Israel Privacy Protection Regulations - Duty To Report A "Severe Security Event" To The Privacy Protection Authority

One of the most significant recent developments in data protection in Israel has been the publication of the Privacy Protection Regulations (Data Security) in May 2017. These significant regulations came into effect in May 2018.

The regulations were enacted after extensive consultation with the Israeli public, and in particular the stake holders that would be effected by the regulations. The regulations apply to both private and public sectors and establish organizational mechanisms aimed at making data security part of the management practices of all organizations processing personal data.

It is anticipated that the regulations will considerably advance the level of data security in Israel. They are both flexible, tangible and precise to a degree that offers organizations regulatory certainty and practical tools that are unpretentious to implement.

The regulations classify databases to four groups according to the level of risk created by the processing activity in those databases: high, medium, basic and databases controlled by individuals that grant access to no more than three authorized individuals. The duties of the controllers are determined in accordance with the level of risk. The level of risk is defined by the data sensitivity, the number of data subjects and number of authorized access holders.

In certain circumstances, the Privacy Protection Authority may instruct a database to implement supplementary obligations in order to strengthen the security level of its activities. On the other hand, the Privacy Protection Authority may use its discretion to exempt a database from applying specific details of the obligations in the regulations.

Until May 2018, Israeli law did not include a general duty to notify a party whose personal information was exposed during a cyber breach. Nonetheless, a limited duty to notify a cyber event was set out in the directives which apply to banks and financial institutions and require them to notify the regulator in case of a cyber breach.

The new regulations include a duty to report a "Severe Security Event" to the Privacy Protection Authority. The Privacy Protection Authority has been given the authority to instruct database owners that have been attacked to notify the parties whose information was exposed.

The term 'Severe Security Event' is defined in the Privacy Protection Regulations as follows:

"In a database which is subject to a high level of security – a cyber event in which information included in the database was used or damaged; In a database which is subject to a medium level of security – a cyber event in which a significant part of the database was used or damaged."

The level of security required from a database is determined in the Privacy Protection Regulations according to:

- the number of people whose information is included therein (generally, a database with information regarding more than 100,000 people requires a high level of security);
- the number of people who have authorized access to a database (generally, a database with more than 100 authorized parties requires a high level of security); and
- the nature of the information held in the database.

On October 21, 2018 the Israeli Securities Authority (ISA) published a written position, according to which, in cases of a significant cyberattack, public companies must examine the need to issue an immediate report to the investors notifying them of the attack. According to the position statement, an immediate report is required in the event:

- a company could not operate for some time as a result of a cyberattack;
- a cyberattack influences a company's activity (where a hacked database is protected under the privacy laws this must be referenced);
- a company's computer system is damaged in such a way that it has a material effect on its activities;
- a company must pay a significant amount as ransom due to a cyberattack;
- a company discovers that its computer systems have been exposed to hostile parties; and
- a vulnerability was discovered in products supplied/manufactured by the company.

The Privacy Protection Regulations will likely lead to application of the regulations to any organization established in Israel that is controller or processor of a database, regardless of where the data subjects may be and whether they are Israelis. However, the regulations will likely also extend to foreign-based entities purposefully processing data about Israeli citizens, consumers or employees. To be sure, a hotel in Los Angeles, USA will not have to comply with Israeli law based on an indiscriminate Israeli customer taking a room with his family at the hotel. However, But a U.S.-based parent company of an Israeli subsidiary, which manages a global HR database including rich data about Israeli employees, or a Silicon Valley-based app developer collecting social networking information about thousands of Israeli users, will have to comply with the new regulations despite a lack of physical presence in Israel.

This document provides a general summary and is for information purposes only. It is not intended to be comprehensive nor does it constitute legal advice. If you are interested in obtaining further information please contact our office at:

Schuman & Co. Law Offices
Beit Bynet, 8 Hamarpe Street, P.O.Box 45392
Har Hotzvim, Jerusalem 97774 Israel
Tel: +972-2-581-3760, Fax: +972-2-581-5432
Shalev@schumanlaw.co.il
http://www.schumanlaw.co.il/