View this email in your browser

Is Your Company Ready for the GDPR?

What is the GDPR?

The new General Data Protection Regulation (the "GDPR") will come into effect on 25 May 2018.

The GDPR sets standards for a uniform level of protection in the "processing" (the collection, recording, storage, or disclosing to third parties) of personal data of European individuals. "Personal Data" may include any information relating to an identifiable person, such as his or her name, ID number, online identifier, or other identifying factors, as well as "sensitive data" such as genetic data, certain biometric data or data concerning health.

The GDPR may apply regardless of the field in which the company operates (high-tech, life sciences, pharmaceutical, banks, software, advertising, etc.), and regardless of the technology used by the company (e.g., blockchain, big data, smart objects, internet of things (IOT), mobile apps or websites).

Does the GDPR Apply to your Company?

Generally speaking, the GDPR applies to: (a) companies established in the EU (such as by having employees or offices in the EU), and (b) companies which are not established in the EU, but either (i) target the EU (by offering goods or services to European individuals), or (ii) monitor the behavior of European individuals (by tracking them online, for example). For companies not established in the EU, a GDPR representative within the EU may have to be appointed.

The GDPR will apply not only to "data controllers" (companies that will determine the "purposes" and "means" of the processing of the personal data), but also to "data processors" (companies performing the processing of personal data on behalf of the

data controller). Companies collecting personal data are typically considered "data controllers" while "processors" include, for example, cloud storage providers or payroll processors.

Key Changes

The GDPR includes some significant changes from the previous European privacy regime (mainly Directive 95/46/EC, which was repealed by the GDPR), providing European individuals (or "data subjects") with greater control over their personal data, while increasing the onus on companies to keep the data secure.

Key changes include:

- Strengthened Transparency and Consent Obligations: Companies collecting and processing personal data need to ensure that they provide all required information under the GDPR to data subjects (such as the identity of the data controller, the purposes of the processing or the recipients of the personal data (including intended data transfers)). Moreover, one of the legal bases of the GDPR must apply to the processing. For example, in certain situations the data subject will be required to provide informed and unambiguous consent for the processing of his or her personal data for the specific purposes established by the data controller. The consent must be demonstrable by the data controller, and subject to withdrawal by the data subject in a simple and easy manner.
- New Data Processor Obligations: The GDPR directly regulates data processors for the first time. For example, under the GDPR, data processors will be required to comply with a number of specific obligations such as record keeping, implementing appropriate security measures or appointing a data protection officer in certain circumstances.
- Security Measures: Data controllers and data processors are required to implement organizational and technical measures, as well as appropriate safeguards (such as encryption or pseudonymisation) aimed to ensure that the personal data processed by them or on their behalf is adequately secured.
- Accountability: Controllers must be able to demonstrate, at any time, compliance with the principles relating to processing of personal data, such as data minimization or the limitation on use to specific purposes.
- Data Breach Notification: Controllers are required to notify the relevant authorities of any data breach within 72 hours, and in certain cases, provide notice to the data subjects. Processors are also required to notify controllers without undue delay.
- Data Subject Rights: New data subject rights have been introduced under the GDPR, such the right to erasure ('the right to be forgotten'), data portability rights and the right to object to profiling.
- Data Protection Officers and Data Protection Impact Assessments: Where large scale processing of "special categories" of personal data (formerly called, "sensitive data") is taking place, a Data Protection Officer needs to be appointed (the requirement applies to both controllers and processors). In addition, where a certain type of processing (in particular using new technologies) is likely to result in a high risk to the rights of data subjects, the controller is required to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data and propose measures to mitigate the risks.

Data Transfers

If your company transfers (whether directly or through third parties) personal data of

European data subjects outside of the EU or European Economic Area (the EU and Iceland, Norway and Liechtenstein), or has employees, suppliers or servers outside of the EU who have access to personal data of European data subjects, it is important to make sure that the transfer is in compliance with GDPR.

There are several methods of achieving compliance with regards to data transfers – companies can rely on the European Commission's adequacy decisions (an up to date list of the jurisdictions which enjoy this status (including Israel) is available here), the EU-US Privacy Shield, standard models clauses, or any of the certifications or codes of conduct, which are expected to be created and approved in the future.

Fines

The potential fines for non-compliance with the GDPR have increased substantially, with fines of up to €20,000,000 or 4% of the annual turnover – whichever is higher.

Additional Remarks

It is important to bear in mind that complying with the GDPR is not a one-time exercise. Companies are required to review their GDPR compliance and their strategy regarding data processing on a regular basis.

Due to the significant obligations and requirements introduced under the GDPR (examples of which have been provided above) we advise companies to commence compliance efforts **as soon as possible**.

As a preliminary point of action, we advise clients to prepare an assessment (and flow chart) of their data processing operations, in order to map out what personal data they are collecting, using and disclosing to third parties, and whether they are doing so as a data controller (or a joint controller), data processor, or in certain cases, both.

To the extent you have any questions regarding the GDPR, or would like our assistance in achieving compliance, feel free to contact us.

Contact Information

David Mirchin, Partner
Technology Group

+972-3-6103199 | dmirchin@meitar.com

For additional information about our firm's Technology group, click here

---

To join our newsletter click here