# GDPR

## PROTECTION OF PERSONAL DATA AFTER 25 MAY 2018

HOW TO PREPARE YOUR COMPANY FOR GDPR?

# Introduction

25 May of 2018 is a breakthrough date for entrepreneurs in the entire European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/45/EC will become enforceable on this date.

As the Regulation is an EU act that is directly applicable in all EU Member States, also Polish entrepreneurs face the challenge of adapting to the regulations adopted in the course of many years work.

The regulation introduces changes to personal data protection system that many call revolutionary.  In a brochure prepared specially for you, we will try to explain the most important issues related to this legal act in the form of questions and answers and indicate the areas in which it may be necessary to undertake adaptation works at your Company's level.

This brochure does not constitute legal or other professional advice.

For detailed information about the process of adapting company to the GDPR requirements, please contact RGW Law Firm.

Anna Porebska, LL.M.
adwokat
a.porebska@rgw.com.pl

# Basic information

## WHAT DOES GDPR STAND FOR?

GDPR is short for Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/45/EC (General Data Protection Regulation).

The GDPR has already come into force on 17 May 2016, however, in accordance with transitional provisions, it will become enforceable on 25 May 2018.

## WHAT IS THE PURPOSE OF THE GDPR?

The GDPR is a result of many years of legislative works at EU level, the purpose of which was to harmonise the principles of personal data protection in all Member States. The GDPR replaces the Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data in force since 24 October 1995.

*n order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.*

*Recital 10 of the GDPR Preamble*

## WHY IS THE PROTECTION OF PERSONAL DATA SO IMPORTANT IN THE EUROPEAN UNION?

Protection of natural persons with regard to the processing of personal data is one of the fundamental rights. Art. 8 (1) of the Charter of Fundamental Rights of the European Union and art. 16 (1) of the Treaty on the Functioning of the European Union provides that every person has the right to the protection of personal data concerning them.

# Scope of the GDPR

## DOES EVERY ENTREPRENUR HAVE TO COMPLY WITH THE GDPR?

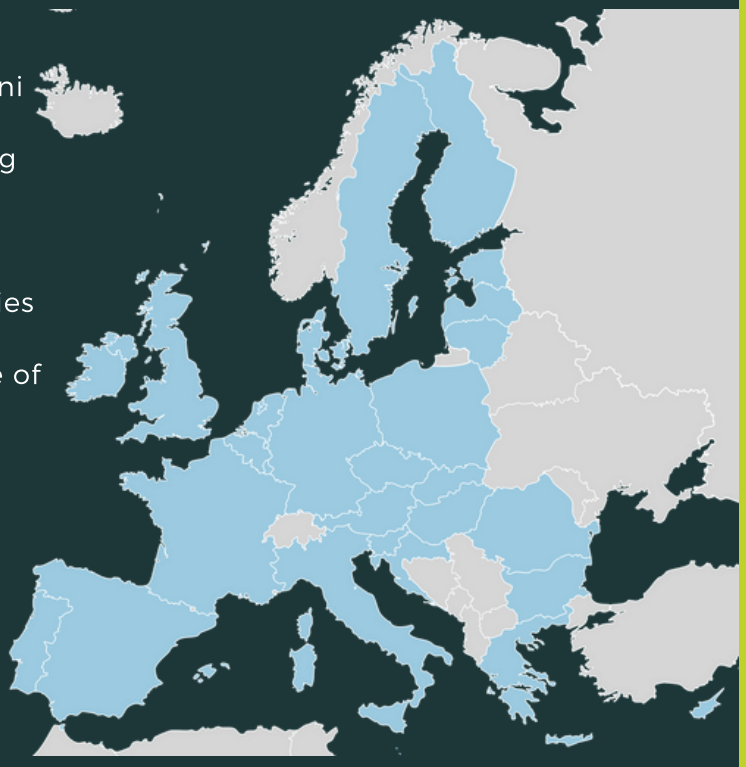
The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of filing system.

If an entrepreneur established in a Member State processes data, regardless of whether the processing takes place in the Union, he is bound by the Regulation. It applies to both, the controller of the data and processor processing data at his request.

## IS THE GDPR ALSO IMPORTANT TO COMPANIES OUTSIDE EU?

This Regulation applies to the processing of personal data of persons who are in the Unioni if the processing activities are related to the offering of goods or services or the monitoring of their behaviour as far as their behaviour takes place within the Union.

