EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Data Protection and Privacy: the new General Data Protection Regulation (GDPR)

Alessandro Spina
Data Protection Officer, EMA

An agency of the European Union

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

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

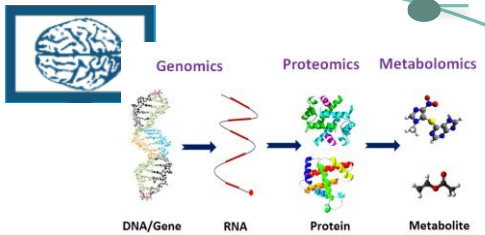
A data-driven society

- Massive production of **digital footprints** with always-on, connected devices such as smartphones, wearables, social media;
- Large scale or **complex collection and analysis of data**; capacity to detect hypothesis-generating patterns and make precise inferences about human behaviour;
- Generating value at the different stages of the data value chain will be at the centre of the **future knowledge economy.** Good use of data can bring opportunities also to more traditional sectors such as transport**, health** or manufacturing.

Imaging data

Clinical trial data

'Omic data (Genetic, proteomic, metabolomic)



Social media data/m-health

Published literature

PubMed.gov
US National Library of Medicine
National Institutes of Health

Datasources

Clinical databases (Prescriptions, EHRs and registries)

Regulatory data (ADR, sales, Safety updates, PASS, PAES)

1/ Reform of data protection legislation-

Regulation (EU) 679/2016 adopted 24 May 2016- apply by **25 May 2018**

General principles of the current legislation 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 20) "..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

- **Profiling** (Articles 21-22); "which produces legal effects concerning him or her or significantly affects him or her…"
- **Data Protection Impact Assessment** (Article 33); DP **by design** and **by default**;
- **DPO** (Articles 35-37)
- **Notification of Personal Data Security breaches** (Articles 31-33)
- **Sanctions** (up to 4% company annual global turnover) and new legal remedies (class actions);
- **EDPB** 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**, 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

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****".*

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

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.

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***"

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

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 towards **Accountability:**

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 by design and by default

Designation of a DPO (Article 37)

Thank you for your attention

alessandro.spina@ema.europa.eu