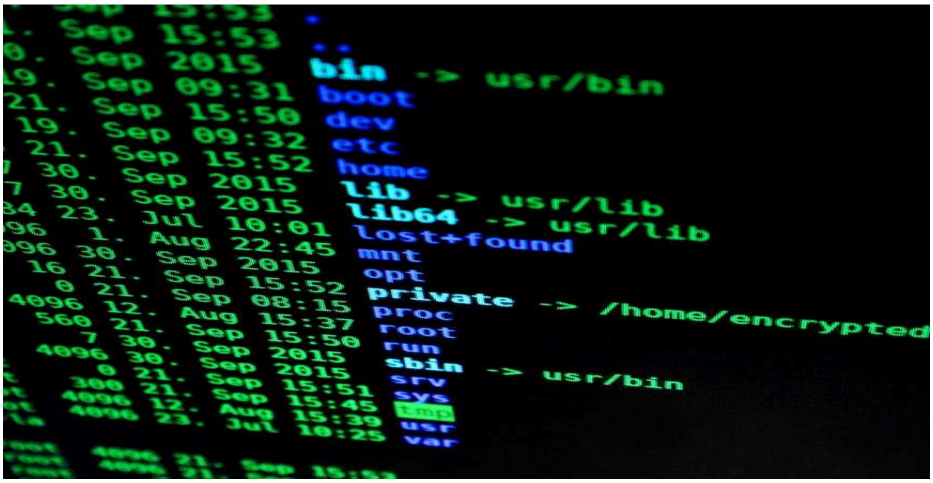
General Data Protection Regulation (GDPR)



This week, Europe's data protection rules will undergo their largest reform in several decades. The General Data Protection Regulation (GDPR) is set to replace the Data Protection Directive, effective as of May 25, 2018.

The GDPR is directly applicable in each EU member state and will lead to a greater degree of data protection harmonization between EU members. The regulation is intended to establish one single set of rules across Europe which EU policy makers believe will make it simpler and cheaper for corporate entities to do business across the Union. Organizations outside the EU are also subject to the GDPR just by collecting data concerning an EU resident.

This article will summarize some of the main provisions and reforms brought about by the GDPR.

1. Definitions

"**Defining Personal Data**"
For purposes of the GDPR “Personal data” is defined as "any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

"Controller"
Means a corporation, person, public authority, agency or other entity which determines the purposes and means of the processing of personal data. According to Article 5 of the GDPR, the Controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data. These are: lawfulness, fairness and transparency, data minimization, accuracy, storage limitation and integrity, and confidentiality of personal data.

"Processor"
Means a corporation, person, public authority, agency or other entity which processes personal data on behalf of the Controller. According to Article 28 of the GDPR, "*Where processing is to be carried out on behalf of a* Controller*, the* Controller *shall use only Processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."*

"Personal Data"
Means any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

"Data Protection Authorities"
Data Protection Authorities ("**DPA**") are independent public authorities that supervise, through investigative and punitive powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the GDPR and relevant national laws. If a company processes data in different EU Member States or is part of a group of companies established in different EU Member States, that main contact point may be a DPA in another EU Member State.

2. Scope
The GDPR applies if either of the Data Controller **or** Processor is based in the EU. The regulation also applies to entities based outside the EU if they collect or process personal data of individuals located inside the EU.

3. Uniformity Throughout the EU
A single set of rules will apply to all EU member states. Each member state will establish an independent Supervisory Authority ("**SA**") to hear and investigate complaints, sanction administrative offences, etc. If a business has multiple establishments in the EU, it will have a single SA as its "lead authority", based on the location of its "main establishment" where the main processing activities take place.

4. Privacy By Design and Privacy By Default
The idea of Privacy by Designs holds that organizations need to consider privacy at the initial design stages of their activities and throughout the complete development process of new products, processes or services that involve processing personal data.

Privacy by Default means that when a system or service includes choices for the individual on how much personal data he/she shares with others, the default settings should be the most privacy friendly ones. Users should be required to "Opt-In" before the organization can collect data from them.

Privacy by Design and Privacy by Default are legal requirements under the GDPR. Successful implementation of both Privacy by Design and Privacy by Default requires that clear policies, guidelines and work instructions related to data protection should be developed and a privacy specialist should be available to assist in applying these requirements.

5. Lawful Basis for Processing

Data may not be processed unless there is at least one lawful basis to do so. Such reasons include the following:

- The data subject has given consent to the processing of personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Controller is subject.
- Processing is necessary to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular if the data subject is a child.

