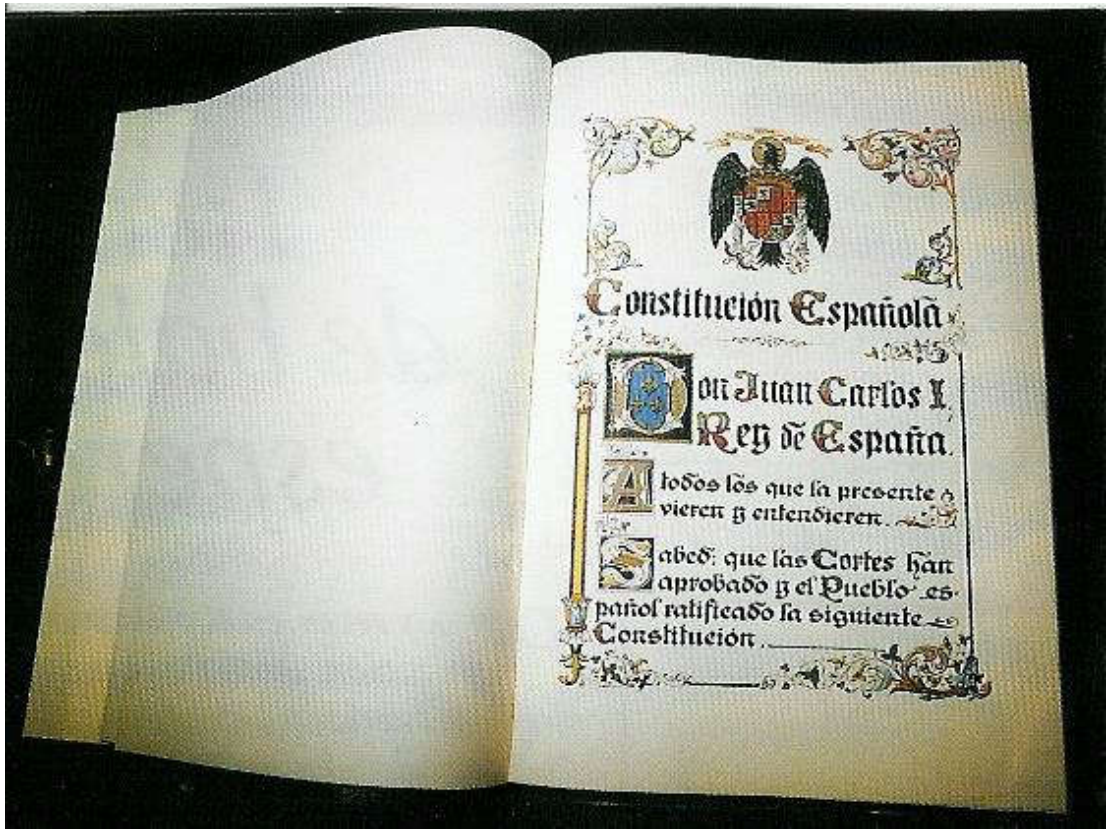
Chapter 5. Personal Data Protection

Marta Fernández Diego

Foundation Stone…

- **The Spanish Constitution, 1978**
  - *Fundamental Rights and Public Liberties*



The Spanish Constitution

- ***Article 18***
  - 1. The right to honour, to personal and family privacy and to protect one's own image is guaranteed.
  - 2. The home is inviolable.
  - 3. Secrecy of communications is guaranteed.
  - 4. The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.

