General Data Protection Regulation

European Parliament and Council

Index

Introduction

In April 2016 the European Parliament and the Council approved a new Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

Introduction

Rapid technological developments and globalisation have brought new challenges for the **protection of personal data**. In this regard, the scale of the collection and sharing of personal data has increased significantly, and technology allows companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.

Those developments require a **strong and more coherent data protection framework** in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data; and legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

In this context, in **April 2016** the European Parliament and the Council approved the **Regulation (UE) 2016/679**[1], on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Some of the most relevant aspects of this Regulation are the following:

- New **rights for data subjects** (natural persons) are introduced. Among others, the Regulation includes the 'right to be forgotten', the right to access to personal data, the right to data portability, etc.
- Several **obligations of controllers and processors** are set out regarding the processing of personal data. For example, proper technical and organizational security measures must be implemented.
- Supervision of the regulatory framework is enhanced by creating **independent supervisory authorities** in each Member State, and through certain **administrative and judicial provisions**.

This technical note includes an analysis of the **new data protection framework** set out by this Regulation.

(1) In April 2016 the Directive 2016/680 was also approved, but it will not be analysed as it refers to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences.

Index

Executive summary

The Regulation includes, among other aspects, principles on data processing, rights of the data subjects, and obligations of the controllers and processors

Executive summary

Scope of application

- Protection of **natural persons** (or **data subjects**) with regard to the processing of personal data.
- It applies to **controllers and processors**[1] **in the UE**, and to those who are not established in the UE where the processing activities are related to **data subjects in the UE**.

Regulatory context

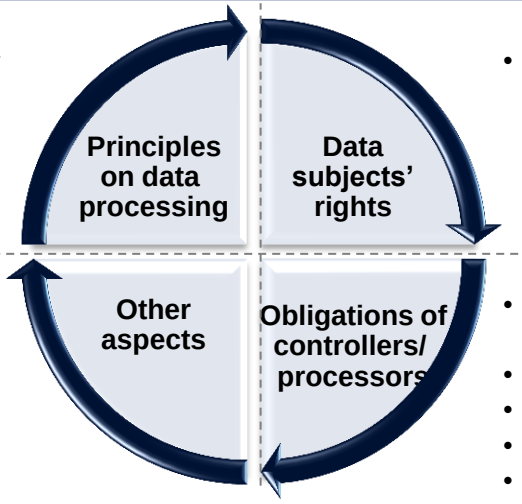
- **Directive 95/46/CE**, on protection of personal data[2].

Next steps

- The new Regulation will be applicable from **May 25 2018**.

Main content

- **Principles** (data processed lawfully, fairly and in a transparent manner, etc.)
- **Prohibition of sensitive data processing** (with exceptions)



- Right of **information**, right of **access**, right of **rectification**, right **to be forgotten**, right to **data portability**, right to **object**, etc.

- **Independent supervisory authorities**
- **European Data Protection Board**
- **Remedies and penalties**
- Data transfer to **third countries**

- **General obligations** (e.g. protection **"**by design and by default")
- **Personal data security**
- **Impact assessment**
- Data protection officer (**DPO**)
- **Codes of conduct and certifications**

(1) The annex includes a list of some key definitions used for the purpose of the Regulation (e.g. processor, controller, etc.).
(2) This Directive shall be repealed once the Regulation on data protection enters into force.

Executive summary

Scope of application

This Regulation does not only refer to the activity of controllers and processors established in the EU, but also applies to those established outside the EU when data subjects are in the EU and processing is related to the offering of goods and services or behaviour control

Scope of application

Scope of application

- This Regulation lays down rules relating to the **protection of natural persons** with regard to the processing of personal data, and **does not cover** personal data which concerns **legal persons**.
- It 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 a **filing system**.

Exceptions

- This Regulation **does not apply** to the processing of personal data:
  - In the course of an **activity which falls outside the scope of Union law**.
  - By the Member States when carrying out activities regarding **external policy and national security**.
  - By a natural person in the course of a **purely personal or household activity**.
  - By competent authorities for the purposes of the prevention, investigation, detection or prosecution of **criminal offences** or the execution of **criminal penalties**.

