GENERAL DATA PROTECTION REGULATION (GDPR)

Andrés Calvo Medina
Spanish Data Protection Authority

Implementation and harmonization

- Comes into force 25 May 2018
- GDPR is a harmonization effort of regulations
  - **Direct application**, no need of transposition into national law, unlike Directive 95/46/CE
  - There will be additional regulations

Area of application

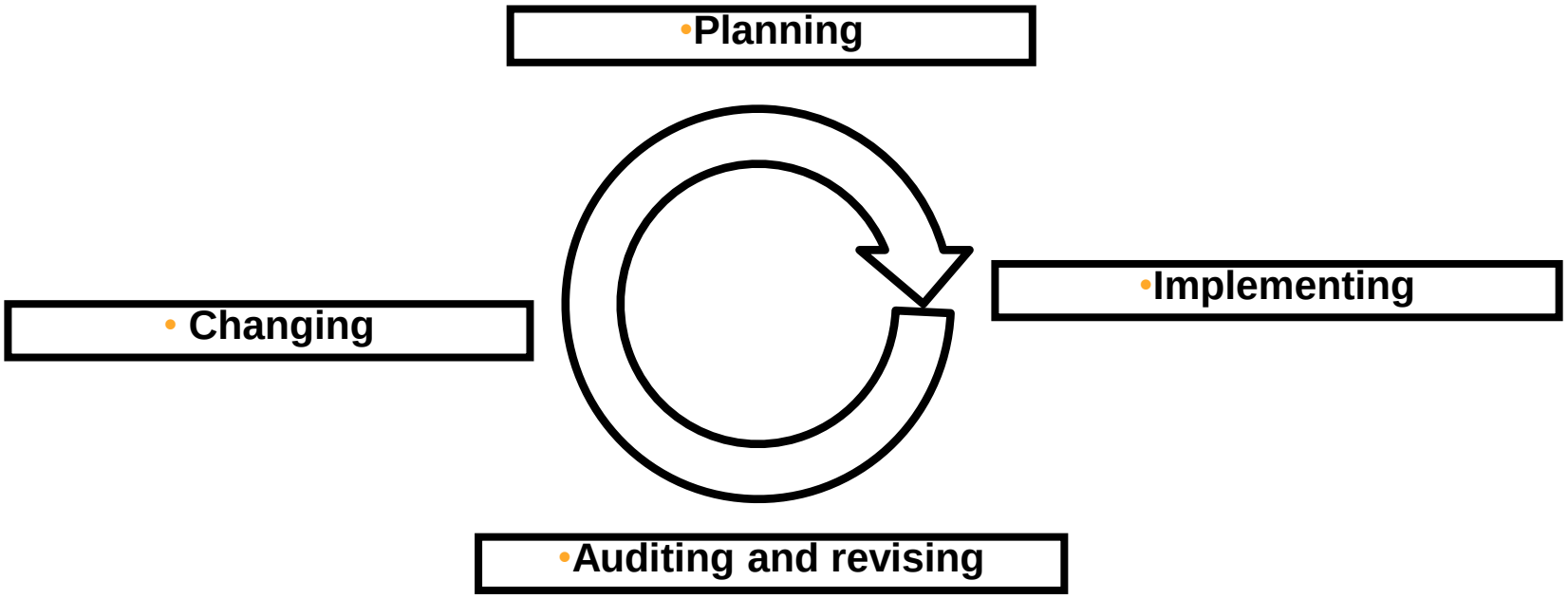
- Applies to data controllers & processors regardless of their location, whenever they process personal data of an EU resident data subject for:
  - The offer of goods and/or services (whether money changes hands or not)
  - Tracking of resident´s behavior(s)
- The controller/processor is deemed to be resident in the location where data control takes place (this is not always where the data is)

Accountability

- Data controllers and data processors will implement the appropriate technical and organizational measures:
  - to guarantee
  - to prove
- That processing of personal data is performed according to the GDPR
- That measures taken for personal data processing are constantly updated and supervised

Accountability

– **Personal data processing security is not a state but a continual process**:



Accountability

Obligations of controllers:

