Dramatic Overhaul of Israeli Data Security Regulations

By Haim Ravia and Dotan Hammer, Pearl Cohen Zedek Latzer Baratz

Last week, the Israeli Parliament (the Knesset) promulgated the Protection of Privacy Regulations (Data Security), 5777-2017 (the "Regulations"). This marks the consummation of a legislative process that began in 2010 with the Israeli Law, Information and Technology Authority (ILITA, the Israeli privacy regulator), when the first draft of the Regulations was published for public comment.

The Regulations introduce a far reaching reform to the existing information security regulations which date back to 1986 and have become ill-suited for our technology era. Among other issues, the new Regulations introduce an overarching data breach notification requirement for the first time in Israel. Such requirements are common in many other jurisdictions. In the United States, for instance, breach notifications have led to a wave of class action suits against data handlers whose databases were breached.

When will the Regulations apply?

The Regulations will enter into force in late March 2018, giving data handlers 12 months to prepare.

To whom will the Regulations apply?

The Regulations apply to anyone who owns, manages or maintains a database containing personal data in Israel. All Israeli organizations, companies and public agencies are subject to the Regulations. The Regulations would require these actors to reevaluate their information security protocols and adapt them to the newly promulgated requirements.

Layered approach

The Regulations classify databases into four categories, each subject to an escalating degree of information security requirement:

A. Databases maintained by individuals;
B. Databases subject to the basic level of data security requirements;
C. Databases subject to the intermediate level of data security requirements;
D. Databases subject to the high level of data security requirements.

- **Databases maintained by individuals.** These are databases maintained by an individual, such as a sole proprietor. Also included in this category are databases held by a corporation with a single shareholder, and to which no more than 3 people have access credentials. In either case, databases in this category may not be used to make information available to other parties (for example, databases used to provide direct marketing services to others); the number of data subjects may not exceed 100,000; and the data must not be subject to professional confidentiality obligations under law or codes of ethics (for example, a database maintained by a sole-practitioner attorney).
- **Databases subject to the basic level of data security.** These are databases that do not fall within any of the other categories.
- **Databases subject to the intermediate level of data security.** A database to which more than 10 people have access credentials and whose purposes include making information available to other parties. Also included in this category are databases maintained by public agencies, or databases that contain special categories of data. These special categories of data include, among others, medical or health information, genetic or biometric data, and information about an individual's political opinions, faith, religious beliefs or criminal convictions. Special categories of data also extend to information about a person's consumption habits that may be indicative of the abovementioned types of data.

Additionally, special categories of data cover financial information about a person's financial obligations, solvency or financial status.

- **Databases subject to the high level of data security.** Databases whose purposes include making information available to other parties, and in which either the number of data subjects are 100,000 or more or to which more than 100 people have access credentials. This category also includes databases with special categories of data and in which either the number of data subjects are 100,000 or more or to which more than 100 people have access credentials.

The triggering criteria relating to one hundred or more users with access credentials appears to capture many databases that will be subject to the highest level of data security requirements, if they include special categories of data. Since financial information is a special category of data, we anticipate that a growing number of databases will fall within this category.

Requirements applicable to all databases except those held by individuals

- **Drafting a database specification document**. Database owners will be required to draft a specification document detailing, among other things, a general description of data collection and processing activities, description of the purposes of the database, details on the types of data processed, information about cross-border data transfers, and the identity of the database manager, its data security officer and its holders (which are defined as those who regularly possess a copy of the database and are entitled to use it). The specification must also include information about processing activities conducted by other processors and details on the primary data security risks and mitigating them.
- **Physical security**. The database's computer systems shall be kept in a secured location safeguarded against unauthorized access.
- **Data security officer**. The Protection of Privacy Law, 5741-1981 ("PPL") requires public agencies, financial institutions and companies maintaining five or more database to appoint a data security officer. In an effort to ensure the officer's independence, the Regulations require that the officer be directly subordinate to the database manager, or to the manager of the entity that owns or holds the database. The Regulations prohibit the officer from being in a position that raises a conflict of interests. They require the officer to establish data security protocols and an ongoing plan to review compliance with the Regulations. The officer must present findings from the review to the database manager and its supervisor.
- **Data security protocols**. These protocols shall bind all employees and shall address, among other issues, instructions on physical and environmental security of the database's premises, administration and use of portable devices, access credentials, instructions applicable to those with access credentials, measures used to safeguard the database's computer systems and risks to which the database is exposed. The protocols shall also include a layered security incident response plan varying in accordance with the incident's severity and the database's degree of sensitivity.
- **Mapping the database's computer systems**. A database owner shall compile an updated list of components and devices that comprise the database's computer systems. The list shall include hardware and software components detailed in the Regulations and a description of the architecture of the systems in which the database is installed.
- **Access credentials, authentication and user administration**. A database owner shall employ in database-related positions only workers with an appropriate level of clearance in relation to the database's degree of sensitivity. The owner must maintain a list of those with access credentials and must take measures to ensure that access credentials are assigned in accordance with each user's duties and only to the extent necessary for them to perform their work.