Pursuant to the provisions of the GDPR, entities not established in the Union are obliged to designate a representative established in one of the Member States where the data subjects, whose data are processed, are.



# Rules applicable to the processing of personal data

Article 5 of the GDPR introduces six main principles that apply to the processing of personal data.

The rules are:

- lawfulness, fairness, transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality.

## WHEN IS THE PROCESSING OF PERSONAL DATA LAWFUL?

Admissibility of data processing is conditioned by the existence of at least one of premises listed in art. 6 of the GDPR. Processing shall be lawful only if:

- the data subject has given consent to the processing of his or her 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 in order 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 or of another natural person;

- processing is necessary in order 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, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

## WHEN IS THE CONSENT FOR PROCESSING PERSONAL DATA EFFECTIVE?

Consent may be expressed in any manner but the controller should be able to demonstrate it. The GDPR underlines that consent must be voluntary. In particular, consent shall not condition the performance of a contract if data processing is not necessary for this purpose. If consent is given in a form of a written declaration as part of a document concerning also other matters, then request for consent shall be presented in a manner which is clearly distinguishable from other matter in an intelligible and easily accessible form, using clear and plain language. Any part of such declaration which constitutes an infringement of this Regulation shall not be binding.

# Obligations of controllers

## WILL IS STILL BE NECESSARY TO REGISTER DATA SETS IN GIODO (INSPECTOR GENERAL FOR THE PROTECTION OF PERSONAL DATA)?

Previously, there was an obligation to register the sets of personal data in GIODO. The Regulation removes this obligation by introducing in its place registration of personal data by controller or processor's representative. The record should be kept in a written form, including electronic form. The controller is obliged to make the record available to the supervisory authority upon request.

The obligation to keep the record does not apply to an enterprise employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subject, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

## WHAT SHOULD THE RECORD KEPT BY THE CONTROLLER CONTAIN?

- name and contract details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer,
- the purpose of the processing,
- a description of the categories of data subject and of the categories of personal data,
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisation,
- where applicable, transfers or personal data to a third country or an international organisation,
- where possible, the envisaged time limits for erasure of the different categories of data,
- where possible, a general description of the technical and organisational security measures.

## WHAT IS THE ESTIMATION OF THE EFFECTS OF DATA PROCESSING?

The data processing must be preceded by risk evaluation by the controller in order to implement appropriate measures of security. This is particularly important if processing is carried out using new technologies and due to the nature, scope, context and purpose is associated with high risk of infringing the rights and freedoms of natural persons. In particularly risky cases, a prior consultation of the controller with the supervising authority may be necessary, which can give a written recommendation to the controller or act in accordance with tasks and powers laid down in the Regulation.

# Rights of natural persons

## WHAT RIGHTS SHOULD A NATURAL PERSON, WHOSE DATA ARE PROCESSED, BE PROVIDED WITH?

- right of information and access to personal data,
- right to rectification of personal data,
- right to object to data processing,
- right to data portability,
- right of erasure of personal data.

## WHAT SHOULD A NATURAL PERSON BE INFORMED ABOUT WHEN THEIR DATA ARE COLLECTED?

The Regulation regulates the scope of the controller's information duties when personal data are obtained.

The controller should provide, among others, the following information:

- the identity and the contact details of the controller, or controller's representative, or contract details of the data protection officer,

- the purposes of the processing as well as the legal basis for the processing,

- the legitimate interests pursued by the controller or by a third party (if that is the basis of the processing),

- the recipients or categories of recipients of the personal data, if any,

- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation,

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,

- the existence of the right to request the controller access and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability,

- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal,

- the right to lodge a complaint with a supervisory authority,

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into contract, as well as whether the data subject is obliged to provide the personal data of the possible consequences of failure to provide such data, the existence of automated decision-making, including profiling.

# Supervision over the observance of the GDPR

## WHAT WILL BE THE POWERS OF THE NATIONAL DATA PROTECTION AUTHORITY?

The draft Act on the Protection of Personal Data prepared by the Ministry of Digitalisation shows that the Polish supervisory authority (so far the Inspector General for Personal Data Protection – GIODO) will be called the President of the Office for Personal Data Protection (UODO).

UODO's powers will largely coincide with the powers of GIODO, however, UODO's structure is to be extended and apart from examining complaints, monitoring violations and keeping their register, imposing administrative penalties for infringements found, UODO will also be responsible for adopting standard contractual clauses, keeping a list of the effects of processing, giving recommendations regarding data processing, accreditation of certifying entities, cooperation with supervisory authorities from other countries.