Territorial scope

- This Regulation applies to the processing of personal data:
  - In the context of the activities of an establishment of a **controller or a processor in the EU**.
  - Of **data subjects who are in the EU** by a controller or processor not established in the EU, where the processing activities are related to:
    - The offering of goods or services in the EU.
    - The monitoring of their behaviour as far as their behaviour takes place within the EU.

Index

Detail

Principles of data processing

The Regulation includes several principles regarding the processing of data that controllers must ensure. In this respect, it is worth highlighting the principle of lawfulness, which is fulfilled only where some conditions are met (e.g. consent)

Principles of data processing (1/2)

Principles

- The controller shall ensure that personal data is:
  - Processed **lawfully, fairly and in a transparent manner**.
  - Collected for **specified, explicit and legitimate purposes**.
  - **Adequate, relevant and limited** in relation to the purposes for which they are processed.
  - **Accurate** and, where necessary, **kept up to date**.
  - Kept in a form which permits **identification** of data subjects for **no longer than is necessary**.
  - Processed in a manner that ensures **appropriate security** .

Lawfulness

- Processing shall be lawful only if and to the extent that **at least one** of the following applies:
  - The data subject has given **consent**.
  - Processing is **necessary**:
    - For the **performance of a contract** to which the data subject is party, or for compliance with a **legal obligation** to which the controller is subject .
    - In order to protect the **vital interests** of the data subject or of another natural person .
    - For the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller .
    - The purposes of the **legitimate interests** pursued by the controller or by a third part[1].

Certain conditions for the consent of the data subject

- The controller shall be able to **demonstrate that the data subject has consented** to processing of his or her personal data.
- The data subject shall have the **right to withdraw his or her consent** at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal..
- When assessing whether consent is **freely given**, utmost account shall be taken of whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Special conditions **applicable to child's consent** are set out (e.g. minimum age of 16, or consent shall be given by the parents).

(1) Except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Detail

Principles of data processing

The Regulation offers special protection to the processing of sensitive data (e.g. data revealing racial or ethnic origin, genetic data, etc.), prohibiting the processing except under certain circumstances, such as when the data subject has given his or her explicit consent

Principles of data processing (2/2)

Prohibition of sensitive data processing

- The processing shall be **prohibited** in relation to:
  - Personal data reveals **racial or ethnic origin**, **political opinions**, **religious or philosophical beliefs**, or **trade union membership**.
  - **Genetic data** and **biometric data** for the purpose of uniquely identifying a natural person.
  - Data concerning **health** or data concerning a natural **person's sex life or sexual orientation**.

Exceptions

- Nevertheless, the prohibition shall not apply when **at least one** of certain conditions is met. Among others, the Regulation sets out the following exceptions:
  - The data subject has given **explicit consent** to the processing of those personal data .
  - Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment** and social security and social protection.
  - Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other **not-for-profit body** with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body.
  - Processing is necessary for reasons of substantial **public interest**.

Detail

Rights of the data subject

The Regulation also establishes several rights to be exercised by the data subject. For instance, the data subject is entitled to a right of information, by which the controller shall provide certain information in a concise form

Rights of the data subject (1/3)

Right to information

- The controller shall take appropriate measures to provide certain information in **a concise, transparent, intelligible and easily accessible form**. The information shall be provided **in writing or** by other means (e.g. electronic means). When requested by the data subject, the information may be provided **orally**.
- In particular, the information that shall be provided by the controller is the following[1]:

	Data obtained from the subject	Data no obtained from the data subject
The identity and the contact details of the controller	✓	✓
The contact details of the data protection officer	✓	✓
The purposes of the processing of personal data	✓	✓
The categories of personal data concerned	✗	✓
The recipients or categories of recipients of the personal data	✓	✓
The legitimate interests pursued by the controller	✓	✓
The controller´s intention to transfer personal data to a third country or international organisation	✓	✓
The period for which the data will be stored	✓	✓

	Data obtained from the subject	Data no obtained from the data subject
Right to request from the controller access	✓	✓
Right to rectification and erasure of personal data	✓	✓
Right to restriction of processing of personal data	✓	✓
Right to data portability	✓	✓
Right to object	✓	✓
Right to withdraw the consent	✓	✓
Right to lodge a complaint with a supervisory authority	✓	✓
Existence of automated decision-making, including profiling	✓	✓
Source from which the personal data originate	✗	✓

(1) In any case, it shall be provided free of charge. However, there is no obligation to provide the information under certain conditions (e.g. the data subject already has the information).

