The General Data Protection Regulation and use of health data: challenges for pharmaceutical regulation

ENCePP Plenary Meeting- *London, 22/11/2016*

Alessandro Spina
Data Protection Officer, EMA

Disclaimer

- The views represented in this presentation are the personal opinion of the author and do not necessarily reflect the position of the European Medicines Agency or any other EU institution.

Introduction

- **Reform of data protection legislation (GDPR)**
- **Consent**
- **Other legal grounds for processing health data**
- **Pseudonymisation/Anonymisation**
- **Data Protection Governance**

1/ Reform of EU data protection legislation

Milestones of the data protection reform:

- *25 January 2012* Commission proposed reform of data protection legislation: repeal of Directive 95/46/EC; a **General Data Protection Regulation (GDPR)** and a Directive for the police and criminal justice sectors;

- *12 March 2014* European Parliament voted in support of the amended proposal for the GDPR;

- *15 June 2015* Council agreed a on a general approach on the GDPR;

- *15 December 2015* "Trialogue" agreement on the final text of the GDPR – followed by vote in the LIBE Committee (17 Dec) and COREPER (18 Dec)

- **Regulation (EU) 679/2016** adopted 24 May 2016- entry into force **25 May 2018**

1/ Reform of data protection legislation

Facts:

A "thick" legislative instrument; ~ 170 recitals; ~ 100 articles; 200 pages.

Structure:

- General provisions,

- Rights of Data Subjects

- Obligations of Controllers and Processors

- Regulatory governance aspects (EDPB/ Co-operation and Consistency)

- Specific data processing situations

1/ Reform of data protection legislation-

General principles of EU data protection law remain the same

but

- **Territorial scope** : Article 3(2) (b)"*This Regulation applies to the processing of personal data …. by a controller or processor not established in the Union…";*

- **Right to erasure ("to be forgotten")** (Article 17) including withdrawal of consent;

- **Right to Data Portability** (Article 18) "..in a structured and commonly used and machine-readable format…"

- Definition of **health data "**personal data related to physical or mental health […] which reveal information about his or health status"

1/ Reform of data protection legislation

- **<u>Profiling</u>** (Article 20); "which produces legal effects concerning him or her or significantly affects him or her..."

- **<u>Data Protection Impact Assessment</u>** (Article 33); DP by design and by default;

- **<u>DPO</u>** (Articles 35-37)

- **<u>Notification of Personal Data Security breaches</u>** (Articles 31-33)

- **<u>Sanctions</u>** (up to 4% company annual global turnover) and new legal remedies (class actions);

- **<u>EDPB</u>** which can adopt binding decisions, ensures consistency among DPAs.

2/Consent

- Consent remains cornerstone of DP law as main legal basis for the processing of personal data.

There are important clarifications on the **characteristics of valid consent**, either in general (Article 7)

Recital 42: "*For consent to be informed, the data subject should be aware at least of the identity of the Controller and the purposes for which the personal data are intended*";

- It requires an affirmative action, silence or inactivity should not constitute consent.

Or with regard to the processing of personal data **concerning health Article 9** : "the data subject has given **explicit** consent to the processing of those personal data…"

2/Consent

With regard to "consent" in the field of clinical trials/scientific research/patient registries, the final text contains other important indications:

Recital 161 "*For the purpose of consenting to the participation in scientific research activities in* **clinical trials** *the* **relevant provisions of Regulation (EU) No 526/2014 should apply** ".

• Interpretative issues between provisions of CT reg and GDPR on consent

Recital 33 " *It is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection. Therefore data subjects should be allowed to give their consent to certain* **areas of scientific research** *when in keeping with* **recognised ethical standards for scientific research**".

3/Other legal grounds for processing health data

There are legal grounds other than consent for processing health data:

Article 9 (2) (i): "processing is necessary for **reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of **quality and safety** of health care and of **medicinal products or medical devices**, on the basis of Union law or Member States law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subjects, such as professional secrecy".

•Highly relevant in the case of pandemic crisis or with regard to the obligations related to pharmacovigilance.

•Not clear whether only public bodies could rely on this provision.

3/Other legal grounds for processing health data

Article 83 Processing of personal data for...**scientific and historical research purposes shall be subject to appropriate specific safeguards** provided by Union or Member States law and where possible to pseudonymisation/anonymisation.

Recital 157 on patient registries: "*"By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. […] In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.*"

3/Other legal grounds for processing health data

Other provisions of the GDPR give a special protection to the use of health data in the context of public health activities:

Article 17 (3) (c) Limitation of the "right to erasure" in case of withdrawal of consent for reasons of public interest in the area of public health

Article 9 (4) "*Member States may maintain or introduce further conditions, including limitations with regard to the processing of **genetic data, biometric data or health data***"

11

4/Pseudonymisation/Anonymisation

There is a definition of **pseudonymisation** – cfr. Article 4 (5) e.g. key-coding data from electronic health records.

"*means the processing of personal data in such a manner that the pesonal data can no longer be attributed to a specific data subject without the use of additional information*"

Recital 26 Data which "*has undergone pseudonymisation*", but still could be attributed to a natural person by the use of additional info **should be considered personal data.**

It is a security measure not a way to anonymise data, in line with Article 29 WP Opinion 5/2014 on anonymisation techniques.

4/Pseudonymisation/Anonymisation

There remains the challenge of the anonymization of datasets in particular for clinical trials: "***No personal data of trial participants shall be recorded in the EU database***" (Recital 67 of Regulation (EU) 536/2014).

EMA published an *External Guidance on anonymisation of clinical reports for the purpose of Policy 70-* non-binding guidance presenting a set of different approaches to the anonymisation of CSR based on masking (redaction) but also other techniques (randomization, generalization) in order to increase the usefulness of published information.

5/New Data Protection Governance

The GDPR introduces a shift in paradigm about **compliance:**

The **Data Controller** has to adopt suitable measures to ensure and **demonstrate** compliance (Article 24).

Examples:

Documentation (Article 30);

Implement security requirements (Article 32);

Data Protection Impact Assessment (Article 32)+ privacy <u>by design</u> and <u>by default</u>

Designation of a DPO (Article 37)

Thank you for your attention

alessandro.spina@ema.europa.eu