mandaris

Newsletter September 2017

THE GENERAL DATA PROTECTION REGULATION (GDPR)

The increase of the exchange of data between economic and social, public and private sectors across the Union has created the need for a stronger and more coherent data protection framework. The EU General Data Protection Regulation will need to be complied with within and outside the EU territory and is therefore especially relevant for all business that are active on an international level.

The General Data Protection Regulation (GDPR) will replace the current existing EU Data Protection Directive 95/46/EC and will be directly applicable in all Member States without the need for implementing national legislation on the 25 May 2018. In 1995 the EU Data Protection Directive was incorporated into the EEA Agreement in a slightly adapted version resulting in the Directive applying to all EEA countries. Once adopted in the EU, the GDPR will also need to be incorporated into the EEA Agreement to apply also in the EEA countries. While maintaining the same core principles of the Directive, this Regulation introduces significant changes to the IT operations of businesses and the way these businesses, **within and outside the EU**, process personal data of their EU resident customers. A single set of rules will apply to all EU member states and each member state will establish an independent Supervisory Authority to sanction administrative offences, investigate complaints etc. Currently, Switzerland also revises its Data Protection Act, which will take over several features of the GDPR.

The Regulation focuses on the right of individuals to have control over their own personal data, more significantly on the right to data portability, that is, the right to transport his/her personal data from one organization to another.

It is aimed to provide legal certainty, coherence and transparency and to provide natural persons in all Member States with the same level of legally enforceable rights. It defines the obligations and responsibilities for data controllers and processors so as to ensure consistent monitoring of the processing of personal data. Sanctions in all Member States will be uniform and there will be an effective cooperation between the supervisory authorities of different Member States.

To Whom Does this Regulation Apply?

This Regulation applies if the **data controller** (the organization that collects data from EU residents), or **processor** (the organization that processes data on behalf of the data controller), or the **data subject** (the Person) is based in the EU. Therefore, this Regulation applies even to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU (e.g. Switzerland). Non-EU data controllers and processors will need to consider the effects of the Regulation on their operations.

What is 'Personal Data'?

Personal Data is any information relating to an individual, whether it relates to his or her private, professional or public life. This can include a name, a home address, photo, email address, bank details, posts on social networking websites, medical information etc.

Processing

This refers to any operation which is performed on personal data, whether by automated means or not, for instance, collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure, erasure or destruction.

Personal data is to be processed lawfully, fairly and in a transparent manner and shall be collected for a specified, explicit and legitimate purpose/s. They shall be limited to what is necessary in relation to the purpose they are processed.

Processing shall be lawful only if at least one of the following conditions applies:

(a) the data subject has given his/her consent to the processing of his/her data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the interests of the data subject or of another natural person;
(e) 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;
(f) processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of personal data, especially in the case of a child.

Consent

Where processing is based on consent, the controller must be in a position to demonstrate that the data subject has consented to the processing of his/her personal data. If such consent is given in a written declaration, which declaration also concerns other matters, the request for consent for processing must be presented in a clear, unequivocal manner from the other matters. Consent cannot be given for a blanket purpose.

The data subject shall have the right to withdraw his/her consent at any time but this withdrawal shall not affect processing lawfully done before withdrawal.

Right to Access

Data subjects shall have the right to obtain confirmation from an organization of what personal data is held concerning them, how it is being processed, where and for what purpose. Organizations should have procedures in place to handle such requests.

Data Portability

The data subject shall have the right to receive his/her personal data provided to the controller in a structured and commonly used and machine-readable format. Individuals can also ask for their data to be transferred directly from one controller to another. There is no right to charge fees for this service.

Data Protection by Design and by Default

The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate measures, which are designed to implement data-protection principles, such as data minimization, in an effective manner and integrate the necessary safeguards to protect the rights of data subjects.

The controller shall implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose for which it is collected are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's consent to an indefinite number of natural persons.

Right To Be Forgotten

The data subject's right to have all of his/her personal data removed was already present in the previous directive, but under the Regulation the standards have been increased. All entities that process personal data must remove all of that data if one condition (out of a list of six) is met. For instance, when data has been unlawfully processed or when a data subject withdraws previously given consent, where the data is no longer necessary in relation to the purposes for which the data was collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation.

Data Protection Officer

Art 35 of the Regulation states:

"The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body; or
(b) the processing is carried out by an enterprise employing 250 persons or more; or
(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects."

Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks independently. The Data Protection Officer will have professional standing, independence, expert knowledge of data

protection, IT knowledge and will be involved properly and in a timely manner in all issues relating to the protection of the personal data

Data Breaches

Data Breaches need to be reported to the supervisory authority within 72 hours and informed to the data subject without delay.

Records of Processing Activities

The controller or controller's representative shall maintain a record of processing activities. The records shall contain all the following information:

(a) the name and contact details of the controller, controller's representative, data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and the categories of personal data;
(d) the categories of the recipients to whom the data have been or will be disclosed;
(e) where applicable, transfers of data to a third country or an international organisation and identification of that third country or international organisation;
(f) where possible, the planned time-limits for erasure of the different categories of data;
(g) where possible, a general description of the technical and organisational security measures for compliance of processing according to the Regulation.

Certification

Data protection certification and data protection seals and marks to show compliance by controllers and processors to the Regulation shall be introduced. This certification shall be voluntary. Attainment of this certification shall not reduce the responsibility of the controller or processor for compliance with this regulation but serves more as a reassurance for consumers about the high standards of data protection that a controller will have.

Stronger Enforcement & Fines

The Regulation sets out the administrative fines that can be incurred for violation. For less serious violations, the maximum is € 10 million or 2% of total worldwide annual turnover of the preceding year, which ever is higher. For more serious violations, this goes up to € 20 million or 4% of total worldwide annual turnover of the preceding year, which ever is higher.

It is vital for firms to be thoroughly prepared for the advent of GDPR and to start addressing any shortfall in compliance in advance. In order to properly assess which are the areas that need to be strengthened in this respect, an impact assessment, including a data audit, should be carried out to find out where the information resides, what data are personally identifiable and how accessible it is. They must monitor their compliance with data protection policies and regularly review the effectiveness of data handling, processing and security controls.

Organizations must review their policies to help ensure that their business operates effectively in line with the GDPR requirements. Senior management and employees need to be educated about the changes that the GDPR will bring about in their organization and staff training should be provided.
Organizations are to have proper systems in place to record and manage consent of data subjects and ensure an effective audit trail.

Please do not hesitate to contact the author if you have any questions or queries.

Our office locations

Mandaris Ltd.
St. Alban-Anlage 46
CH-4052 Basel
Tel. +41 61 285 17 17
Fax +41 61 285 17 77

Mandaris Ltd.
Beethovenstrasse 49
CH-8002 Zurich
Tel. +41 43 344 33 55
Fax +41 43 344 33 66

Mandaris Ltd.
Bahnhofstrasse 23
CH-6300 Zug
Tel. +41 41 500 01 15
Fax +41 41 500 01 16

Mandaris Group (Malta) Ltd.
Forni Complex 1E, Level 2,
Pinto Wharf,
Valletta Waterfront
Floriana, FRN 1913
Malta
Tel. +356 2779 1900
Fax +356 2713 2410

The author:

Dr. Erika Vella
Dip.Not.Pub., LL.D.
Legal and Compliance Manager (Malta)
erika.vella@mandaris.com
Phone: +356 2779 1900