Detail
Rights of the data subject

Further, the data subject is also entitled to the right of access, right to rectification, right 'to be forgotten', right to restriction of processing…

Rights of the data subject (2/3)

Right to access

- The data subject shall have the right to obtain from the controller **confirmation as to whether or not personal data concerning him or her are being processed**, and in that case, **access to the personal data**.
- The controller shall provide a **copy of the personal data** undergoing processing.

Right to rectification[1]

- The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data** concerning him or her. Moreover, the data subject shall have the right to have **incomplete personal data completed**, including by means of providing a supplementary statement.

Right to erasure ('right to be forgotten')[1]

- The data subject shall have the right to obtain from the controller the **erasure of personal data** concerning him or her. The controller shall have the obligation to erase personal data **without undue delay** where **one of the following conditions applies**:
  - The personal data are **no longer necessary** in relation to the initial purposes.
  - The data subject **withdraws consent**, or opposes to the processing.
  - The personal data have been **unlawfully processed**.
  - The data have to be erased for **compliance with a legal obligation**.
  - The personal data have been collected in relation to the **offer of information society services.**
- However, there are **exceptions to the right to erasure** (e.g. public interest reasons, right of freedom of expression and information, etc.).

Right to restriction of processing[1]

- The data subject shall have the right to obtain from the controller **restriction of processing**, and shall be informed by the controller, where one of the following applies:
  - The **accuracy of the personal data is contested** by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
  - The processing is **unlawful**.
  - The controller **no longer needs the personal data** for the purposes of the processing, but they are required by the data subject for the establishment of legal claims.

(1) The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out.

Detail
Rights of the data subject

…right to data portability , right to object and right to not being subject to a decision based only on automated processing

Rights of the data subject (3/3)

Right to data portability

- The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a **structured, commonly used and machine-readable format** and have the right to transmit those data to another controller, where:
  - The processing is based on **consent** or on a **contract.**
  - The processing is carried out by **automated means**.
- Moreover, the data subject shall have the right to have the personal data **transmitted directly from one controller to another**, where **technically feasible**.
- Nevertheless, there are some **exceptions** to this right (e.g. reasons of public interest).

Right to object

- The data subject shall have the right to **object** at any time , on grounds relating to his or her **particular situation**, to processing of personal data concerning him or her. The controller shall no longer process the personal data unless he demonstrates **legitimate grounds** which **override the interests** of the data subject.
- Where personal data are processed for **direct marketing purposes**, the data subject shall have the right to object at any time to processing of personal data, which shall no longer be processed for such purposes.

Automated individual decision-making

- Except in some cases, the data subject shall have the right not to be subject to a decision **based solely on automated processing**, including **profiling**.

UE bodies or Member States may **restrict** by way of a **legislative measure** the scope of the obligations and rights previously exposed for several reasons (e.g. national security, defence, public security, etc.)

Detail

Obligations of controllers and processors

After the range of rights of data subjects, the Regulation establishes several obligations the controllers and processors shall comply with. For instance, the processor shall implement data protection by design and by default

General obligations

Controller[1]

- The controller shall implement appropriate **technical and organisational measures**, including appropriate **data protection policies**, to ensure compliance with the regulatory framework. Those measures shall be **reviewed and updated** where necessary.

Protection "by design and by default"

- The controller shall implement, **at the time of the determination of the means for processing and at the time of the processing itself**, appropriate technical and organisational measures (e.g. pseudonymisation) which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.
- The controller shall implement appropriate technical and organisational measures for ensuring that, **by default**, only personal data which are **necessary for each specific purpose** of the processing are processed.

Records

- Each controller shall maintain a **record of processing activities under its responsibility** (e.g. purposes of the processing, categories of recipients, general description of the technical and organisational security measures, etc.).