## WHAT WILL BE THE FINANCIAL SANCTION FOR INFRINGEMENT OF THE PERSONAL DATA PROTECTION RULES?

For breaching personal data protection rules, the GDPR provides for a sanction in the form of administrative fine, which depending on the type and severity of the infringement may be:

- up to EUR 10,000,000.00 and in the case of undertakings
- up to 2% of its total worldwide annual turnover of the preceding financial year, or
- up to EUR 20,000,0000.00 or 4% of the total worldwide annual turnover.

## WHAT OTHER POWERS DOES THE SUPERVISORY AUTHORITY HAVE?

The supervisory authority shall have all the following corrective powers:

- to issue warning that intended processing operations are likely to infringe provisions of the regulation,
- to issue reprimands,
- to order to communicate a personal data breach to the data subject,
- to order to bring processing operations into compliance with the provisions of the regulation,
- to impose a temporary or definitive limitation including a ban on processing,
- to order the rectification or erasure of personal data,
- to withdraw a certification.

## WHAT CIRUMSTANCES WILL BE TAKEN INTO ACCOUNT WHEN IMPOSING SANCTIONS?

When imposing administrative fine in each individual case due regard shall be given to the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them, the intentional or negligent character of the infringement, any action taken to mitigate the damage suffered, the degree of responsibility of the controller, any relevant previous infringements, the degree of cooperation with the supervisory authority , the categories of personal data, the manner in which the infringement became known to the supervisory authority, adherence to approved codes of conduct or approved certification mechanisms, any other aggravating or mitigating factors.

## CAN A PERSON WHOSE DATA WERE PROCESSED CLAIM COMPENSATION?

The data controller or processor may bear civil liability for infringement of protection of personal data. According to the art. 82 GDPR any person who has suffered material or non-material damage caused as a result of an infringement of the regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

The GDPR introduces a presumption of guilt in this respect. The condition to be exempt from liability is to prove that in no way the given entity is responsible for the event giving rise to the damage. Court proceedings shall be brought before the courts competent under the law of the Member States.

## IS IT OBLIGATORY TO DESIGNATE A DATA CONTROLLER?

Administrator of information security will be taken over by the data protection officer. The appointment of the officer was so far voluntary, but GDPR determines the situations in which it is obligatory to designate data protection officer.

Nothing stands in the way of designating the officer voluntarily also where there is no such obligation.

Detailed rules regarding the selection of a person acting as a data protection officer are set out in the Guidelines of article 29 Working Party regarding data protection officers of 13 December 2016.

## WHAT ARE THE TASKS OF THE DATA PROTECTION OFFICER?

The officer's obligations are, among others, to inform the controller, the processor and employees who process personal data about obligations lawfully incumbent upon them and advising them in this matter, monitoring compliance with data protection regulations and controller's policies in the field of protection of personal data including division of obligation, actions increasing awareness, training of staff participating in processing operations and associated audits, providing on-demand recommendations for the assessment of the impact on data protection and monitoring its implementation, cooperation with the supervisory authority.

## WHICH DOCUMENTATION ON THE PROTECTION OF PERSONAL DATA SHOULD BE KEPT IN A COMPANY?

In accordance with the provisions of the Act on the Protection of Personal Data, the documentation on the protection of personal data includes, inter alia, security policy, IT system management instruction, authorisations for data processing and their records.

The GDPR does not provide for the obligation to keep such documentation, but in the event of an inspection, the entrepreneur will have to demonstrate with some documentation that he processes the data in accordance with the law.

That is why it is so important to implement in the company obligations arising from the GDPR, updating the personal data protection policy and supplementing the documentation before 25 May 2018. This will help to avoid sanctions for infringement of the Regulation.

# WHAT STEPS SHOULD BE TAKEN TO COMPLY WITH THE GDPR REQUIREMENTS?

- Familiarisation with the new regulations
- Review of previously used procedures of processing personal data
- Identifying the type and methods of collecting and processing data in the organisation
- Preparing or updating a data security policy and a plan for implementing new regulations and risk estimation
- Training of managerial staff and employees whose obligations are associated with the processing of personal data
- Implementing changes according to the adopted plan by, among others, assigning roles to appropriate persons, strengthening technical and legal security in the required scope.