Bloomberg Law® Privacy & Data Security

Country Profile: ISRAEL

Haim Ravia and Dotan Hammer, of Pearl Cohen Zedek Latzer Baratz, Tel Aviv, provided expert review of the Israel Country Profile and wrote the Risk Environment section. [Last updated September 2017. — Ed.]

I. APPLICABLE LAWS AND REGULATIONS

Basic Law: Human Dignity and Liberty § 7(a) (in Hebrew; in English) states that "all persons have the right to privacy and intimacy." Sections 7(b)–7(d) restrict entry into the private premises of a person without consent; searches of private premises of individual persons or personal effects; and violation of confidentiality of conversations or a person's writings or recordings. Any law that would limit the rights set out in the Basic Law must conform with the values of the State of Israel, be enacted for a proper purpose, and be proportional, that is, enacted to an extent no greater than is required (§ 8). Israel does not have a complete constitution, but the Supreme Court of Israel has held that Basic Laws have constitutional status.

The main privacy protection law is the Protection of Privacy Law, 5741-1981 (PPL) (in Hebrew; unofficial English translation). Section 1 states that "no person shall infringe the privacy of another without his consent." Chapter One of the PPL deals with privacy infringement in a broad sense and lists a number of activities that constitute an invasion of privacy if performed without data subject consent. Chapter Two of the PPL deals with database privacy and other database-related obligations and contains provisions more similar to data protection laws around the world. In CA 439/88 *Database Registrar v. Ventura*, 48(3) PD 808, 821 (1994) (in Hebrew), the Israeli Supreme Court applied the provisions of Chapter One, which restrict certain privacy-invading conduct, to the subsequent processing of data gleaned from such restricted conduct in databases regulated under Chapter Two.

With reference to databases, PPL § 7 defines "information" to mean data on an individual's personality, personal status, intimate affairs, health, financial status, vocational qualifications, and opinions or beliefs. "Sensitive information" is nearly identical to "information," but does not include personal status or vocational qualifications. PPL § 7 defines "database" as "a collection of data, stored by magnetic or optical means and intended for computer processing," with certain exceptions, and also defines "Registrar" as a "person who has the qualifications to be appointed judge of a Magistrate's Court, and was appointed by Government, by notice in Reshumot (the official Gazette), to the position of Registrar of Databases." The law determines that only natural persons are protected by the PPL's database protections (§ 3). The PPL does not require that the individual be a resident or citizen of Israel.

PPL § 8(c) mandates that if a database contains the information of more than 10,000 individuals, sensitive information, or any information that was not provided by, on behalf of, or with the consent of the data subjects, it must be registered with the Registrar, which serves as a unit of the Israeli Law, Information and Technology Authority (ILITA) (in Hebrew; in English). In addition, any database belonging to a "public entity" (as defined under the PPL § 23) or used for direct mailing services (i.e., providing "direct mailing services to others, by transferring lists, labels, or data by any other means") must also be registered.

ILITA provides a FAQ (in Hebrew) about database registration applications. Registration of a database consists of an application including:

- the names of the owner, possessor, and manager of the database, and their Israeli addresses;
- the purpose of the database, and the purposes for which the data is collected;
- the types of information the database will contain;
- particulars on any intended data transfers outside of Israel; and
- particulars on receiving information, on a permanent basis, from a public body (PPL § 9(b)).

Use of information regarding a person's private affairs not for the purpose for which it was provided constitutes an invasion of privacy under the PPL's general privacy provisions, and use of data included in a database other than for the purpose for which it was provided constitutes a violation of the PPL's database provisions.

Forthcoming information security regulations taking effect in May 2018 will require database controllers and holders to notify the Registrar of security breaches in certain cases, and the Registrar can then require that the database controller or holder notify data subjects of the breach.

PPL § 17B requires anyone who possesses five or more databases subject to registration requirements to appoint a data security supervisor. Appointment of a data security supervisor is also required for public entities (defined in PPL § 23) and for banks, insurance companies, and companies involved in rating or evaluating credit. The data security supervisor is responsible for database security, and anyone convicted of an offense involving moral turpitude or any violation of the PPL cannot serve as a data security supervisor.