- The controller or processor must maintain records of all processing activities

"registry of personal data processing"

- Privacy/Data protection by design
- Privacy/Data protection by default
- Privacy impact assessments (PIA´s)

Accountability

Obligations of controllers:

- **Prior consultations** to the data protection authority
- **Appointment of a data protection officer (DPO)**
- **Duty to notify or communicate security breaches** to the data protection authority
- **Codes of conduct**
- **Certification**

Security measures

- Controller and processor shall implement appropriate **technical and organisational measures** to ensure a level of security appropriate to the risk:
  - State of technology
  - Implementation costs
  - Nature, scope, context and purposes of the processing
  - Risks to the rights and freedoms of data subjects

Security measures

- **Risks will particularly be taken into account when data processing, in particular as a result of:**
  - **The destruction of personal data, loss of data & unauthorized data modification**
  - **Unauthorized access to the data**
  - **Unauthorized sharing of data**

Security measures

- The registry of personal data processing must include:
  - When possible; the description of the security measures
- The adherence to a code of conduct or to a certification mechanism may be used:
  - To demonstrate compliance with security requirements of the GDPR security measures

Relationship controller-processor

- A must for data controllers to properly select competent data processors
- Relationship controller-processor under detailed contractual terms:
  - Detailed instructions of data controller about the data processing, and the restriction to carry out any other data processing
  - Confidentiality, duty of secrecy
  - Measures according to GDPR article 32: pseudonymisation, encryption, anonymization, resilience of processing, permanent re-evaluation of risks, …

Relationship controller-processor

- The data **sub-processors** must be authorized by data controllers
- Data controller may **refuse access to a sub-processor** to process personal data
- Data processor has the obligation to assist data controller in **data subjects rights**

Relationship controller-processor

Other details:

- Data controller may **audit** data processor, and data processor must cooperate with data controller
- The end of the contract involves the **return** of the personal data processed or the **destruction** of data
- If data processor **violates** the instructions of data controller, then he becomes data controller and will be sanctioned (no consent)
- Personal data authorities will provide **models of contracts** to be used in order to guarantee lawful personal data processing

International data transfers

- Only possible to transfer data to countries with **adequate level of protection** according to Commission decisions
- More instruments to guarantee international data transfers:
  - Data controller and data processors can **both** perform international data transfers
  - legally binding and enforceable contracts **between authorities or public bodies**

International data transfers

- More mechanisms to strengthen guarantees in personal data transfers:
  - **BCR** (Binding Corporate Rules) between data controller and data processors
  - **Standard contractual clauses** approved by the Commission
  - **Standard contractual clauses** approved by a **national DPA** and accepted by the Commission

International data transfers

- Codes of conduct
- Certification schemes
- Legitimate interest of data controller

Supervisory model

- Strengthening and harmonization of DPAs
- Mechanisms of coordination and consistency
- European Personal Data Protection Board (now WP29)
- Single European data protection office (one stop shop)
- Sanctioning system

Data subject´s rights

- **Principle of transparency:**
  - **Consent must be given with clear, concise, intelligible and transparent information, using clear and simple language**
  - **Special attention for minors consent**
- **Right to be forgotten (internet) / Cancellation**
- **Right of personal data portability**
- **Right to compensation**

Sanctioning system

- Sanctions must be effective, proportionate and dissuasive
- Graduation of the sanctions must be specific to each case
- Sanctions apply to data controller and data processors
- Mechanism of coherence: same infringement and same sanction in every country
- Criminal penalties (i.e. to seize the profits of the infringement)

Sanctions

- Types of infringements (administrative fines) and sanctions/warnings:
  - Up to 10 M € or up to 2% of the total annual global turnover in the preceding financial year whichever is higher :
    - Obligations of the controller and the processor
    - Obligations of the certification body
    - Obligations of the monitoring body of code of conduct
  - Up to 20 M € or up to 4 % of the total annual global turnover in the preceding financial year whichever is higher:
    - Basic data protection principles
    - Data subjects rights
    - International data transfers
  - Up to 20 M € or up to 4 % of the total annual global turnover in the preceding financial year whichever is higher
    - Non-compliance with an order by the supervisory authority