Processor[1]

- Where processing is to be carried out on behalf of a controller, it shall use only **processors** providing **sufficient guarantees** to implement appropriate technical and organisational measures.
- Processing by a processor shall be governed by a contract that stipulates, among other requirements, that the processor:
  - Processes the personal data only on documented **instructions** from the **controller**.
  - Assists the controller by appropriate **technical and organisational measures**.
  - At the choice of the controller, **deletes or returns all the personal data** to the controller after the end of the provision of services.
- Each processor shall maintain a **record of processing activities** carried out on behalf of the controller.

(1) When the Regulation applies to controllers and processors outside the EU, they shall designate in writing a representative in the UE.
(2) The processor shall not engage another processor without prior authorization of the controller.

Detail

Obligations of controllers and processors

Regarding security, the controller and the processor shall implement appropriate technical and organisational measures according to the risk. Moreover, in case of a security breach, a notification to the supervisory authority and to the data subject shall be made

Security of personal data

Security of processing

- Taking into account several aspects (specially the risks that are presented by processing[1]), the **controller** and the **processor** shall implement appropriate **technical and organisational measures** to ensure a level of security **appropriate to the risk**, including, among others:
  - the **pseudonymisation** and encryption of personal data.
  - the ability to ensure the ongoing **confidentiality, integrity, availability and resilience** of processing systems.
  - the ability to **restore the availability and access** to personal data in a timely manner in the event of a physical or technical incident.
  - a process for **regularly testing, assessing and evaluating** for ensuring the security of the processing.
- Adherence to an approved **code of conduct** or **certification mechanism** may be used as an element by which to demonstrate compliance with the security requirements.

Notification of a security breach

- A difference must be made between the notification of a personal data security breach to the **supervisory authority** and the notification to the **personal data subject**.

Supervisory authority

- **The controller** shall **without undue delay** and, where feasible, **not later than 72 hours** after having become aware of it, notify the personal data breach[2].
- This notification shall have a **minimum content** specified in the Regulation (e.g. nature of the personal data breach, likely consequences , etc.). The controller shall **document** any personal data breaches .
- The **processor** shall notify the **controller** without undue delay of the breach.

Data subject

- When the personal data breach is likely to result in a **high risk to the rights and freedoms**, the controller shall communicate it to the data subject **without undue delay**. It shall include a **minimum content** specified in the Regulation (e.g. likely consequences, etc.), and use **clear language**.
- The communication shall not be required in **certain specified cases** (e.g. the controller has implemented appropriate technical and organisational protection measures and were applied).

(1) Derived from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
(2) When the notification is not made within 72 hours, it shall be accompanied by the reasons.

Detail

Obligations of controllers and processors

Another amendment introduced by the new protection framework is the obligation of the controller to conduct an impact assessment of the processing when it is likely to result in a high risk to the rights of data subjects

Data protection impact assessment

Impact assessment

- Where a **type of processing** in particular using new technologies, is likely to result in a high risk to the rights of natural persons, the **controller** shall carry out an **assessment of the impact** of the processing operations on the protection of personal data[1].
- A data protection impact assessment shall be required in certain case specified by the Regulation (e.g. processing on a large scale of special categories of data). The supervisory authority shall make public a list of the kind of processing operations for which no data protection impact assessment is required.
- The assessment shall contain **at least**:
  - A description of the envisaged processing **operations** and the **purposes** of the processing.
  - An assessment of the **necessity and proportionality** of the operations in relation to the purposes.
  - An assessment of the **risks** to the rights and freedoms of data subjects.
- The controller shall **seek the advice of the data protection officer**.

Prior consultation

- The controller shall **consult the supervisory authority** prior to processing where a data protection impact assessment indicates that the processing would result in **a high risk** in the absence of measures taken by the controller to mitigate the risk .
- Where the supervisory authority is of the opinion that the intended processing would infringe this Regulation, the **supervisory authority** shall provide **written advice** to the **controller** (and where applicable to the processor) within period of up **to 8 weeks of receipt** of the request for consultation (it may be extended for other 6 weeks).

(1) A single assessment may address a set of similar processing operations that present similar high risks.

