

IMPLEMENTATION OF THE NEW GENERAL DATA PROTECTION REGULATION



NNTT

¿What is the GDPR?

¿Why it is compulsory for the companies?

Penalties

The figure of the Data Protection Officer

Methodology

Conclusions

Which regulations?

- 1. 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 on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- 2. Draft Law on the Protection of Personal Data.**

What is the General Data Protection Regulation?

1. General Data Protection Regulation (GDPR)

- The European Data Protection Regulation unifies and modernizes the European regulation on data protection, allowing citizens to have better control of their personal data and companies to maximize the opportunities of a digital single market.
- "It will be mandatory in all its elements and directly applicable in each Member State."
- **It will come into force on May 25, 2018.**

What is the General Data Protection Regulation?

1. Draft Law on the Protection of Personal Data:

It was presented in June 2017 and is scheduled to be approved before March 2018.

It respects the General Data Protection Regulation at all times and it clarifies its content.

It will replace the current Organic Law on Data Protection.

What changes legally?

- The previous European Directive 95/46/EC is abrogated.
- The Organic Law 15/99 on Data Protection is abrogated.
- The Royal Decree 1720/2007 is abrogated..
- The General Regulation of Data Protection UE 2016/679 enters into force: **May 25, 2018.**
- It is not necessary to transpose (it will be the same in all the countries of the EU).

What changes conceptually?

OLPD

- Tacit Consent.
- 3 levels: basic, medium, high.
- Public Registration of Files.
- External Regulation.
- Security Measures established in the RD.
- 4 Rights: ARCO .

GDPR

- Express Consent
- 2 levels: special and not special.
- Internal Registration of Files
- Self-regulation
- Security Measures defines by the Company.
- 6 Rights:
ARCO + to be forgotten + portability

How consent is given?

OLPD

- Declaration of will
- Tacit, Contrary or negative, implicit
- Several consents in one
- Positive Silence

GDPR

- Declaration of express will (unequivocal)
- There is no room for tacit or presumed consents
- Each consent separately (Privacy by Design).
- Negative Silence (Privacy by Default)

Why it is compulsory for the Companies?

The article 24 GDPR and article 30 of the Draft Law

- **All the companies shall nominate a Data Protection Officer**, who, after weighing the risks that the treatment may generate in the rights of those affected and, in particular, in their right to protection, will be responsible for establishing the technical and organizations in order to guarantee and be able to demonstrate that data processing is in accordance with Community regulations.

Which requirements does the Data Protection Officer have to meet?

Art. 45 OLPD

- 1.- The minor infringements will be sanctioned by fines between 900 and 40.000 euros.
- 2.- The serious infringements will be sanctioned by fines between 40.001 and 300.000 euros.
- 3.- The very serious infringements will be sanctioned by fines between 300.001 and 600.000 euros

Art. 83 GDPR

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

What data appears with the new GDPR?

In **article 9.1 del GDPR** appears the figure of special categories of personal data that defines it by the following way:

*“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of **genetic data, biometric data** or the purpose of uniquely identifying a natural person, **data concerning health** or **data concerning a natural person’s sex life or sexual orientation** shall be prohibited”*

Which obligations appear according to that type of data?

For the category of **special data** the obligations that appear are the following:

- Conducting an **Privacy Impact Assessment (PIA)**.
- **Record** of Processing Activities.
- Nomination of **Data Protection Officer**.

What is the Privacy Impact Assessment?

Provided by the **article 35 del GDPR**, the responsables shall carry out an PIA before implementing those treatments that affect special data and that may entail a high risk for those interested. It must be done when:

1. Based on the data, profiles are generated based on decisions that produce legal effects.
2. When doing large-scale treatments of sensitive data.
3. When there is systematic observation on a large scale of a public access area.
4. Data protection authorities are obliged to draw up additional lists of treatments that will require an PIA.

What is the Record of Processing Activities?

Provided in **article 30 GDPR**:

- It replaces the previous registration of public files with the Spanish Agency for Data Protection.