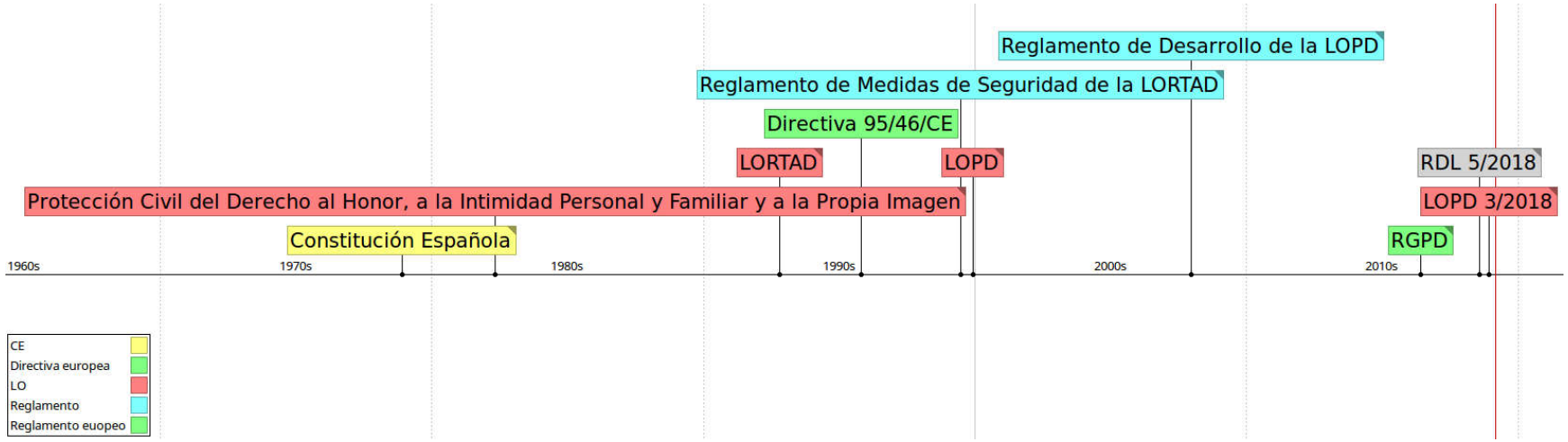
Index

- History of Data Protection in Spain
- General Regulation of Data Protection (GRDP)
  - Objectives
  - Material scope and territorial scope
  - Definitions
  - Key principles
  - Individual rights
  - International data transfers
  - Active responsibility
- LOPDGDD
  - Objectives
  - Digital rights

Background

- Organic Law 1/1982 of 5 May on the civil protection of the right to honour, to personal and family privacy and to protection of one's own image
- Organic Law 5/1992 of 29 October regulating the automatic processing of personal data (LORTAD)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Organic Law 15/1999 of 13 December on the Protection of Personal Data (LOPD)

Timeline


Reglamento de Desarrollo de la LOPD
Reglamento de Medidas de Seguridad de la LORTAD
Directiva 95/46/CE
LORTAD
LOPD
RDL 5/2018
Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen
LOPD 3/2018
Constitución Española
RGPD
1960s
1970s
1980s
1990s
2000s
2010s
CE
Directiva europea
LO
Reglamento
Reglamento euopeo

General Regulation of Data Protection

- Entered into force on **25 may 2016**
- But was not applied until two years later, the **25 may 2018**
- Repeals Directive 95/46/EC
- Leads to increased harmonisation of data protection law across the EU Member States

GRDP

- The period of two years until the implementation of the GRDP aimed to enable the adaptation of states of the European Union, the European institutions and also organizations.
- The new Spanish Organic Law on Data Protection an Digital Rights Guarantee (LOPDGDD) complements the GDPD.

LEGISLACIÓN CONSOLIDADA

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Jefatura del Estado
«BOE» núm. 294, de 6 de diciembre de 2018
Referencia: BOE-A-2018-16673

Objectives

- This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
- The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Material scope

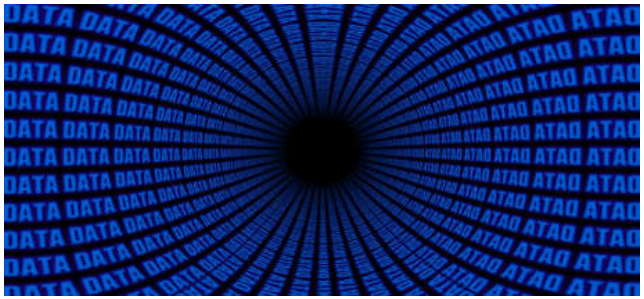
- Does not apply:
  - in the course of an activity which falls outside the scope of Union law;
  - by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
  - by a natural person in the course of a purely personal or household activity;
  - by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal
  - offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

