Epstein Rosenblum Maoz
Law Office

New EU Data Protection Regulation

What are the changes relevant to Israeli companies operating in the EU?

The General Data Protection Regulation ("GDPR") of the European Union has significant consequences even for those companies located outside of the EU, raising the standards for data protection and introducing new and significantly higher fines for non-compliance to ensure that they comply with the new regulatory framework. The following bulletin summarises those provisions that are most relevant to companies located outside the EU.

WHAT IS THE GDPR?

As noted in ERM's previous bulletin on EU data protection, the GDPR is designed to harmonise national data protection laws across the EU, and to strengthen data protection rights of individuals. The GDPR is going to replace the current EU Data Protection Directive and contains a new set of rules which will be directly applicable to all EU Member States.

WHO WILL IT AFFECT?

The GDPR will apply to both data controllers and data processors, even if the company is established outside the EU, where their processing activities relate to the offering of goods and services to individuals in the EU or to the monitoring of such individuals' behaviour.

One of the most significant changes is that the GDPR will also be applicable to **non-EU based companies** who offer goods or services to data subjects in the EU or process personal data of EU-residents, for example via a website that uses a language or a currency that is generally used in one or more EU Member States, and the possibility of ordering goods and services in that language.

FINES FOR NON-COMPLIANCE

Non-compliance with the GDPR can lead to heavier sanctions, which will also affect businesses located outside the EU. National data protection authorities can impose fines of up to **€20 million or 4% of the global annual turnover** for the preceding financial year, whichever is the greater, for the breaches of certain provisions. This is a steep increase from the initial draft as the fines are intended to make data protection a boardroom issue and to increase its compliance.

DATA PROTECTION OFFICER

Both data controllers and data processors must appoint a Data Protection Officer (a "**DPO**"), regardless of the company size, if their core activities require **regular and systematic monitoring of data subjects on a large scale**, or if their core activities consist of processing of **special categories of data on a large scale**. The DPO needs sufficient expert knowledge of data protection regulations. The responsibilities of a DPO can be outsourced to an external service provider or law firm.

CONSENT REQUIREMENT

The data subject's consent is one of the main legal bases for any processing activities of personal data. The GDPR requires that such consent is **freely given, specific, informed and unambiguous**, and given by a clear affirmative action or a statement, such as ticking a box. As is the case under the current regime, personal data can only be processed for those purposes for which it was originally collected. Consent therefore has to be granted specifically for all the

purposes of the data processing activities. If a company relies on a data subject's consent for collecting and processing personal data, it is recommended to review the current practices and ensure that such consent is valid under the GDPR.

CHILD PROTECTION

The GDPR introduces a higher level of protection for children. Consent from a child in relation to online services will only be valid if it is authorised by a parent. A child is someone under 16 years old, though Member States can reduce this age to 13 years. Additionally, privacy policies of such online services that are aimed at children must be written in very clear and simple language. The national supervisory authorities are expected to monitor such activities that are addressed specifically to children with particular attention.

RIGHT "TO BE FORGOTTEN", RIGHT TO DATA PORTABILITY

A data subject may, under certain circumstances, request that the data controller erase personal information relating to him/her. Consequently, a data controller will have to implement procedures to ensure that it can comply swiftly with erasure requests, and also notify third parties to whom data was disclosed.

The new right to data portability requires that the data controller must provide "*a copy of the personal data undergoing processing*" in machine readable format upon request either to the data subject or directly to another controller. Data subjects can thus **transfer their data from one service provider to another**.

OBLIGATION TO REPORT DATA BREACHES

Another significant change is the new general obligation on companies to report "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*" In the event of such data breach, data controllers must **notify the supervisory authority** "*without undue delay and, where feasible, not later than 72 hours after having become aware of it.*" Where the data breach might result in certain risks to the rights and freedoms of the data subject, such as identity theft, fraud, or loss of confidentiality of data, it also has to be reported to the data subject.

WHAT'S NEXT?

Following its publication in the Official Journal of the European Union, the GDPR will come into effect on 25 May 2018. It is crucial for companies to start preparing for the new regulatory framework as early as possible before this date and to **revise current practices**. Each company is likely to face different challenges under the GDPR. It might be necessary, for example, **to implement new procedures in order to adapt to the new rights of data subjects**, or to adapt the appropriate data protection policies and current agreements with third parties. Companies should also ensure that the security measures they have in place for the personal information collected and processed comply with the GDPR's requirements.

Technology and Corporate and M&A Practices

Epstein Rosenblum Maoz (ERM)'s Technology Practice and Corporate and M&A practice 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. Please click here to read more about our Technology practice and Corporate and M&A practice.

If you have further queries about data transfer or data privacy issues or to learn more about ERM's technology practice please contact a member of our team.

Simon Marks
Partner
marks@erm-law.com
+972 (0) 3 6061605

Natalie Noy
Partner
noy@erm-law.com
+972 (0) 3 6061626

Dr. Laura Jelinek
Associate
jelinek@erm-law.com
+972 (0) 3 6061622