CYBER-SECURITY, DATA PROTECTION AND PRIVACY

Israel adopts new regulations for protecting personal data transferred from the EU

On May 7, 2023, the Ministry of Justice published regulations that impose new requirements on owners of databases that contain personal data from the European Economic Area (EEA) - the Privacy Protection Regulations (Instructions Regarding Data Transfers from the European Economic Area to Israel), 5783-2023 (the "**Regulations**").

The Regulations were enacted in the context of a re-evaluation process carried out by the European Union Commission regarding the renewal of the adequacy status granted to Israel in 2011, with regard to transfers of personal data from Europe to Israel. The adequacy status requires that the level of protection of personal information in Israel be equivalent with the level of protection of personal data in the EEA, as regulated by the EU General Data Protection Regulation (GDPR). This recognition is of great importance to the Israeli economy.

1. Applicability.

The Regulations apply to databases in Israel that contain personal data that was transferred from the EEA (excluding data that a data subject provided directly about himself) ("**Qualifying Databases**"). Note that the new requirements will apply to all personal data in Qualifying Databases including, e.g., personal data collected from data subjects in Israel.

2. New requirements under the Regulations.

- Deletion of data: A database owner is required to delete data from the database following the receipt of a written deletion request from the data subject, if:
    - the data was created, received or collected in violation of applicable law,
    - the continued use of the data is in violation of applicable law; or
    - the data is no longer necessary for the purposes for which it was created, received or collected.

  There are certain exceptions for which the database owner may deny such deletion request, such as: (i) freedom of speech; (ii) performance of a legal obligation; (iii) protection of a public interest; (iv) legal proceedings or collection of debts; (v) prevention of fraud, theft or other acts that may impair the accuracy or reliability of the data; or (vi) performance of obligations stemming from an international agreement to which the Government of Israel is a party.
- Data minimization: A database owner is required to implement a mechanism to ensure that the database does not contain data that is no longer required for the purpose for which it was collected or held, or for another legal purpose.

- Data accuracy: A database owner shall implement a mechanism ensure that the data contained in the database is correct, complete, clear and up to date. The database owner must take reasonable measures to correct or delete data that does not meet those requirements.
- Disclosure obligation: A database owner that received data regarding a data subject shall notify such data subject, directly or indirectly through the entity that transferred the data, as soon as possible after the receipt of the data and in any event within a month from the receipt of the data, of the following:
    - the identity of the database owner and the database manager, their addresses and contact details;
    - purpose for the transfer of the data;
    - type of data transferred; and
    - data subject's rights to deletion, correction and review of the data.

Exceptions to this requirement include, e.g., an unreasonable burden, lack of contact details, assumed awareness of the data subject to the said details, and protection of journalism activity.

- Sensitive information: With respect to Qualifying Databases, the Regulations broaden the definition of "Sensitive Information" under the Privacy Protection Law, 1981 to include information about a person's ethnic origin and trade union membership. This means that database owners will be required to register such databases with the Registrar of Databases.

3. Effect.

The Regulations will enter into force as follows:

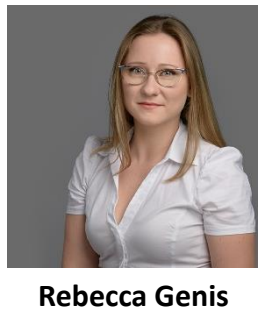
- **On August 7, 2023** – with respect to personal data received from the EEA starting that date;
- **On May 7, 2024** – with respect to personal data received from the EEA prior to August 7, 2023.
- **On January 1, 2025** – with respect to personal data in Qualifying Databases that was not transferred from the EEA.

4. What you should do to comply.

- map your company's databases, specifically with respect to personal data received from the EEA;
- consider separating non-EEA data from Qualifying Databases;
- implement mechanisms to comply with the data minimization and accuracy requirements;
- Review and update the company's privacy policies and agreements under which it receives information from EEA.
- Assess whether there are company databases that require registration following the expansion of the definition of Sensitive Information.

Please feel free to contact us with any questions that you have on this matter.

Assaf Harel, Partner
Leads the Cyber and Privacy Practice
assafh@Gornitzky.com



Rebecca Genis
Senior Associate
rebeccage@Gornitzky.com

This client update was prepared with the assistance of Melisa Poiron.