Territorial scope

- The GDPR applies to business
  - That are established in any EU Member State and that process PD (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of this establishment.
  - Outside the EU if they process the PD of data subjects who are in the EU in relation to:
    - The offering of goods or services to data subjects who are in the EU
    - The monitoring of the behaviour of data subjects who are in the EU

Definitions

- Personal Data
- Processing
- Controller
- Processor
- Data Subject
- Sensitive Personal Data
- Data Breach
- Pseudonymisation



Personal Data (Definition)

- Any information relating to an identified or identifiable natural person
- Identifiable natural person
  - One who can be identified directly or indirectly, in particular by reference to
    - An identifier
      - A name, an identification number, location data, an online identifier
    - One or more factors specific of that natural person
      - The physical, physiological, genetic, mental, economic, cultural or social identity

Processing (Definition)

- Any operation or set of operations which is performed on personal data
  - Whether or not by automated means
  - 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

Controller (Definition)

- Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Processor (Definition)

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

Data Subject (Definition)

- Individual who is the subject of the relevant personal data

Sensitive Personal Data (Definition)

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership
- Data concerning health or sex life and sexual orientation
- Genetic or biometric data

Data Breach (Definition)

- Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Pseudonymisation (Definition)

- 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

Key Principles

- Transparency
- Lawful basis for processing
- Purpose limitation
- Data minimisation
- Accuracy
- Retention
- Data security
- Accountability

Transparency (Principle)

- PD must be processed lawfully, fairly and in a transparent manner.
- Controllers must provide minimum information to data subjects regarding the collection and further processing of their personal data.
- Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Lawful basis for processing (Principle)

- Prior, freely given, specific, informed and unambiguous consent
- Contractual necessity
- Compliance with legal obligations
- Legitimate interests

Types of consent

- **Express consent**
  - **Explicit** agreement, generally documented in writing
  - **The default option**, in the absence of express consent
- **Implied consent**
  - **Presumed** consent
    - **Implicit** consent
  - **Tacit** consent
    - Consent that is expressed silently or passively by omissions or by failures to indicate or signify dissent

Consent

- Has the way in which we must obtain the consent changed?
  - Prior, free, specific, informed and unambiguous
  - Unambiguous: The Regulation requires a statement or a positive action indicating the agreement of the person concerned.
  - Consent cannot be deducted from the silence or inaction of citizens.

Consent

- What age may **children** give their **consent** for the processing of their PD?
  - The age at which minors may provide for themselves their consent for the processing of their PD in the area of the information society (for example, social networks) is **16 years**.
  - Establishing a lower limit of **13 years**
  - In the case of Spain, **14 years**

Lawful basis for processing (Principle)

- Sensitive personal data
  - Explicit consent
  - The processing is necessary
    - In the context of employment law
    - For the establishment, exercise or defence of legal claims

Purpose limitation (Principle)

- PD may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

Data minimisation (Principle)

- PD must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.
- A business should only process the PD that it actually needs to process in order to achieve its processing purposes.

Accuracy (Principle)

- PD must be adequate must be accurate and, where necessary, kept up to date.
- A business must take every reasonable step to ensure that PD that are inaccurate are either erased or rectified without delay.

Retention (Principle)

- PD must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the PD are processed.

Data security (Principle)

- PD must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability (Principle)

- The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Individual Rights

- Right of access to data / copies of data
- Right to rectification of errors
- Right to deletion / right to be forgotten
- Right to object to processing
- Right to restrict processing
- Right to data portability
- Right to withdraw consent
- Right to object to marketing
- Right to complain to the relevant data protection authorities
- Right to basic information

Right of access to data / copies of data

- A data subject has the right to obtain from the controller the following information:
  - Confirmation of whether, and where, the controller is processing the data
  - Information about
    - The purposes of processing
    - The categories of data being processed
    - The categories of recipients with whom the data may be shared
    - The period for which the data will be stored (or the criteria used to determine that period)

