If you dont see this email click here

Privacy Update: New Israel Privacy Protection Regulations (Data Security) 2017

June, 2017

Following a long legislative process that began in 2010, the Constitution, Law, and Justice Committee of the Knesset (Israeli Parliament) recently approved the Privacy Protection Regulations (Data Security) 2017 (the "**Regulations**"). The Regulations will come into effect on May 8, 2018.

Until the enactment of the Regulations, database security obligations had only been regulated under a general obligation of the database owners, holders and managers to be responsible for the security of the data under Section 17 of the Privacy Protection Law, 1981 (the "**Law**") and under additional Data Protection Regulations enacted in 1986, which provided limited and unspecified security requirements.

The current Regulations provide a broad, specified and comprehensive arrangement regarding the security requirements, measures and procedures which should be implemented by the owners, holders and managers of databases in order to ensure the security of the data included in those databases. In addition, one of the most significant changes is that there are, for the first time in Israel, data breach notification obligations in certain instances in connection with medium and high-level security databases.

The following is a general overview of the Regulations and the requirements that will soon apply.

To which databases do the Regulations apply?

The Regulations will apply to all databases containing personal data.

However, for the purpose of the Regulations and in order to determine the requirements that will apply to each database, the Regulations classify databases into four types:

(1) **A database controlled by an individual**: a database that is owned by an individual or by a corporation owned by an individual that has, in addition to such individual, no more than 2 additional authorized users (except in cases the database is used for direct mailing services, has more than 10,000 data subjects or in case the owner of the database is subject to any ethical or lawful confidential obligations).

(2) **A Basic Security Level Database**: a database which is not controlled by an individual as indicated above and which does not fall under the stricter two classifications below.

(3) **A Medium Security Level Database**: any one of the following:

- A database owned by a public body;
- A database used for direct mailing services; or
- A database which contains information on any of the following: the data subject's private affairs, medical information or information regarding the data subject's mental health, genetic information, financial condition, financial obligations and assets, political opinions or faith, biometric information, criminal record, communication data (such as traffic or location data) and information regarding data subject's consumer habits, which may provide information regarding any of the above or regarding a data subject's personality, opinion or faith.

The Regulations specifically exclude two types of databases from the Medium Security Level Database category, which instead shall be considered to be Basic Security Level Databases, even though they technically fall within the definition of a "Medium Security Level Database". These databases are:

- Databases which include medical information, criminal records, communication data (e.g. traffic or location data), biometric information regarding a data subject's facial image, and financial conditions – about employees or suppliers of the database owner; provided that the purpose of the database is to manage the database owner's business and provided that the database does not include any information regarding data subject's private affairs, genetic and biometric information, consumer habits and political opinions or faith; or
- A database that has no more than 10 authorized users.

(4) **A High Level Security Database**: a database which is used for direct mailing services or that includes information as set forth in the third bullet point in Section 3 above, which either (i) includes more than 100,000 data subjects, or (ii) has more than 100 authorized users.

Obligations under the Regulations

The Regulations set forth security measures, requirements and procedures that a database owner, holder and manager must comply with. The scope of the requirements and their applicability to each database depends on the database security level classification and the nature of the data stored in the database.

The requirements under the Regulations include the following:

Documentation Requirements

- **Documentation of Security Events; Data Breach Notification** – any suspected security event must be documented and, in certain cases, immediately reported to the Database Registrar. In addition, the Database Registrar has the authority in certain instances to order notification to data subjects. We would not be surprised if these data breach notification obligations create a situation where companies are more exposed to lawsuits, including class actions.
- **Database Definitions Document** – a database owner must draft a database definition document that should include, *inter alia*, a general overview of the collection and use of the data, the purposes for which data is used, types of data, details regarding transfer of data abroad, processing the data by a holder, etc. The database definition document must be reviewed on an annual basis and updated in case of material changes.
- **Security Procedure** – a database owner must draft a security procedure that will include instructions regarding the physical and environmental security of the database, access rights, procedures in connection with handling security events and authorizations and instructions to authorized users.
- **Mapping Database's Computer Systems and Executing Risk Assessment Reports** – a database owner must draft (and update as necessary) a document specifying the database structure and its computer systems, including its infrastructure, hardware and communication means, as well as the systems that are used to operate and manage and support the database.

Security Requirements

- **Physical and Environmental Security Measures** – in order to prevent unauthorized access, all systems that are

used to operate and manage the database must be kept in a secure location, in a manner that will correspond with the nature of the database and the data included thereof.

- **Personnel Security Management** – a database owner must implement reasonable security measures in order to ensure that access to the database is granted only to suitable personnel and on a "need to know" basis. Personnel granted access must go through privacy and security training.
- **Managing Access Rights** – a database owner is required to determine and allocate access rights to the database and its systems based on the relevant position definitions.
- **Identification and Verification** – identifying and verifying that access to the database is performed only by authorized personnel.

Additional Requirements

- **Mobile Devices** – a database owner must limit or prevent connection of the database to mobile devices, dependent on the security level of the database, the sensitivity of the data, and other factors.
- **Media Security** – the database may not be connected to the internet or to any other public network without installing proper security measures to prevent unauthorized penetration.
- **Outsourcing** – a database owner that contracts with an outsourcer to receive any services involving access to the database shall be required to implement and meet certain requirements, including examining data security risks related to the engagement with the outsourcer as well as an obligation to include in the contract with the outsourcer certain aspects related to the data such as its processing by outsourcer, security requirements, confidentiality obligations etc..
- **Periodic Audit** – In certain cases, a database owner will be required to perform periodic audits. These must be performed by a person with proper training in the field of data security. Such auditor may not, however, be the database security officer.
- **Backup and Restoration** – in certain cases, the database owner must set procedures to perform backup and restoration of the data.

As may be gleaned from reading the information above, the requirements are quite detailed. We have just provided a general overview of the requirements and additional and specific requirements may apply, depending on the classification of the database and the personal data included therein.

Database Registrar's Authority

The Regulations authorize the Database Registrar to grant a certain database an exemption from the data security requirements as set

forth in the Regulations, on a case-by-case basis. The Registrar's considerations for such an exemption may include, *inter alia*, the number of data subjects, type of information, or the scope of the activity in the database.

In addition, the Database Registrar may also conclude that databases which meet certain national or international standards or meet certain regulatory authority requirements with respect to data security, shall be deemed in compliance with the Regulations.

Sanctions

Failure to comply with the Regulations will be a breach of Section 17 of the Privacy Law, which may expose a non-compliant company to criminal and civil liability as well as to administrative fines.

Recommendations

Due to the significant obligations and requirements introduced under the Regulations, the owners, holders and managers of databases are advised to commence compliance efforts as soon as possible.

As a preliminary point of action, we advise clients to perform an audit in order to ascertain under what security level classification their existing databases fall and to thereby assess the measures required in order to comply with the applicable requirements and obligations under the Regulations.

Contact Person

David Mirchin, Partner, Technology, IP and Data Protection

Tel: +972-3-6103199
Mail: dmirchin@meitar.com

More Information

For more information about Meitar's Technology and Intellectual Property group, click here