Introduction to GDPR

Document number	20171017
Author	P.Leclercq - pl@osix.be
Owner	P.Leclercq
Version	1.0
Date	2017-10-17
Status	Released

Goals

- Protect the right of EU subjects to protection of personal data;
- Facilitate the exchange of personal data within the EU.

Scope

GDPR applies to the processing of personal data of natural persons wholly or partly by automated means, or as part of a filing system.

GDPR is a European Regulation, so it does not have to be translated into the different Member States' law like a Directive. It is immediately applicable as of the date of its entry into force and is the same for all Member States.

Territorial Scope

GDPR applies to:

- Controllers and processors established in the EU;
- Controllers and processors not established in the EU but processing personal data of EU subjects
    - If they offer goods or services to EU subjects;
    - If they monitor the behaviour of subjects within the EU.

Principles

1. Personal data must be processed lawfully, fairly and transparently.
2. Collection must be specific, legitimate and explicit.
3. Data minimisation: the collection of personal data must be relevant and limited to what is necessary for the processing.
4. Personal data must be accurate and kept up to date.
5. Personal data must be kept in a form permitting identification only for as long as it is necessary for the processing.
6. Personal data must be processed with adequate security against unlawful processing, loss, destruction or damage.

Lawfulness

Processing is lawful if

- Data subject has given consent, or
- Processing is necessary for the execution of a contract, or
- Processing is necessary for compliance with legal obligation, or
- Processing is necessary to protect vital interest of data subjects, or
- Processing is necessary for public interest or performed in the exercise of an official authority, or
- Processing is necessary for the legitimate interest of the controller or a third party, except where it is overridden by the fundamental rights of the data subject (esp. children).

Consent

Data controller must be able to demonstrate that the data subject has given his consent.

If the consent is part of a written declaration, the consent part must be easily distinguishable.

Data subject has the right to withdraw his consent at any time, as easily as giving consent.

For children younger than 16 year, the consent must be given by a holder of parental authority. (Member States can lower the minimum age, but not under 13 year).

Special Categories of Personal Data

Processing of special categories of personal data (racial, ethnic, political, religious, union membership, health, biometric, genetic, sexual) is prohibited.

Exceptions:

- The data subject has given consent;
- It is necessary for social security, vital interest, performed for a legitimate activity by a non-profit, data is already public, judiciary matters, public interest, medical reasons, archive.

Processing of personal data related to criminal convictions may only be performed by official authority.

Rights of the Data Subject

Transparency

At collection time, the following information must be given to the data subject:

- Identity and contact of the controller;
- Contact details of the DPO when applicable;
- Purpose of the personal data processing;
- Where the processing is based;
- Recipients of the personal data;
- Whether the controller intends to transfer personal data to a third country or an international organisation;
- Retention period;
- Existence of rights to access, rectification, erasure, restriction, portablility;
- Right to withdraw consent;
- Right to complain to the supervisory authority;
- Whether the provision of personal data is contractual, needed for a contract, and the consequences of not providing the data;
- The existence of an automated decision-making process.

If the information has not been given by the data subject, the information on the source of the data must be added.

Access

The data subject has the right to request the data held by the controller. The controller has 1 month to answer.

The information to be given includes the information needed at collection time, plus the data itself.

First request is free, subsequent ones may be charged for at a fair amount.

Rectification

The data subject has the right to have his data corrected in case of inaccuracy.

Erasure

The data subject can request the erasure of all his personal data held by a controller when it is no longer needed.

Restriction

The data subject has the right to restrict the usage of his personal data when the accuracy is contested, the processing is unlawful, the controller no longer needs the data, or the legitimate interest of the controller is contested.

Portability

Data subject has the right to receive his personal data in machine readable format and to transmit it to another controller.

Right to Object

The data subject has the right to object to profiling or marketing processing at any time. In this case, the controller must stop processing his personal data.

Automated Individual Decision

Data subject has the right not to be subject to a decision solely based on automated processing, including profiling, which has a legal effect.

Exceptions:

- Data subject has given consent;
- It is permitted by law;
- It is necessary to enter or perform a contract.

Controller and Processor

Responsibility of the controller

The controller shall take appropriate technical and organisational measures to ensure compliance to this regulation, and shall be able to demonstrate it.

Data Protection by Design and by Default

Data protection by design and by default: the controller shall implement measures that are designed to implement data protection, and ensuring that, **by default**, only personal data which are necessary for each purpose of the processing are processed.

In case of joint controllers, respective responsibilities must be clearly defined.

Controllers Not Established in the EU

Controllers not established in the EU shall designate in writing a representative in the EU.

Responsibility of the Processor

The controller shall use only processors giving sufficient guarantees that processing will comply with this regulation.

The processor shall not engage another processor without the authorisation of the controller.

