How to prepare properly for the implementation of the EU General Data Protection Regulation?

ECOVIS Proventuslaw
Loreta Andziulytė, attorney at Law
Brigida Bacienė, assistant Attorney at Law

→ Tax Services → Accounting → Auditing → Legal Services

Application of the Regulation

The General Data Protection Regulation ("the Regulation") **is a directly applicable law** in the European Union **from 2018, May 25th.**

After the entry into force of the Regulation, the legal regulation of personal data across the European Union is harmonized, which means that data controllers operating on an international level **have the same legal regulation in different countries.**

The regulation places great emphasis on the responsibility and accountability of data controllers, so **it is IMPORTANT to prepare** for this Regulation and **to properly evaluate** the long-term measures required by the Regulation in the field of data protection.

The scope of the Regulation

The Regulation applies to companies that process personal data, so it is important to identify what is considered **"data processing companies**" and what falls under the definition of **"personal data".**

Data processing companies are considered to be those who handle **data processing**.

Data processing is basically any kind of action with personal data such as collecting, storing, sorting, using, accessing, adapting, matching, combining with other data, and similar actions.

Personal data means any information relating to an identified or identifiable natural person, such as IP address or randomly generated telephone number.

Personal data is processed by data controllers (websites, e-shops, phone apps, etc.) and data processors (IT service providers or cloud computing providers), so the provisions of the Regulation apply to both of these categories.

New rules

Regulation:

- tightens duties and responsibilities of data controllers, processors;
- establishes new rights for personal data subjects;
- establishes new responsibilities for controllers and processors of personal data;
- provides for severe sanctions for violations;
- other.

Preparatory actions

- Preparation for the implementation of the rights of data subjects.
- Performing an impact assessment on data protection.
- Arrangement of internal documents related to personal data.
- Appointment of a Personal Data Officer, if necessary.
- Ensuring the security of personal data (adaptation, review of appropriate technical and organizational measures).
- Preparation for the recording of data processing activities.
- Other.

Sanctions

Failure to comply with the requirements of the Regulation may result in fines and, therefore, it is necessary to assess the areas in which problems might arise after the entry into force of the Regulation.

up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	**up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.**

The main innovations of the Regulation

Personal data processing principles

- The data subject has given the consent - this requirement is not new, but after the entry into force of the Regulation, the rules previously drawn up must be reviewed and adjusted in accordance with the provisions of the Regulation.
- The processing of the data is necessary for the performance of the contract.
- Data processing is the result of a legal obligation.
- Data processing is conditional on the protection of the vital interests of the data subject.
- Data processing is stipulated by public interest.
- Data processing is caused by the legitimate interests of the controller or third party.

Evaluation of the valid consent of the data subject

Consent should be given by a clear affirmative act establishing **a freely given, specific, informed and unambiguous indication** of the data subject's agreement to the processing of personal data relating to him or her.

When having the consent of or when trying to receive the consent of the data subjects**, it is necessary to assess**:

- Was the consent freely given and the data subject had the opportunity to refuse to give such consent?
- Is there the purpose for which data is collected and will be processed (is the new purpose in line with the valid consent)?
- Is there a term indicated for which the consent was given?
- What data with this consent have been collected and for what purpose are they used in practice?
- Are there any connections among the purposes for which data are collected or intended to be used?
- Are the appropriate safeguard measures granted?
- Is there a possibility to cancel the consent?

Rights of the Data subject

- Right to be forgotten;
- Right to restrict data processing;
- Right to data portability;
- Right to know about the processing of your personal data;
- Right to access your personal data;
- Right to request correction of inaccurate data or to supplement incomplete data;
- Right to disagree with the processing of personal data.

The data controller must ensure the proper implementation of these rights.

Large volume of data and profiling

Requirements:

- Use impersonal data that has been given pseudonyms.
- Adhere to the requirement of proportionality and minimum data processing.
- It is necessary to prepare proofs that impersonal data has been used for profiling.
- It is necessary to prepare to be able to provide information to data subjects about their data and it‘s movement.

Threats:

- Old, invalid data is used for profiling.
- Discrimination against individuals or groups.
- Limitation of freedom of information.
- Excessively large volume of processed data.
- Data processing for purposes other than those data was collected for.

Responsibilities of Data controller and Data processor

The data controller should only use such processors who provide sufficient guarantees regarding their expertise, reliability and resources required to implement the technical and organizational measures that are in compliance with the requirements of the Regulation.

Data processing by the data processor should be governed by an agreement or other legal act in accordance with the law of the EU or the Member State which sets out **the obligations of the data processor to the data controller**, the **subject matter and duration of the data processing**, **the nature and purpose** of the data processing, **the type of personal data and categories of data subjects.**

The Regulation stipulates that responsibility for the agreement will have to be shared both between the controller and the data processor, and it is therefore essential to have professionally prepared agreements for the processing of personal data.

If the processor defines the purposes and means of data processing in violation of the requirements of the Regulation, the data controller shall be considered as the data controller in relation to the processing of the data.

Infringement notice

The obligation to inform the State Data Protection Inspectorate of the threat to the security of personal data, therefore, it is necessary to ensure that appropriate procedures are established for detecting, reporting and investigating personal data security violations.

We recommend the take the following actions:

- To review violation management procedures;
- To assess the emergence of threats "from the inside out" and "from the outside to the inside";
- To grant the storage of data processing records;
- To execute the real-time tracking and control of users who process personal data.

Data protection officer

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, except for courts acting in their judicial capacity;

(b) 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 on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data.

Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, **the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.**

A data protection impact assessment **shall in particular be required in the case of:**

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

Data protection impact assessment

The State Data Protection Inspectorateshall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. By publishing a list, a business that processes personal data of its customers will have to check whether it is among the entities subject to such impact assessment.

Impact assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Preparation for the Regulation – „Inventory“ of processed data

It is necessary to evaluate whether the current process of data processing complies with the requirements of the Regulation.

During the review of the data management process, the following questions need to be answered

- where the data is obtained?
- whose and what personal data is being processed or what data is planned to process?
- for what purpose are these data processed?
- who and where is this data being processed, how the storage and destruction is granted?
- for how long is such data processed?
- are there excess data processed?
- what is the data movement?
- are the rights of data subjects indicated in Regulation granted, such as the right to be forgotten, the right to data portability, the right to be informed and other?
- are internal rules and / or procedures governing data processing developed?
- revision of contracts for the provision of personal data and other agreements;
- Other.

Preparation for the Regulation – „Inventory“ of processed data

Be sure to check ***if you really have adequate data subjects' consents*** regarding the processing of personal data, or whether the content of the consent clearly and correctly identifies the purposes, scope, and terms of data processing.

It is necessary to decide ***on the organizational / technical measures*** that will ensure that the data subjects' rights, such as access to processed data, modification, erasure of data ("right to be forgotten") or the right to data portability in a structured, commonly used and machine-readable format, are met., etc.

It is necessary to decide **who will be responsible** for informing the data subjects and the State Inspectorate about violations of personal data security.

It is necessary to assess whether there is an obligation to appoint a **Data Protection Officer.**

THANK YOU FOR YOUR TIME!

ECOVIS ProventusLaw

Loreta Andziulytė, Attorney at Law

Brigida Bacienė, Assistant Attorney at Law

Mėsiniu str. 5, Vilnius

Email: info@proventuslaw.lt,

www.ecovis.lt