February 2018

GORNITZKY&CO

Israel's New Data Protection Regulations will Enter into Force in May 2018 – Is Your Company Ready?*

Israel's new Privacy Protection Regulations (Data Protection), 2017 (the "**Regulations**") impose new obligations on individuals and entities that hold, manage or own databases containing personal data (e.g., customer or human resources databases). Contrary to the existing data protection regulatory requirements in Israel, which are mostly sector-specific (such as requirements that apply to banks, insurance companies, etc.), the Regulations will apply to any business that collects or stores personal data (such as information relating to employees, customers, suppliers, etc.), regardless of its size. The obligations imposed by the Regulations will vary between businesses, and will take into account factors such as the number of people in the database, the types of personal data stored and the purpose of the data collection. Based on these and other considerations, the Regulations distinguish between four types of databases: low security level; medium security level; high security level; and databases managed by an individual.

Obligations imposed under the Regulations include, among others:

- **Database Specification Document –** the database owner is required to prepare a database specification document which must include, *inter alia*, a description of the purpose of the database; the types of data contained in the database; cross-border transfer of data from the database; main data protection risks; and measures to mitigate such risks. The database owner is required to examine, at least once annually, the need to update the database specification document, and to further examine whether the database contains more data than is necessary for the purposes of the database.

- **Data Protection Procedure –** the data protection procedure should specify, among others, instructions regarding the physical security of the database; access permits to the database and its systems; a description of data protection measures used for protecting the database systems; and instructions on the use of mobile devices. The data protection procedure must be reviewed at least once annually.

- **External Vendors –** Prior to providing access to the database to an external vendor, the database owner must evaluate the data protection risks relating to the granting of such access. The services agreement between the database owner and the external vendor must explicitly set out the terms of use of the database by the vendor, including the scope of the data that the vendor is allowed to process; the purposes for which the vendor may use such data; and the manner in which the vendor is to carry out its obligations under the Regulations. The database owner is further required to monitor and supervise the vendor to ensure compliance with the services agreement and the Regulations, to the extent required considering the potential risks due to the vendor's access to the database.

- **Access Permits and Training –** prior to granting employees access to the database (or changing their level of access), the Regulations require: (a) implementing reasonable human resources evaluation and screening measures; and (b) conducting training on the requirements under the Privacy Protection Law, 1981, the Regulations and the company's data protection procedure (see above).

- **Data Breach Notification –** For medium security level and high security level databases, the Regulations require issuing an immediate notification to the Israeli Registrar of Databases (the "**Registrar**") for data protection incidents, such as infringement of the integrity of the data or unauthorized use of the data. The Registrar may, after consulting with the National Cyber Agency, instruct the database owner to further notify the individuals who may be affected by the data protection incident.

- **Other Security Measures –** the Regulations also include requirements on the physical security of the database, access permit management, identification and authentication measures, network security, etc.

The Regulations will come into effect on May 8, 2018, and will impact a wide variety of entities. Companies are encouraged to take steps to prepare for the introduction of the new requirements under the Regulations as soon as possible.

For further information please contact:

Assaf Harel, Partner
assafh@gornitzky.com

Adi Shoval, Advocate
adis@gornitzky.com