GDPR & ISRAELI PRIVACY LAW - KEY DIFFERENCES

***Yoheved Novogroder-Shoshan* & *Miriam Friedmann* of *Yigal Arnon & Co*. outline the key differences between GDPR & Israeli Privacy Law.**

Summary

Due to recent changes in global privacy and data protection laws, certain entities may be subject to both Israeli data protection laws and the European Union's General Data Protection Regulation ("GDPR"). There exist substantial differences between GDPR compliance and Israeli law, and certain key obligations under Israeli law exceed GDPR requirements. Companies that adopt a comprehensive GDPR compliance programme may result in partial compliance with Israeli data protection laws, but additional actions must be taken in order to be fully compliant. Increased penalties for data protection violations are likely to come into effect in Israel, which, if passed, will increase the risk profile of non-compliance substantially, and random audits by the Israeli authorities are expected to become a feature of the new environment.

Key Differences between Israeli Data Protection Requirements and GDPR

While a full comparison of Israeli data protection laws and the GDPR is beyond the scope of this article, the list below identifies certain areas in which Israeli laws exceed requirements

under the GDPR. Companies that have implemented robust GDPR compliance programmes will still need to undertake additional efforts in order to be compliant under Israeli law.
Data Security. The GDPR requires controllers and processors to take appropriate technical and organisational measures to ensure the level of security that is appropriate to the level of the risk. By contrast, the Israeli Data Security Regulations (2017) impose specific, granular requirements with respect to personal data collected and maintained in databases. For example, these regulations include detailed requirements for controlling, monitoring and recording database access. They also impose specific requirements and timeframes for performing PEN testing and rotating passwords.

Data Export Restrictions. Subject to specific derogations, the GDPR permits exports of data outside the EU to entities that are determined by the European Commission as having an adequate level of protection of personal data (i.e., appear on the EU 'white list') or when the data exporter provides adequate safeguards. Under Israeli law, in addition to the exporter and importer executing a data transfer agreement, in many cases data subjects will either need to consent to data export, or the data recipient will need to commit to protect the information in accordance with Israeli law. Other grounds legitimising export under the GDPR are not available under Israeli law. In addition, while the GDPR permits data recipients to transfer data to sub-processors in certain cases, these subsequent transfers may violate Israeli law.

Data Protection Officer. Under the GDPR, controllers and processors must designate a Data Protection Officer ("DPO") under certain circumstances. Similarly, under Israeli law, entities must appoint a "data security officer" (whose role is roughly equivalent to that of a DPO) in certain cases. However, Israeli requirements will require appointment of a data security officer where no comparable obligation exists under the GDPR, for example, in the case of entities holding five or more databases requiring registration.

Outsourcing. Under the GDPR, processing of data may be outsourced by a controller to a processor, subject to specific written agreements ensuring that the processor will process the personal data on behalf of and under the instructions of the controllers and subject to specific data protection obligations. Additional specific terms must be added to agreements for the outsourcing of data processing activities in order to comply with Israeli law.

Database Registration. The GDPR does not include the requirement of registration of a database. Israeli law requires that certain databases be registered with the Database Registrar, and for data exports and other activities to be notified to the Registrar.

Who is subject to Israeli Data Privacy Laws?

The GDPR by its terms stipulates that the law applies to organisations (including those situated outside the EU) which offer goods or services to, or monitor individuals in, the EU. Israeli law and court decisions do not definitively define the scope of geographic applicability of Israeli data privacy laws. Depending on the circumstances, it is possible that Israeli law may apply where any of the following are true: (i) servers are located in Israel, (ii) an Israeli person or entity controls how data may be accessed or used; (iii) data is processed in Israel, or (iv) data of Israelis is processed.

Enforcement and Penalties

Violations of Israeli privacy laws are subject to civil and criminal penalties and may be the subject of individual tort claims. In addition, proposed Amendment 13 to the Israeli Protection of Privacy Law (1981), expected to become law in the near future, will vest Israel's data protection authority with enhanced supervisory powers, and will also result in exponentially higher penalties for Privacy Law violations, including fines up to NIS 3.2 million (approximately US$910,000), two percent daily increases for uncured breaches of law, double fines for repeat offenders and personal liability for officeholders.

Recommendations

Entities that are subject to Israeli data protection laws are advised to take steps to ensure compliance with Israeli data protection laws, even where a robust GDPR compliance program exists.

The online link to the article can be found here.