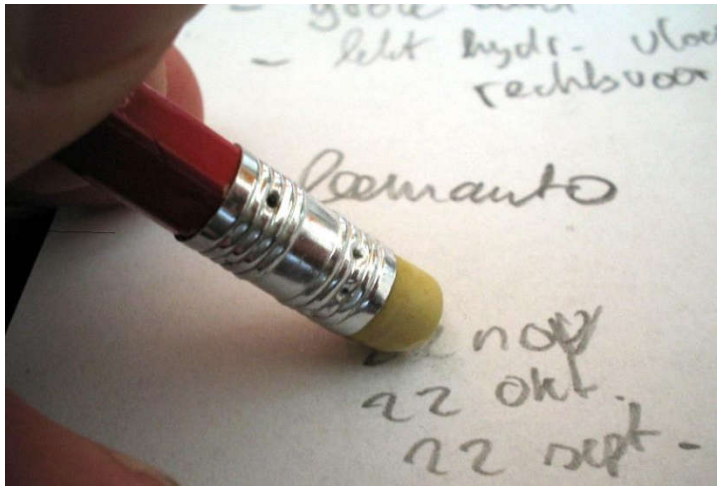
Right of access to data / copies of data

- The existence of the rights
  - To erasure, to rectification, to restriction of processing and to object to processing
  - To complain to the relevant data protection authority
- The source of the data, where the data were not collected from the data subject
- The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject

- The data subject may request a copy of the PD being processed.

Right to rectification of errors

- Controllers must ensure that inaccurate or incomplete data are erased or rectified.
- Data subjects have the right to rectification of inaccurate PD.

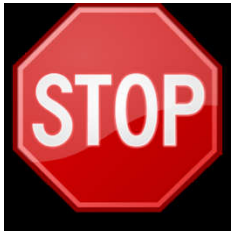


Right to deletion / right to be forgotten

- The data are no longer needed for their original purpose.
- The lawful basis for the processing is the data subject´s consent, the data subject withdraws that consent, and no other lawful ground exists.
- The data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing.
- The data have been processed unlawfully.
- Erasure is necessary for compliance with legislation.

Right to object to processing

- Data subjects have the right to object, on grounds relating to their particular situation, to the processing of PD where the basis for that processing is either public interest or legitimate interest of the controller.
- The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.



Right to restrict processing

- The data may only be held by the controller, and may only be used for limited purposes if:
  - The accuracy of the data is contested (and only as long as it takes to verify that accuracy)
  - The processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure)
  - The controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights
  - Verification of overriding grounds is pending, in the context of an erasure request

Right to data portability

- Data subjects have a right to receive a copy of their PD in a commonly used machine-readable format, and transfer their PD from one controller to another or have the data transmitted directly between controllers.

Right to withdraw consent

- A data subjects has the right to withdraw their consent at any time.
- The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.
- Prior to giving consent, the data subject must be informed or the right to withdraw consent.
- It must be as easy to withdraw consent as to give it.

Right to object to marketing

- Data subjects have the right to object to the processing of PD for the purpose or direct marketing, including profiling.

Right to complain to the relevant data protection authorities

- Data subjects have the right to lodge complaints concerning the processing of their PD with the competent data protection authority in Spain, if the data subjects live in Spain or the alleged infringement occurred in Spain.