Processing by a processor shall be governed by a written contract (or other legal act). The contract shall specify that

- the controller processes the personal data only in documented instructions of the controller;
- the persons processing the personal data commit themselves to confidentiality;

- the processing ensures confidentiality, integrity, availability and resilience;
- the processor shall assist the controller in fulfilling the obligations related to the data subject rights;
- personal data are returned or deleted at the end of the contract.

Records of Processing Activities

Each controller shall maintain a record of processing activities.

The record shall contain:

- Contact details of the controller and, when applicable, the DPO;
- Purpose of the processing;
- Categories of data subjects and categories of personal data;
- Categories of recipients of personal data;
- Transfers of personal data to third countries or international organisations;
- Data retention period;
- General description of the technical and organisational security measures.

Each processor shall maintain a record of processing activities.

The record shall contain:

- Contact details of the processor and controller;
- Categories of processing performed on behalf of each controller;
- Transfers of personal data to third countries or international organisations;
- General description of the technical and organisational security measures.

Records shall be made available to regulatory authority upon request.

Exception: organisation employing less than 250 persons are exempt, except if the processing carries a risk to the rights and freedom of data subject, the processing is not occasional, or special categories of personal data are processed.

Cooperation with Supervisory Authority

Controllers and processors shall cooperate with the supervisory authority.

Security of Processing

The controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- Pseudonymisation and encryption;
- Confidentiality, integrity, availability and resilience of processing systems and services;
- Ability to restore access to personal data in a timely manner after an incident;
- A process for regularly testing and assessing the effectiveness of the measures.

Notification of a Data Breach

To the Supervisory Authority

In case of data breach, the controller shall notify the supervisory authority within 72 hours, unless the breach is unlikely to result in risk to the rights and freedom of natural persons.

The processor shall notify the controller without delay.

The notification shall mention:

- Nature of the breach, categories and number of affected data subjects;

- Name and contract details of the DPO;
- Consequences;
- Measures taken.

To the Data Subject

When the data breach is likely to result in high risk to the rights and freedom of the data subjects, the controller shall communicate the data breach to the data subjects.

Exceptions:

- The controller has implemented appropriate protection measures to render the data illegible;
- The controller has taken measures which ensure the risk will not materialise;
- It would involve disproportionate efforts. In this case, a public communication is acceptable.

Data Protection Impact Analysis

When the processing is likely to result in high risk to the rights and freedom, the controller shall perform a risk assessment.

A DPIA is required in case of:

- Systematic and extensive evaluation of personal aspects based on automated processing;
- Processing on a large scale of special categories of personal data, or data related to criminal convictions and offences;
- Systematic monitoring of publicly accessible area on a large scale.

Supervisory authority shall make a list of activities where a DPIA is mandatory.

The DPIA shall at least contain:

- Systematic description of the processing;
- Assessment of the necessity and proportionality of the processing in relation with the purpose;
- Assessment of the risks to right and freedom;
- Measures envisaged to reduce the risk.

Prior Consultation

The controller shall consult the supervisory authority before processing when a DPIA indicates a high risk in absence of measures.

The supervisory authority shall answer within 8 weeks, with a possible extension of 6 additional weeks.

Data Protection Officer

DPO

The controller and the processor shall designate a DPO when:

- The processing is performed by a public authority (except courts);
- The core activity of the controller or processor implies regular and systematic monitoring of data subjects on a large scale;
- The core activity of the controller or processor consists of processing special categories of data on a large scale.

The DPO may be an employee or an external person. It must be selected on basis of professional expertise of data protection law.

Position of the DPO

The DPO shall be involved in all issues related to the protection of personal data.

He shall have enough resources.

He shall receive no instructions regarding the exercise of his tasks and shall report to the highest level of management.

Tasks of the DPO

- Inform and advise controller or processor;
- Monitor compliance with the regulation;
- Provide advice regarding DPIA;
- Cooperate with supervisory authority;
- Act as contact point for the supervisory authority.

Codes of Conduct and Certifications

Codes of Conduct

Codes of conduct for categories of enterprises are encouraged.

Monitoring of Approved Code of Conduct

A supervising body may be accredited to monitor the compliance with the code of conduct. This is not applicable to public authorities.

Certification

Certification is encouraged, but it shall be voluntary, and shall not reduce the responsibility of enterprises.

Certification Bodies

Certification bodies shall be accredited by the supervisory authority or national accreditation bodies.

Transfer of Personal Data to Third Countries or International Organisations

General Principle

Transfers are only permitted if the following articles are applied.

Adequacy Decision

A transfer is authorised if the Commission has decided that the third country organisation ensures an adequate level of protection. Such transfers shall not require specific authorisations.

Transfers Subject to Appropriate Safeguards

In absence of adequacy decision, transfers are authorised if the controller or processor has provided appropriate safeguards, like:

- Legally binding instruments between authorities;
- Binding corporate rules;
- Standard clauses adopted by the Commission or a supervisory authority;
- An approved code of conduct;
- An approved certification.