PPL Chapter Two, Part Two, concerns direct mailing. Section 17D prohibits managing or possessing a database for direct mailing services unless it is registered, and § 17E prohibits managing or possessing a database for direct mailing unless the controller keeps a record of every data source from which information was gathered and the date it was received, as well as the recipients of such information. Section 17F(b) entitles anyone to demand, in writing, his removal from any database used for direct mailing purposes. However, it should be noted that such removal in accordance with § 17F(b) does not necessarily mean the deletion of all the person's data from the database itself, but merely the deletion of his details from the direct mailing list.

Certain sector-specific laws provide additional protection for the types of information referenced in such laws. Among these are the Patients' Rights Law 1996 (medical information); Genetic Information Law, 5761-2000 (in English) (genetic information); the Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law, 5770-2009 (in Hebrew) (establishing a biometric database); the Electronic Signature Law 2001 (in Hebrew) (electronic signatures); and the Credit Information Service Law 2002 (credit information), which is expected to be substituted by the Credit Data Law, 5776-2016 (in English), in late 2018 or early 2019.

Regulations promulgated under the PPL restrict data exports from databases subject to the PPL to recipients outside of Israel. ILITA has recently issued some clarifications regarding the legal situation in Israel as regards exporting database information abroad, due to the dismissal of the Safe Harbor framework by the Court of Justice of the European Union in 2015. In addition, the Registrar published a series of directives on matters such as the use of outsourcing services for processing personal information, usage of surveillance cameras and databases of the images, and databases created by service providers to national health providers. The Registrar's directives, once published, are not legally binding *per se*, but reflect the Registrar's position and serve as guiding principles when it exercises its supervisory and investigative powers.

On Jan. 31, 2011, the European Commission deemed Israel to have adequate protection of personal data for data transferred from the European Union to Israel, but only for automated international data transfers and processing as well as non-automated transfers that are subject to further automated processing in Israel, not to data transfers where the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means (see 2011/61/EU).

Data Management

Data Retention

Israel does not have any data retention laws, yet telecom metadata retained by telecom providers in their course of business is made available, subject to certain judicial procedures, to investigative and intelligence agencies for the purpose of search and rescue, investigating or preventing crime, or seizing property, pursuant to the Criminal Procedure Law (Enforcement Powers – Communication Data), 5767-2007. In addition, the Prime Minister is granted sweeping statutory powers to order that metadata and non-real time communications (traffic data at rest), which are retained by telecom providers, be surreptitiously made available to the Israeli Security Agency, pursuant to § 11 of the General Security Service Law, 5762-2002 (in Hebrew; unofficial English translation).

Data Localization

Israel does not have any data localization laws, except in very particular instances such as territorial localization of data in accounting systems for tax audit purposes.

Data Disposal

Israel does not have any data disposal laws, other than the forthcoming information security regulations taking effect in May 2018, which require an organization outsourcing the processing of personal data to contractually obligate the service provider to destroy its copies of the data at the end of the engagement.

II. REGULATORY AUTHORITIES AND ENFORCEMENT

The data protection authority is the Israeli Law, Information and Technology Authority (ILITA) (in Hebrew; in English). ILITA is an independent body that was established by the Ministry of Justice in 2006. Its objectives are to strengthen personal data protection, regulate and monitor the use of electronic signatures, and enforce legal sanctions for violations of the PPL. ILITA also keeps a registry of certain databases containing personal information, which, pursuant to PPL § 12, is open to public inspection.

Individuals wishing to file a complaint relating to data protection can do so online (in Hebrew). Complaints can also be filed by e-mail or by fax. ILITA is responsible for handling complaints and investigating offenses and can issue administrative fines. Individuals and companies can also apply to ILITA for a preliminary opinion (pre-ruling) on questions of interpretations of the PPL or ILITA regulations. Information on requesting a preliminary opinion is available on ILITA's website (in Hebrew), and ILITA has also promulgated a document on the procedures for issuing a preliminary opinion (in Hebrew).