6. Consent

If consent is used as the lawful basis for processing, consent must be explicit for data collected and the purposes the data is used for. Consent for children must be given by the child's parent or custodian, and verifiable. Data Controllers must be able to prove "consent" (opt-in) and consent may be withdrawn at any time.

The area of GDPR consent has a number of implications for businesses who record calls as a matter of practice. The typical "calls are recorded for training and security purposes" warnings will no longer be sufficient to gain assumed consent to record calls. Additionally, when recording has commenced, should the caller withdraw their consent then the agent receiving the call must somehow be able to stop a previously started recording and ensure the recording does not get stored.

7. Data Protection Officer ("DPO")

Under Article 37 of the GDPR, the Data Protection Officer is a **mandatory position** for all entities that collect or process EU citizens' personal data. The DPO's responsibilities include: educating the company and employees on important compliance requirements, training staff involved in data processing, serving as the point of contact between the company and GDPR Supervisory Authorities and monitoring performance and providing advice on the impact of data protection efforts.

8. Pseudonymization

The GDPR recommends "pseudonymization" of personal data to reduce risks from the perspective of the data subject, as a way for Data Controllers to enhance privacy, and, among others, making it easier for Controllers to process personal data beyond the original personal data collection purposes or to process personal data for scientific and other purposes.

Pseudonymization is a technique that is used to reduce the chance that personal data records and identifiers lead to the identification of the data subject whom they belong too. By replacing the most identifying fields in a data record with one or more pseudonyms, which are fictional identifiers, the risk of identification decreases substantially.

9. Data Breaches

The GDPR introduces a duty on all organizations to report certain types of personal data breach to the relevant supervisory authority. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. Organizations must also keep a record of any personal data breaches, regardless of whether they are required to notify.

10. Sanctions

The GDPR has attracted media and business interest in part because of the increased administrative fines for non-compliance.

The administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be "effective, proportionate and dissuasive".
There are two tiers of administrative fines that can be imposed:

- Up to €10 million, or 2% annual global turnover – whichever is higher.
- Up to €20 million, or 4% annual global turnover – whichever is higher.

When deciding whether to impose a fine and the level, many factors may be considered, including: the nature , gravity and duration of the infringement, actions taken by the organization to prevent the infringement and to mitigate the damage suffered, previous infringements by the organization or data Processor, the types of personal data involved and more.

11. Right of Access

The right of access (Article 15) gives citizens the right to access their personal data and information about how this personal data is being processed. A Data Controller must provide, upon request, an overview of the categories of data that are being processed as well as a copy of the actual data. Furthermore, the Data Controller has to inform the data subject on details about the processing, such as the purposes of the processing, with whom the data is shared, and how it acquired the data.

12. Right to Erasure

Under Article 17 of the GDPR individuals have the right to have their personal data erased. The right is not absolute and only applies in certain circumstances, for example when: the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed,

the data subject withdraws consent on which the processing is based, the personal data has been unlawfully processed, and more.

However, there are certain circumstances in which the right to erasure does not apply, including: to exercise the right of freedom of expression and information; to comply with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority, for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing, and more.

13. Data Portability

The right to data portability is one of the fundamental rights in the GDPR. The right to data portability allows data subjects to (1) receive personal data they provided to a Controller in a structured, commonly used and machine-readable format; and (2) to transmit those data to another Controller.

Essentially data portability is the right to transfer personal data from one organization (Controller) to another organization or to the data subject in the context of digital personal data and automated processing.

14. Records of Processing Activities

Each Controller has the responsibility to maintain records of all the processing activities which take place within the organization. This obligation does not apply to organizations employing fewer than 250 persons, unless the processing is of a high-risk nature, including processing of special categories of personal data such as ethnic or health information, or data about criminal behavior.

Summary

The implementation of the GDPR will require comprehensive changes to business practices for companies that had not implemented a comparable level of privacy before the regulation entered into force, especially non-European companies handling EU personal data.

This document provides a general summary and is for information purposes only. It is not intended to be comprehensive nor does it constitute legal advice. If you are interested in obtaining further information please contact our office at:

Schuman & Co. Law Offices
Beit Bynet, 8 Hamarpe Street, P.O.Box 45392
Har Hotzvim, Jerusalem 97774 Israel
Tel: +972-2-581-3760, Fax: +972-2-581-5432
Shalev@Schumanlaw.co.il
http://www.schumanlaw.co.il/