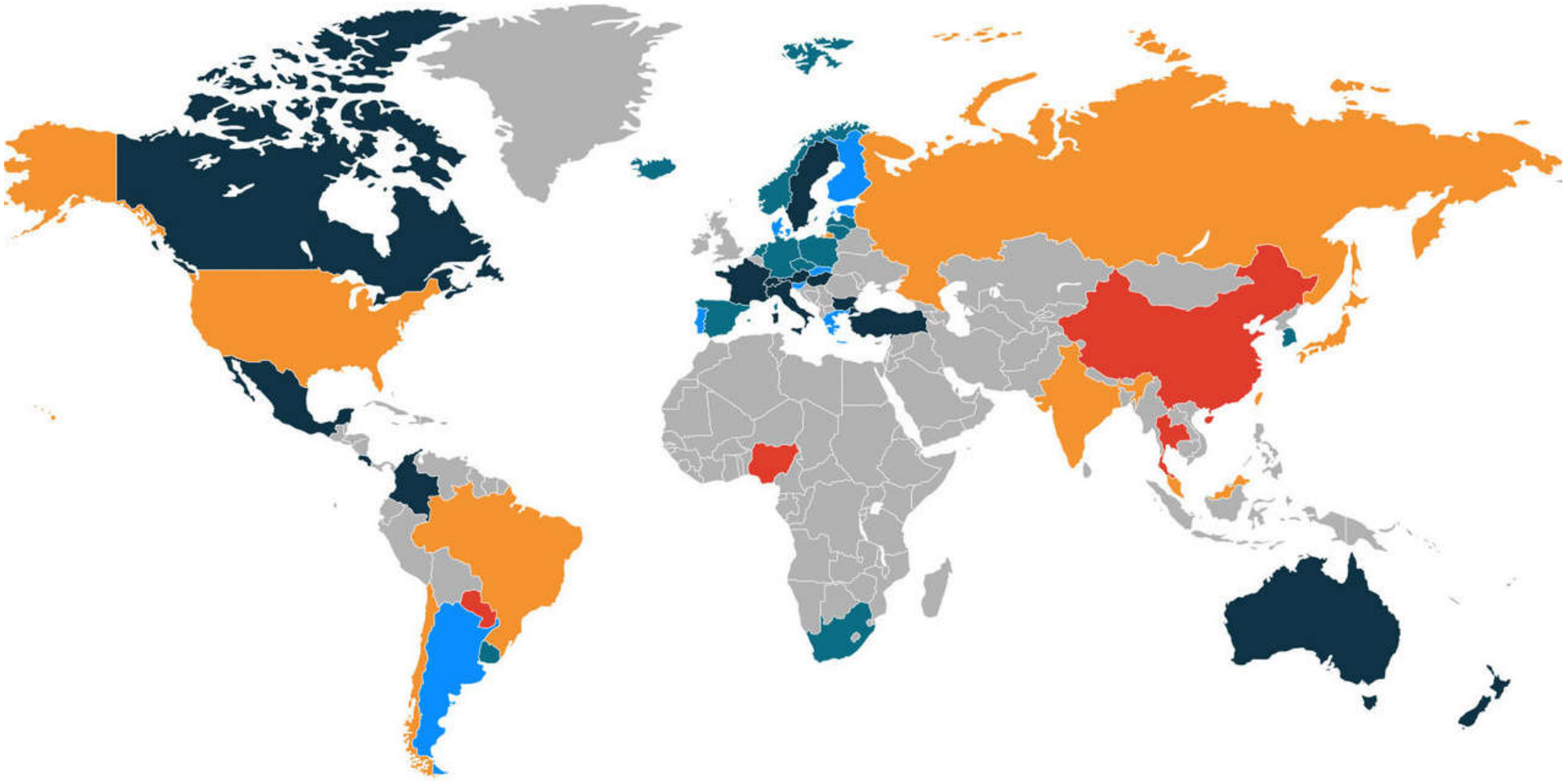
Right to basic information

- Data subjects have the right to be provided with information on:
  - The identity of the controller
  - The reasons for processing their PD
  - Other relevant information necessary to ensure the fair and transparent processing of PD

International Data Transfers

- Outside the European Economic Area
  - If the transfer is to an “Adequate Jurisdiction” or the business has implemented one of the required safeguards as specified by the GDPR
    - Consent of the relevant data subject
    - Standard Contractual Clauses or Binding Corporate Rules
    - EU-US Privacy Shield Framework
- Most of the safeguards outlined in the GDPR will need initial approval from the data protection authority.

Privacy and data protection by country



Most restricted
Restricted
Some restrictions
Minimal restrictions
Effectively no restrictions
No information

Source: Forrester

Active responsibility

- Companies must take reasonable **measures** to ensure that they are in a position to comply with the principles, rights and guarantees that the Regulation states:
  - Data protection by **design**
  - Data protection by **default**
  - **Security measures**
  - Maintenance of a processing of data **register**
  - **Impact assessments** on data protection
  - Appointment of a data protection **delegate**
  - Notifying **violations** of data security
  - Promoting **codes of conduct** and **certification schemes**

Responsibility of the controller

- Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.
- Those measures shall be reviewed and updated where necessary.