An infringement of privacy is a civil tort that entitles the offended party to the right to claim damages under the Tort Ordinance [New Version]. In some cases, an infringement of privacy and other violations of the PPL are considered criminal offenses. For instance, intentional infringement of the privacy of another in violation of PPL § 2 is punishable by up to five years in prison (§ 5) and civil damages paid to the injured party up to approximately 60,000 NIS without proof of damage (§ 29A(a)), or up to approximately 120,000 NIS if the infringement was intentional; such amounts are linked to the consumer price index (§ 29A(d)). Disclosure of personal information in violation of PPL § 16 or deliberate violation of the right to privacy in accordance with PPL § 5 is punishable by up to five years' imprisonment (§ 16 and § 5).

PPL § 31A sets forth the penalties for strict liability offenses. These offenses require no proof of criminal intent or negligence, are punishable by up to one year's imprisonment, and include:

a. managing, possessing, or using an unregistered database that requires registration under § 8;

b. providing incorrect information on a database registration application;

c. failing to provide the required notice with a request for information from a data subject under § 11;

d. failing to comply with information inspection, correction, and deletion provisions of the PPL;

e. failing to appoint a data security supervisor in accordance with § 17B;

f. violating the provisions of PPL regarding direct mailing; and

g. providing information in violation of § 23(b)-(e).

III. RISK ENVIRONMENT

In the past year, Israel's privacy regulator, the Registrar, has been engaging in more proactive enforcement and regulatory activities.

The Registrar, operating under ILITA, is vested with investigative and audit powers. Pursuant to the PPL, Registrar inspectors can conduct announced or unannounced audits at premises where databases are administered, collect evidence, and seize computers. The Registrar is also authorized to impose administrative sanctions in several forms: mere declarations of fault, fines, and suspension or revocation of database registration.

Pursuant to §2 of the Administrative Offenses Regulations (Administrative Fine – Protection of Privacy), 5764-2004, corporations can be sanctioned by administrative fines for violations of the PPL in amounts ranging from 10,000 NIS (approximately US $2,500) to 25,000 NIS (approximately US $6,500), depending on the violation in question. Continuous violations following a cease and desist letter from the Registrar can increase the fine by an additional 10% for each day during which the violation continues.

Registrar enforcement activities made public recently have dealt with data breaches associated with violations of the statutory duty to employ information security measures, violations of duties regarding direct mailing activities, and use of databases for purposes inconsistent with their registered purposes. These have resulted in declarations of fault and, in certain cases, fines.

The Registrar has also been focusing its enforcement efforts in recent years on data brokers that unlawfully engage in data enhancement services using, among others, government-administered databases that have been unlawfully leaked, such as the Registry of Population (containing detailed information of all Israeli residents and citizens, including the deceased) and the voters' roll database. One such data broker was forced to discontinue its business following the Registrar's enforcement activity and the Registrar's order that it cease using its database, which included unlawfully obtained data.

In addition, a number of enforcement activities were taken against unlawful dealings in personal data, such as trafficking of personal health information unlawfully obtained from hospitals and health care providers.

In 2011, the Israeli government proposed a bill to amend the PPL by enhancing the Registrar's enforcement and regulatory powers. No progress was made with the bill since 2011. But nowadays, with further advances in technology, the Registrar feels that it lacks effective enforcement tools suitable for the nature of today's data protection and privacy risks. It has therefore expressed its desire to resume discussions on the bill.

Notably, infringement of privacy committed in the context of relations between businesses and consumers establishes grounds for class action under Israeli law.

Additionally, the Registrar has issued in the past two years a number of new guidelines and draft guidelines on topics such as use of personal data for direct mailing purposes, use of security and surveillance cameras (CCTV) at the workplace, data subjects' right to access their data, and transferring the ownership of databases in the context of merger or acquisition transactions.

The forthcoming data security regulations (taking effect in May 2018) are potentially impactful on the risk landscape, as they could have broad implications from legal, technological, and business perspectives for virtually anyone in Israel that handles personal data. They warrant preparation well in advance of their effective date, in areas such as internal business protocols, training, technology procurement, and outsourcing. They raise complex questions on topics such as the use of cloud storage services where the cloud user's control over security measures may be more limited.

IV. EMERGING ISSUES AND OUTLOOK

A. Biometrics

In 2009, the Knesset (the Israeli legislature) enacted the Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law, 5770-2009. The law would create a biometric database of Israeli residents using a facial feature image and two fingerprints (left and right index finger).

