General Data Protection Regulation

The clock is ticking. The European General Data Protection Regulation (short: "**GDPR**") will come into force in May 2018 and Israeli companies need to ensure that they comply with the new laws on data protection and privacy. This bulletin outlines the ten most critical steps that should be taken in preparation for the GDPR.

What is the GDPR?

ERM has summarised the changes that the GDPR will bring, and how they will apply to Israeli businesses, in two previous bulletins (January and August 2016). In a nutshell, though, the GDPR aims to strengthen the rights of data subjects residing in the European Union, and to harmonize the data protection laws of the EU member states.

"**Personal Data**" can be any information which relates to an identified or an identifiable natural person. It can be a person's name, photo, email address, bank details, medical information, or even IP addresses or device identifiers.

One way by which the GDPR intends to ensure strengthened privacy rights of data subjects is by introducing significant fines for non-compliance, which can amount to up to 4% of the global annual turnover, or € 20 million, whichever is greater.

10 Steps to Take Now

1. Check Applicability

Now is the time for an organisation to review its current practices and evaluate whether it is or may be subject to the GDPR. The GDPR will apply even to those data collectors and processors without any establishment in the EU, if they process data of EU residents in connection with offering goods or services. In addition, the GDPR will also apply to a data controller that **monitors the behaviour of individuals** within the EU. "Monitoring" may include, for example, profiling of EU data subjects to analyse or predict the data subject's personal preferences or behaviours.

2. Revise Structure and Responsibility in the Organisation

The heightened obligations under the GDPR, together with the significant fines for non-compliance, require that data protection not only becomes the management's responsibility, but is also brought to the attention

of the entire organisation. Such general awareness can be created through **data protection guidelines** and a detailed regulation of internal responsibilities. Further, an entity with 250 or more employees, or whose core activities regarding data processing consist of a regular and systematic monitoring of EU data subjects, needs to appoint a **data protection officer** who has sufficient knowledge of data protection law and practices.

3. Keep an Overview of Processing Activities

Under the GDPR, organisations need to maintain **detailed records of their data processing activities** (also known as "**data mapping**"). Such data map should provide an overview of the data flow within an organisation and for example outline the various categories of data held and processed, as well as data transfers between different units and to third parties. An organisation should keep such records of processing activities and, in case of an audit by the supervisory authority, be able to present these records in order to demonstrate compliance with the standards for lawful processing.

4. Prepare for Data Breaches

Controllers must notify a personal data breach to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Data controllers should therefore establish internal processes that ensure that the organisation can, at first, identify and handle potential data breaches, which also includes ensuring that data breaches are communicated to the relevant management levels. Further, the organisation must implement the necessary processes for being able to submit a detailed notification of a data breach within 72 hours.

5. Implement Privacy by Design and by Default

These concepts are newly codified in the GDPR and require controllers to ensure that individuals' privacy is considered from the outset of each new processing, product, service or application, and that, by default, only minimum amounts of personal data as necessary for specific purposes are collected and processed. Data controllers should ensure implementation of certain measures, such as pseudonymisation or data minimisation that are designed to ensure data protection principles are applied from the outset of any project.

6. Review Agreements with Third Parties

Any agreements with data processors that are entered into from now on must include certain provisions regarding the implementation of security measures, an obligation to notify the data controller of breaches, maintenance of records of processing activities, etc. Such obligations cannot be avoided by a choice-of-law clause. In addition, agreements that are already in place need to be reviewed and, if necessary, amended. This is especially important in light of the fact that under the GDPR, supervisory authorities have the right to audit compliance with these obligations and may request organisations to provide such agreements for their review.

7. Ensure Transparency and Compliance with Information Duties

Affirmative Consent: An organisation that relies on a data subject's consent for the collection and processing of personal data needs to review the existing mechanism under which consent is obtained: The GDPR requires that consent is given expressly and in an informed manner, for example by ticking a box "I agree". Equally, it should be checked whether the data subjects can withdraw their consent as easily as they have given it.

Information of the Data Subject: A data collector has to provide certain information to data subjects, such as the purpose of the data

processing, contact details of the data protection officer, or information on the transfer of data to other countries, if relevant. Organisations, therefore, should now review and adapt the texts that provide such information to ensure they are in line with the requirements of the GDPR.

8. Revise Profiling Activities

The GDPR restricts "profiling" activities, i.e. the automated processing of personal data in order to **analyse or predict certain aspects** concerning a natural person's economic situation, health, personal preferences, interests, behaviour, location or movement. Individuals have a right not to be subject to a decision based solely on automated processing, which means that the data controller must implement suitable measures to either obtain explicit consent from the data subject, or to include an option for the data subject to "opt out" of the automated processing. Only in certain cases may a controller rely on an authorisation by law, for example, for profiling in connection with monitoring of fraud and tax evasion.

9. Establish a Procedure to Respond to Requests to Data Access and to Data Portability

In addition to data subjects' rights that have been existing under the current legislation, the GDPR contains several new rights for the data subject, such as the right to access his or her personal data collected by an organisation, and receive information on the processing activities. Similarly, a data subject can request to receive his or her personal data in a commonly used format and have it transferred to another data controller. It is therefore important to establish internal procedures in order to satisfy such requests for data access or data portability by data subjects.

10. Prepare for Data Protection Impact Assessments

Under the GDPR, controllers will be required to undertake data protection impact assessments ("**DPIAs**") prior to data processing - in particular processing using new technologies - which is likely to result in a high risk to the rights and freedoms of individuals (for example: automated processing for purposes of profiling). A DPIA assesses the impact of envisaged data processing operations on the protection of personal data, and more specifically the likelihood and severity of risks for the rights and freedoms of individuals resulting from such processing. Such DPIAs will likely play an important role under the GDPR; and controllers should establish guidelines and processes for determining if a data protection impact assessment has to be conducted, and embed DPIAs within the internal operations.

Corporate and M&A and High-Tech and Start-Ups Practices

Epstein Rosenblum Maoz (ERM)'s Corporate and M&A and High-Tech and Start-Ups practices are widely renowned for their cross-border expertise and ERM regularly advises leading Israeli and international clients on the most complex transactions carried out in Israel or by Israeli companies abroad.

Find out more

Please click here to read more about our and Corporate and M&A and High-Tech and Start-Ups practices or contact a member of our team.

Simon Marks, Partner
marks@erm-law.com
+972 (0) 3 606 1605

Natalie Noy, Partner
noy@erm-law.com
+972 (0) 3 606 1626

Dr. Laura Jelinek, Associate
jelinek@erm-law.com
+972 (0) 3 606 1622