Data Protection Officer (DPO)

- The appointment is mandatory in some circumstances
  - Large-scale regular and systematic monitoring of individuals
  - Large-scale processing of sensitive personal data
- The appointment must be notified by the controller or processor

Data Protection Officer (DPO)

- Minimum tasks
  - Informing the controller, processor and their relevant employees who process data of their obligations
  - Monitoring compliance with legislation and internal policies including internal audits
  - Advising on data protection impact assessments and the training of staff
  - Cooperating with the data protection authority and acting as the authority´s primary contact point

One-stop shop

- What is the system of **one-stop shop**?
  - Designed to ensure a single data protection authority as a interlocutor
  - Does not affect companies that are only in a member state and make data processing affecting only data subjects in that state

LOPDGDD

- The new Spanish Organic Law on Data Protection an Digital Rights Guarantee (LOPDGDD) complements the GDPD.

LEGISLACIÓN CONSOLIDADA

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Jefatura del Estado
«BOE» núm. 294, de 6 de diciembre de 2018
Referencia: BOE-A-2018-16673

LOPDGDD

- Although they have the characteristic of being directly applicable, regulations may in practice require other complementary internal rules in order to make their application fully effective.
- In this sense, rather than transposition, we can speak of “development” or complement to European Union law.

Objectives

- a) Adapt the Spanish legal system to Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of their personal data and on the free movement of such data, and complete its provisions.
- The fundamental right of natural persons to the protection of personal data, under Article 18.4 of the Constitution, shall be exercised in accordance with the provisions of GRDP and in this organic law.
- b) Guarantee the digital rights of citizens in accordance with the established mandate in Article 18.4 of the Constitution.

Digital rights

- One of the biggest changes that the LOPDGDD introduces is new citizen rights for the internet age.
- Although many of them only constitute a reinforcement from the digital point of view to the rights regime already established in the GDPR, others are completely original.

List of digital rights

- The right to universal access to the internet
- The right to digital education
- The right to privacy and use of digital devices in the workplace
- The right to digital disconnection in the workplace
- The right to privacy in front of video surveillance and sound recording at work
- The right to digital will

Personal data of deceased persons

- Does your digital identity die when you die?
- The GPDR does not apply to the personal data of deceased persons.
  - Member States may provide for rules regarding the processing of personal data of deceased persons.
- LOPD recognizes individuals have the right to digital testament.
  - Moreover, the heirs of the deceased are entitled to exercise the rights to access, erasure and rectification of data unless the deceased person would have prohibited it or this is not in line with applicable law.

DPO

- The LOPDGDD includes a list of entities that must appoint a DPO as mandatory for their activity:
  - Professional associations
  - Education centres, public and private universities
  - Entities that operate networks and provide electronic communications services
  - Providers of information society services when they develop large-scale profiles
  - Insurers
  - Credit finance institutions
  - Investment service companies
  - Health centres
  - Private security companies

Competent authorities

- Main data protection authority
  - Agencia Española de Protección de Datos (AEPD)
- Regional data protection authorities
  - Cataluña and País Vasco
  - With powers essentially over public entities within their respective territory

Data Protection Agency (AEPD)

- Body under public law, with its own legal personality and unlimited public and private legal capacity, **which acts fully independently of the public administrations** in the performance of its tasks
- Main function:
  - **To ensure compliance with the legislation on data protection** and ensure its application, in particular as regards the rights of information, access, rectification, objection and cancellation of data
- The General Data Protection Register
  - Data relating to files which are necessary to exercise rights of information, access, rectification, cancellation and objection

Security measures

- **Royal Decree 994/1999**, of 11 June, approved the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data.
  - There were three levels of applicable security measures for files and processing: basic, medium and high.
  - It was repealed by Royal Decree 1720/2007.
- **Royal Decree 1720/2007**, of 21 December, approved the Regulation implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data.
  - It covered the area previously protected by Royal Decree 994/1999.

Some questions

- Data Protection Day
  - Why 28 January?

References

- https://iclg.com/practice-areas/data-protection-laws-and-regulations/spain#chaptercontent
- https://www.out-law.com/en/articles/2018/november/spain-new-data-protection-digital-rights-law/