- It is registeret internally in the company: :
“Principle of Accountability”

What does the Record of Processing Activities contains?

Shall contain:

- Name and contact data of the responsible company
- Name and contact data of the processor
- Name and data of the DPO
- Purposes for which the data is collected
- Category of concerned (connection between the owners and the company)
- Types of data (mentioning if those are special)
- Where applicable, international transfers
- Legal base (reason for which I have the data)
- If those are special data, give documentary evidence on the impact assessment for the owner.

Which Security Measures the company must carry out?

The security measures scheme that is provided on the RD 1720/2007 **is NOT going to be applicable automatically.**

- The measures are decided based on the results of the risk assessment.
- They must be applied BEFORE beginning the treatment.
- Based on continuous improvement.
- The technical and organizational measures should be established taking into account:
 1. The costs and the state of the art
 2. The application costs
 3. The nature, scope, context and purposes of the treatment.
 4. The risks for the rights and freedoms of those affected..
- It is configured as a Privacy Management System based on self-learning and improvement, which requires self-analysis of the system (audits).

What is the Data Protection Officer?

It is provided in the **article 37 del GDPR**:

“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;*
- 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 pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10”.*

Which functions does the Data Protection Officer have?

- a) Inform and advise the controller or the processor and the employees who deal with the processing of personal data about their obligations under the Regulation and other data protection provisions of the European Union or of the Member States;

- b) Supervise the compliance of what is provided on the Regulation, on other data protection provisions of the European Union or of the Member States and the policies of the data controller or processor, including the assignment of responsibilities, the awareness and training of personnel involved in processing operations, and the corresponding audits;

Which functions does the Data Protection Officer have?

- c) Offer the advice that is requested about the privacy impact assessment relative to the data protection and supervise its fulfillment;
- d) Cooperate with the supervisory authority;
- e) Act as the contact point of the supervisory authority for matters related to the processing of personal data including prior consultation, and consult, when applicable, on any other matter.

Which requirements does the Data Protection Officer have to meet?

- a) Broad experience and knowledge of the subject and of the interpretation and practical adaptation to apply the data protection regulation, including the security measures in all the technical and administrative processes and development of the company.
- b) Specific knowledge of the subject applied to the different sectors.
- c) Experience and ability to attend the company before inspections, requirements of the competent authorities and any type of consultation of third parties affected by the data processing of the company name.
- d) Negotiation, training and empathy skills to work with workers' representatives, and of course with the company's own workers.

Metodology

1- Nomination of the RPD o del DPO.

- The company shall nominate a Data Protection Responsible (DPR) or a Data Protection Officer (DPO) as stated on the article 37 GDPR.

2- Risk Assessment

- The DPR or the DPO shall carry out a risk assessment and where appropriate (data particullary protected) realizará una evaluación de riesgos y en su caso (datos especialmente protegidos) an impact assesstment on the risks that may affect the company.

Metodology

3- Record of Activity

- The DPR or the DPO creates a registry of internal files, together with the necessary security measures for protect the company from the detected risks.

4- Security Measures

- Once the above procedures have been carried out, everything is collected in a single Document, which should govern the behaviour of the memebers of the organization in matters of Data Protection.

Examples of risks

Illegal access to confidential information

Physical theft of digital or paper information

Sending confidential information to third parties without authorization

Insufficient design of security measures

Insufficient Chain of Custody

Accidental leak of information

Interception of documentation

Interception, accidental or not, of conversations

Do not close a computer application after use

Disclosure of personal data of customers, workers, suppliers ...

Conclusions

All companies must comply with the community standard

Any company must develop and comply with policies adopted on data protection

The offered service must be adapted to the needs required by the Law

Sensitive processes must be analyzed and create organizational programs adapted to each situation

The phases for the implementation of data protection policies are based on a methodology and the participation of the company

The sanctions that can be imposed in case of non-compliance can reach up to 4% of the company's turnover