- **Documenting information security incidents**. Database owners shall maintain documentation for each incident that raises suspicion of a data breach. Automated logging tools shall be used to the greatest extent possible.
- **Portable devices**. Restrictions shall be placed on using portable devices with database-related computer systems, in accordance with the database's degree of sensitivity. These include smartphones, laptops and memory sticks.
- **Segregation of systems**. To the extent possible, database owners shall segregate database-related computer systems from other computer systems.
- **Communication security**. To the extent that database-related computer systems are connected to the Internet, appropriate security measures shall be implemented to safeguard against unauthorized access and malware. Transmission of personal data over the Internet must be encrypted. Remote access to the database by employees shall be authenticated.
- **Outsourcing**. Engaging an outsourced data processing provider requires pre-engagement due-diligence review of the risks entailed in the engagement. The contractual engagement shall address issues such as the purposes for which the data will be used, the type of data processing to be performed, the period of engagement and return of the data upon conclusion of the engagement.

Requirements applicable to databases subject to the basic level of data security

In addition to the above requirements applicable to all databases, the Regulations introduce the following requirements applicable to databases subject to the basic level of security:

- **Annual reviews**. Database owners shall review the security protocol annually to determine whether updates are needed.
- **Training**. Before granting access privileges or after changing the scope of access privileges, database owners shall provide training to users with access credentials with respect to the security protocols and security requirements under the PPL and the Regulations.
- **Recordkeeping**. Information about compliance with the Regulations, including documentation of security incidents, information about communication security, access privileges and authentication measures, shall be retained for 24 months.

Requirements applicable to databases subject to the intermediate level of data security

The Regulations introduce additional requirements applicable to databases subject to the intermediate level of security. For databases subject to this intermediate level, the following requirements apply in addition to the requirements applicable to all databases and to those applicable under the basic level.

- **Physical and environmental security**. Access to the database's premises shall be monitored. Equipment brought in or taken out of the database's premises shall also be monitored. These will be used in the event of a security breach.
- **Extended security protocol**. The security protocol shall cover, among other issues, user authentication measures applicable to the database, backup procedures, access controls and periodic audits.
- **Authentication.** Users with access privileges shall be authenticated with physical devices such as smart cards. A protocol shall be established for means of identification, frequency of password change and response to errors in access control.
- **Monitoring access**. An automated mechanism for monitoring access to the database shall be established. The logs shall be maintained for at least two years.
- **Periodic audits**. Either an internal or external audit shall be performed at least once in 24 months. The audit shall include a report addressing the security measures' compliance with the security protocol and identification of deficiencies and proposals for remediating them.

The report shall be reviewed and assessment shall be made of the need to update the database's specification document and security protocols.

- **Backup and recovery**. A backup and recovery plan shall be established.
- **Security incidents.** Security incidents shall be reviewed at least once a year and an assessment shall be made of the need to update security protocols.
- **Data breach notifications**. Prompt notification shall be provided to the privacy regulator (ILITA) regarding any severe data breach in which a material part of the database was access or used without authorization, or in the course exceeding authorized access, or where the database's integrity was compromised. A typical incident of this kind is an unauthorized intrusion into the database and theft of data therefrom. The regulator is authorized to order the database owner to notify all affected data subjects. The Regulations do not prescribe any sanctions for violating the breach notification requirement.

Requirements applicable to databases subject to the high level of data security

The Regulations introduce additional requirements applicable to databases subject to the high level of security. For databases subject to this level, the following requirements apply in addition to the requirements applicable to all databases and those applicable under the basic and intermediate level.

- **Risk assessment**. The database owner shall perform an assessment of risks once every 18 months, using a qualified professional, in order to identify and review security risks and deficiencies. Database owners are required to remedy the deficiencies identified and update protocols accordingly. Risk assessment can also be leveraged to satisfy the requirement for periodic audits.
- **Penetration tests**. The database's computer systems shall be subjected to penetration tests once in 18 months, in order to evaluate their robustness in the face of internal and external risks.
- **Security incidents**. Security incidents shall be reviewed at least once every calendar quarter and an assessment shall be made of the need to update security protocols.
- **Data breach notifications**. At this high level of data security, the breach notification requirement applies to any severe data breach in which any portion of the database was breached (not just a material part).

Requirements applicable to databases held by individuals

The requirements for these databases are more lenient. They consist of the following: drafting a database specification document; physical security; access credentials, authentication and user administration; documenting information security incidents; restrictions on using portable devices; segregation of systems; and communication security.

Take away

The potential ramifications of the Regulations are far reaching 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 internal business protocols, training, technology procurement and outsourcing. They also 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.