israel generally does not require organizations to provide any other cyber incident notification.

However, sector-specific obligations apply in some areas. For example, the Bank of Israel's Proper Conduct of Banking Business Directive 361 (03/15) (Bank Directive) requires banking corporations to notify the Supervisor of Banks of broadly defined cyber incidents (Paragraphs 81-82, Bank Directive).

Industry standards typically call for formal cyber incident response planning and management. A robust well-tested incident response plan can help organizations respond more effectively to these events. For an example plan, see Standard Document, Global Cyber Incident Response Plan (IRP). Organizations that experience a cyberattack or other information security incident should consider:

- Reporting the event to any applicable authorities (see Reporting Cyberattacks and Cybercrime).
- Seeking assistance and sharing information through established computer emergency response teams (CERT) or other cybersecurity information sharing programs (see Getting Help with Cyber Incident

Response).

For more details on Israel's information security obligations that require organizations to take steps to protect data and prevent cyber incidents, see Practice Note, Information Security Considerations (Israel).

Enforcement and Litigation

Regulatory Enforcement

Registrar of Databases

The Registrar:

- Heads the Ministry of Justice's unit that supervises 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 justified (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 is 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 DC 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.

Getting Help with Cyber Incident Response

Israel supports public-private partnerships and various CERT resources to coordinate cyber incident response and help organizations recognize, respond, and recover from cyberattacks.

Some notable resources include:

- The INCD's:
  - Principles for Action for Coping with Cyber Threats (in Hebrew), which sets out guidelines for dealing with cybersecurity threats; and
  - Cyber Defense Methodology for an Organization, which helps organizations recognize relevant risks, formulate a defense response, and create a risk-reduction program.

- The INCD is responsible for cyber defense in the civilian sphere, from formulating policy and building technological power to operational defense.
- Israel's Computer Emergency Response Team (IL-CERT), a professional organization that addresses information security and cyber events.
- The Inter-University Computation Center (in Hebrew), a non-profit established by Israel's universities that 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 Ministry of Finance. FC3 ensure the resiliency of the financial services sector against cyberattacks by proactively identifying threats, promoting protection, driving readiness, and collaborating with worldwide financial institutions by:
  - increasing Israeli cyber financial resilience;
  - providing a platform for information sharing and cooperation among financial institutions;
  - providing situation analysis for decision makers;
  - operating response teams; and
  - providing incident handling.

Reporting Cyberattacks and Cybercrime

The National Cyber Unit (in Hebrew) in Lahav 433 of the Israel Police combats cybercrime. As part of its various functions, the National Cyber Unit:

- Conducts investigations.
- Handles cybercrime involving economic damage, critical infrastructure, and financial institutions.