Detail

Obligations of controllers and processors

The Regulation also establishes the requirement of designating a data protection officer (DPO) in certain cases. Further, it also includes other provisions in relation to codes of conduct and certification

Data protection officer and codes of conduct and certification

Data Protection Officer (DPO)

- The **controller** and the **processor** shall designate a data protection officer in any case where[1]:
  - The processing is carried out by a **public authority or body**.
  - The core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of **data subjects on a large scale**.
  - The core activities of the controller or the processor consist of processing on a **large scale of special categories.**

Position of the DPO

- The controller and the processor shall ensure that the data protection officer is involved, **properly and in a timely manner**, in all issues which relate to the protection of personal data. In that sense, they shall provide the **necessary resources**, and ensure the DPO **does not receive any instructions** regarding the exercise of those tasks. Data subjects may contact the DPO.

Tasks of the DPO

- The DPO shall have **at least** the following tasks :
  - To **inform and advise** the controller or the processor of their obligations.
  - To **monitor compliance** with this Regulation and with the policies of the controller or processor.
  - To provide advice where requested as regards the **data protection impact assessment**.
  - To **cooperate** and act as the contact point for the **supervisory authority**.

Codes of conduct

- Associations and other bodies representing controllers or processors may prepare **codes of conduct** or **amend or extend such codes**, for the purpose of specifying the application of this Regulation (e.g. issues regarding pseudonymisation, rights of data subjects, etc.).
- The **monitoring** of compliance with a code may be carried out by a body which has an appropriate level of expertise in relation to the subject and is accredited by the competent supervisory authority.

Certification

- **Data protection certification mechanisms, seals or marks approved** by a certification body or supervisory authority may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are **not subject to this Regulation.**

(1) The DPO shall be designated on the basis of professional qualities. A group of undertakings may appoint a single DPO provided that it is easily accessible from each establishment.

Detail

Other aspects

Finally, the Regulation addresses certain additional issues regarding the oversight of the compliance of the regulatory framework, such as the creation of independent supervisory authorities or the penalties regime

Other aspects

Independent supervisory authorities

- Each Member State shall provide for one (or more) **independent public authorities** to be responsible for monitoring the application of this Regulation , which shall act **independently.**
- The Regulation establishes the **tasks** each supervisory authority shall carry out on its territory (e.g. to monitor the application of this Regulation, to promote the awareness of controllers and processors of their obligations, etc.).
- Furthermore, the Regulation specifies the **investigative powers** (e.g. to carry out investigations in the form of data audits, to obtain from the controller and the processor access to any kind of information, etc.) and also the **corrective powers** (e.g. to sanction the controller or the processor in case of infringement of the present Regulation).

European Data Protection Board

- The **European Data Protection Board** is established, and shall act **independently** .
- The Regulation specifies the **tasks** of the Board (e.g. to ensure the correct application of this Regulation, to advise the Commission on any issue related to the protection of personal data, etc.).

Remedies and penalties

- Every data subject shall have the right to lodge a complaint with a **supervisory authority** if he or she considers that the processing of personal data infringes the Regulation.
- Furthermore, any person who has suffered **material or non-material damage** 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 **supervisory authority** may impose **administrative fine**s (e.g. the infringement of certain obligations may lead to the imposition of fine up to 20M€ or 4% the total worldwide annual turnover of the preceding financial year, whichever is higher).

Transfer of personal data to third countries

- Any transfer of personal data which are undergoing processing (or are intended for processing) to a **third country or to an international organisation** shall take place only if **certain conditions** laid down in this Regulation are complied with by the controller and processor.

Index

Annex
Definitions

Some useful definitions used for the purpose of this Regulation are included below

Definitions

Processing

- Any **operation or set of operations which is performed on personal data** or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling

- Any form of **automated processing** of personal data consisting of the use of personal data to evaluate **certain personal aspects relating to a natural person**, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation

- The **processing of personal data** in such a manner that the personal data **can no longer be attributed to a specific data subject without the use of additional information**, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Filing system

- Any **structured set** of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Controller

- The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines **the purposes and means of the processing**.

Processor

- Natural or legal person, public authority, agency or other body which **processes personal data** on behalf of the controller .