Binding Corporate Rules

The supervisory authority will approve binding corporate rules if they guarantee the same level of protection and the same mechanisms for the data subjects as in the EU.

Transfers Not Authorised

Any judgment or decision of an administrative authority requiring transfer or disclosure of personal data may only be recognised if based on an international agreement.

Derogations

In absence of an adequacy decision or binding corporate rules, the transfer of personal data is only allowed if:

- The data subject has explicitly consented;
- The transfer is necessary for the conclusion or execution of a contract with the data subject;
- The transfer is necessary for important reason of public interest;
- The transfer is necessary for a legal claim;
- The transfer is necessary for the vital interest of the data subject or other persons;
- The transfer is made from a register which is intended to provide information to the public.

International Cooperation

The Commission and supervisory authorities shall take appropriate steps to develop cooperation mechanisms to facilitate the enforcement of this legislation.

Independent Supervisory Authorities

Each Member State shall provide at least one independent supervisory authority for monitoring the application of this regulation.

Cooperation and Consistency

These articles describe the cooperation of the lead supervisory authorities between them, and describes the role of the Board.

Remedies, Liability and Penalties

Right to Lodge a Complaint with a Supervisory Authority

Every data subject shall have the right to lodge a complaint with a supervisory authority, who shall inform the complainant on the progress and outcome of the complaint.

Right to an Effective Judicial Remedy against a Supervisory Authority

Every natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority.

In particular, this right shall be ensured when the supervisory authority does not inform the data subject within 3 months after the complaint is lodged.

Right to an Effective Judicial Remedy against a Controller or Processor

Every data subject shall have the right to an effective judicial remedy when he considers that his privacy rights have been infringed by a controller or processor.

Representation of Data Subjects

A data subject shall have the right to be represented by a non-profit organisation whose statutory objectives are the protection of privacy.

Suspension of Proceedings

Proceedings of a court may be suspended if the same affair is handled by the court of another Member State.

Right to Compensation and Liability

Any person who has suffered damage from an infringement of this regulation shall have the right to be compensated.

If more than one controller or processor is responsible for the damage, they will all be liable to the full compensation of the data subject. After full compensation, the paying party may claim back from the other ones the part of the compensation corresponding to their respective responsibilities.

General Conditions for Imposing Administrative Fines

Each supervisory authority shall ensure the imposition of administrative fines in case of infringement shall be effective, proportionate and dissuasive.

The fines can be up to 10 M€ or 2% of the total worldwide annual turnover, whichever is higher, or 20 M€ or 4% of the total worldwide annual turnover, whichever is higher, depending on the kind of infraction.

Penalties

Member States shall lay down rules for the penalties not subject to the administrative fines listed above.

Provisions Relating to Specific Processing Situations

Processing and Freedom of Expression and Information

Member States shall by law reconcile the protection of personal data with the right to freedom of expression and information, including processing for journalistic, academic, artistic or literary purposes.

Processing and Public Access to Official Documents

Personal data in official documents held by a public authority may be disclosed by the authority in accordance with the EU or Member State law.

Processing of the National Identification Number

Member States may further determine the specific conditions for the processing of the national identification number or any other general identifier.

Processing in the Context of Employment

Member States may provide specific rules to ensure the protection of the rights and freedom for the processing of employee's personal data by the employer.

Safeguards and Derogations for Processing for Archiving, Public Interest, Scientific or Historical Reasons

Processing for archiving, scientific, historical or statistical reasons shall be subject to appropriate security technical measures, data minimisation and pseudonymisation where possible.

Obligations of Secrecy

Member States may adopt specific rules for controllers or processors subject to professional secrecy.

Existing Data Protection Rules of Churches and Religious Associations

Churches or religious associations that apply comprehensive rules for the protection of natural persons may continue applying these rules if they are brought in line with this regulation. They will be under supervision of a supervisory authority, which may be specific.

Delegated Acts and Implementing Acts

Exercise of the Delegation

The Parliament and Council give delegation of power to the Commission from 24/5/2016. It may be revoked.

Committee Procedure

The Commission shall be assisted by a Committee.

Final Provisions

Repeal of Directive 95/46/EC

Directive 95/46/EC (Data Protection Directive) is repealed as of 25/5/2018.

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relationship with the public telecommunication networks.

Relationship with Previously Concluded Agreements

International agreements involving transfers of personal data to third countries concluded before 24/5/2016 and complying with this Regulation shall remain in force.

Commission Report

The Commission shall submit a report on the evaluation and review of this Regulation every 4 years, starting on 25/5/2020.

Review of Other Union Legal Acts on Data Protection

If appropriate, the Commission shall submit legislative proposals to amend other legal acts to ensure uniform and consistent protection of personal data.

Entry into Force and Application

This Regulation shall apply from 25/5/2018.