Registrants would then be issued an identification card with a chip that contained this biometric information, and the card would be the standard form of identification. After many delays, in addition to a great deal of opposition and concern over privacy, a two-year trial of the database was launched in mid-2013 (see "Israel Set to Launch Biometric ID Pilot Long-Delayed Over Privacy Concerns," *Privacy Law Watch* (June 27, 2013)).

In February 2014, the Israeli Supreme Court ruled that in any advertising for the trial period, the government must clarify that enrollment in the program is fully voluntary and that citizens' rights would not be in any way limited if they did not join (see "Israel High Court Rejects Privacy Petition Against Biometric Program, Requires Notice," *Privacy Law Watch* (March 3, 2014)). The trial period was set to expire on June 30, 2015, but prior to the issuance of a negative report (in Hebrew), the government extended the program for an additional nine months, and the trial period was recently extended for an additional nine months until Dec. 31, 2016. This extension will be used to address issues raised in the report. In April 2015, the outgoing Interior Minister stated that the program would be made mandatory at the conclusion of the trial period, but the nine-month extension of the trial period overrode that decision. At the conclusion of the trial period in 2016, Israel's parliament will decide whether to preserve the database and if joining should be mandatory. For more information, see "Israel Extends Biometric ID Trial Period as Comptroller Slams System's Flaws," *Privacy Law Watch* (June 26, 2015). The proposal remains controversial.

B. Data Security Regulations

On March 21, 2017, the Knesset approved the Protection of Privacy Regulations (Data Security) (in Hebrew), which will come into effect on May 8, 2018. The Regulations apply to businesses that own, manage, or have access to databases in Israel containing personal information. Databases are separated into four categories: Individual-Managed Databases, Basic Security Databases, Medium Security Databases, and High Security Databases. These categories are based on criteria including the type and sensitivity of personal information contained in the database, the number of data subjects whose data is contained in the database, and the number of individuals that have access to the database. These categories of databases are subject to differing levels of compliance obligations in the Regulations. For example, the owner of a High Security Database must report all data breaches to ILITA immediately, while the owners of a Medium Security Database are only obligated to report a breach to ILITA if it affects a material segment of the database. The Regulations also contain provisions relating to data minimization, data outsourcing, documentation obligations, and security officers. See "Companies Now Face Israel Data Security, Breach Notice Rules," *Privacy Law Watch* (Mar. 28, 2017).

C. Credit Rating Data

In 2016, a new Credit Data Law, 5776-2016 (in English) was enacted by the Knesset. It is expected to take effect in late 2018 or early 2019 and will substitute for the existing Credit Information Service Law. The new Credit Data Law seeks to enhance competition in the Israeli consumer credit market, by establishing a centralized database at the Bank of Israel (Israel's central bank) with information concerning the creditworthiness of Israelis. The database will enable assessment of the insolvency risks of prospective borrowers. The new Credit Data Law includes provisions establishing broader and arguably more invasive collection of personal data than those established in the current Credit Information Service Law. Presently, pursuant to the existing Credit Information Service Law, various entities that possess information on the creditworthiness of individuals and sole proprietors are required to make that information available to licensed Credit Reporting Agencies, who are in turn authorized to disseminate the information subject to certain conditions and limitations.

The new database to be established under the Credit Data Law will contain, among other data, information about loans extended by banks and non-bank credit providers. The data will be collected without need for prior consent of data subjects. Individuals who wish to opt out of having information about them collected will be able to do so, except that certain so-called "negative data," such as information regarding bounced checks and loan defaults, will nevertheless be mandatorily collected and processed despite any opt-out request. The Bank of Israel will appoint a data protection officer to supervise the database's operation and guide the Bank of Israel on privacy and data protection compliance in accordance with the PPL.

The Credit Data Act will also establish "Credit Bureaus" that will obtain pseudonymized data from the Bank of Israel's database in order to develop risk assessment models. Only when an individual seeks a

loan or credit and consents to having his financial risk profile compiled will the bureaus be able to re-identify the information by cross-checking the pseudonymized data with identifying information. Pursuant to such individual consent, credit providers will be able to request information concerning the person's solvency. Most of the raw financial data will be retained in the Bank of Israel's database for 12 years, but only data pertaining to the three most recent years will be divulged to credit providers when they evaluate a person's solvency.

