
**Legal Update – Information Technologies** **March 2017**

*

Information Security Regulations

*

Please visit us:

www.fbclawyers.com

And follow us:

**Dear Clients and Colleagues,**

On March 21, 2017, the Knesset Constitution, Law and Justice Committee approved the Protection of Privacy Regulations (Information Security) 5777-2017 (hereinafter: the "**Regulations**"). The Regulations mark a landmark change in the field of information security in Israel and they impose substantial obligations on database owners. Among the duties in the Regulations are: the requirement to adopt a comprehensive policy and procedures on information security, mapping out the information systems in the organization and carrying out a risk assessment review, implementing information security practices in the area of human resources management and requirements relating to the reporting of security incidents. In addition, for databases containing information that is more sensitive, the Regulations establish the requirement to carry out vulnerability assessments and penetration tests, and the implementation of advanced security mechanisms. The Regulations will come into force one year following their publication.

**Different Database Security Levels**

In general, the Regulations will apply to every database that is required to be registered under the Protection of Privacy Law. However, some provisions will only apply to medium or high security level databases which will be subject to stricter practices. **Medium security level database**s include, among others, databases that include: medical information, personal information, information on an individual's political opinions or religious beliefs, biometric information, economic information such as the individual's consumer habits, as well as databases designated for direct mailings. **High security level databases** include the information contained in the medium security databases described above, if such information is collected on 100,000 or more individuals or the number of people who are authorized to access the databases is greater than 100.

**Policy Statements, Practices and Officers**

The Regulations obligate every database owner to adopt an information security policy statement that defines the purposes of its database, the ways it is used, the main risks for security breaches and the methods for handling such breaches. It is necessary to update the policy statement from time to time to correctly reflect how the organization is using the database.

In addition, every database owner will be obligated to establish information security procedure that suits the definition of its database. All of the employees in the organization will be bound by the procedures that will among other things, deal with: the mapping and the securing of the information systems in the organization, authorizations to access the databases and the information systems, the security measures that have been deployed, existing security risks and ways of dealing with them - including in real time. Owners of medium and high security databases will be obligated to also include a description of how they back-up the information in their possession, a description of their periodic database checks and a description of how portable devices are used in the organization.

The Regulations also mandate that the Information Security Supervisor, appointed in accordance with the Protection of Privacy Law - whether the appointment is statutorily required or if it is a voluntary appointment - will not carry out another role at the organization that may cause him to be in a conflict of interest (for example, the chief information technology officer or the manager of the information systems in the organization). The Regulations establish that the Supervisor will be subject to the CEO or another senior officer and that the Supervisor shall have all of the required resources to enable his compliance with the Regulations.

**Mapping Information Systems, Vulnerability Assessment and Penetration Tests**

In addition to the policy statements and the internal practices, database owners will be required to prepare and keep a document that outlines the information systems that are connected to each and every database (including hardware, software and user equipment) and the security measures employed to protect them. Once every 18 months, owners of high security databases will also be required to carry out vulnerability assessments and penetration tests on their information systems, deliberate over the results of these assessments and checks and adopt practices and security measures in accordance with the conclusions that are reached.

**Information Security Measures**

The Regulations require database owners to implement various information security measures. For example, database owners will have to ensure, among other things, the physical security of the database, management of access authorizations, establishing identification and verification mechanisms (including strong passwords and sophisticated identification measures), documentation of security incidents on the information systems, the separation between different information systems in connection with the database, and the encrypting of information in transit from the database to public networks.

Further, owners of medium and high security databases will be required to document the physical access to the information systems at the organization, to operate a stringent user identification and authentication

mechanism (including automatic disconnection mechanisms and physical identification measures), to document automatically the electronic access to the information systems at the organization and to keep the documentation data for a period of at least 24 months. The Regulations also mandate that the owner of the database must establish procedures for the backing up and the restoration of the information and must execute, at least once every 24 months, an internal or external audit that is aimed at assessing the level of compliance with the provisions of the Regulations.

**Information Security in Human Resources Management**

The Regulations require database owners to take appropriate measures to ensure that employees who have access to the databases are suitable to receive such access, while taking into account the sensitivity of the information contained in the databases. In addition, database owners will be mandated to hold training sessions for the employees before they receive access to the databases. Owners of medium and high security databases will be required to hold periodic training sessions for their employees – at least once annually. These obligations will also pertain to **current employees in an organization** who have access to the database.

**Reporting an Information Security Incident**

Apart from the provisions relating to information security measures that the organizations must take, the Regulations impose – in certain circumstances – a reporting obligation to the Registrar of Databases for those organizations that experienced information security incidents. The Regulations grant the Registrar of Databases the authority to order such organizations to also report the information security incidents to every individual whose information was revealed.

**Summary**

The Regulations constitute a revolution in the regulation of information security in Israel and their application is far reaching. We emphasize once again – every owner who is required to register his database **will be subject to at least some of the Regulations**. Although the Regulations do not establish which information security measures a database owner must adopt, the Regulations do mandate the adoption of a series of corporate and managerial measures, as well as technological measures that conform to the types of information that the organization keeps and the uses that are made of the information. Therefore, the Regulations demand that each company carries out its own internal assessment and preparation.

Though the Regulations will come into force one year following their publication, we recommend considering beginning the necessary internal processes, since these include both legal and technological aspects which will require cooperation between various professionals both external to and from within the organization.

**This update was written by Adv. Omri Rachum-Twaig**

**Sincerely,**

**Fischer Behar Chen Well Orion & Co.**

**For further information please feel free to contact:**

Adv. Amit Dat adat@fbclawyers.com +972.3.6941320