The new GDPR. Implications in the pharmaceutical industry

Lisbon, 17 May 2017

Agustín Puente Escobar
State Counsel – Head of the Legal Cabinet
Agencia Española de Protección de Datos

New regime. Key topics

Personal data:

- **Singling-out information/ pseudonymisation/ anonymization**

Definition of sensitive data and reference to genetic data

Minimization principle

- **Implications in e-health and processing on the basis of big data storage**

Legitimacy for processing sensitive data

- **Consent (possible domestic restrictions)**
- **Legal basis.**
  - **Particularly compatible purposes and use of data for scientific research purposes**

Information and data subject rights

- **Increasing data subjects control**

New compliance model based on the accountability principle

Compliance model

From the check list approach to the accountability approach

The risk based approach as the basis of the system

- **Processing of health data as a high risk processing**
- **Large scale monitoring of individuals as high risk**
- **Profiling as part of an appropriate treatment**

Compliance model

The adoption of proactive measures as a result of the evaluation

- **Utmost importance of the DPIA**
  - **Consultation to the main stakeholders (specially patient associations)**
  - **Map of risks and countervailing safeguards**
  - **Participation in self regulation schemes at national or supranational level**
  - **Collaboration with and, where appropriate, consultation and authorization of the DPA**
- **Data protection by design and by default**
  - **Delimitation of a minimum set of data necessary for the purpose**
  - **Adoption of anonymization or pseudonymisation techniques**

Compliance model

Relevant technical and organisational measures

- Establishment of clear and transparent procedures for collecting the data subject explicit consent
  - Complete information. ¿layered or standard format?
  - Clear consent clauses connected to those required by other legal provisions
  - Reasonable interpretation of the legal basis for processing when admitted (article 9.1 i) and j))

Compliance model

Relevant technical and organisational measures

- **Establishment of joint controllership systems**
  - **Clear determination of each stakeholder's role**
  - **Delimitation of each stakeholder's duties regarding compliance with the GDPR**
- **Establishment of clear pseudonymisation procedures when anonymization is not possible due to the nature of the processing**
  - **Access restrictions to non pseudonymised data**

Compliance model

Relevant technical and organisational measures

- **Establishment of secure environments for data processing**
  - **Access control and limitation related to the position of each stakeholder or system user**
  - **Pseudonymisation or anonymization whenever as possible**
  - **Information encryption**
  - **Strict rules regarding the use and dissemination of media**

Privacy-Oriented Organization

- **Essential role of the DPO for assuring compliance**
- **DPO's Constant advise**
- **Internal compliance and security audit**
- **Constant dialogue with DPAs**

The role of self regulation schemes

Delimitation of clear and up-to-date standards in order to facilitate:

- **Continuous assessment of the processing activities**
- **The adaptation of the technical processing techniques to the standards**

Useful tool in order to:

- **Clarify the limits of processing operations according to the different purposes**
- **Set homogeneous security standards**
- **Establish common standards in order to guarantee the principles and fulfil the obligations provided by the GDPR**
- **Specify the role of the different stakeholders**
- **Provide an adequate legal basis for international data flows**

The role of self regulation schemes

Implementation of out-of-court dispute resolution mechanisms

- **Safeguarding a quick and easy protection of the fundamental right**
- **Facilitating near-real-time compliance and resolution of gaps**
- **Providing a friendly and non sanctioning solution**

Some experiences: the "Standard code on personal data protection in clinical research and pharmacovigilance"

Clear data protection rules in the framework of medical trials

Specifies the roles of the different participants

- The sponsor and the medical institution as joint controllers
- The investigator as (commonly) user
- The monitor and the auditor as sponsor's processors

Provides a protocol governing the relationship between the sponsor and the medical institution

- Establishing different obligations in case of pseudonymisation
- Limiting the sponsor's legal obligations providing specific safeguards are adopted to avoid re-identification
- Fulfilment is basically in charge of the centre and the investigator
  - Proving information to the patient and collecting his or her consent
  - Attending the data protection rights
  - Fulfilling data retention rules linked to medical records retention
- Adoption of technical and organisational undertakings in order to avoid access to non pseudonymised data

Thanks for your attention!

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS