Europe's General Data Protection Regulation (GDPR), health data and research

Facilitating data flows and ensuring a high level of protection in a digitally connected world

Why me?

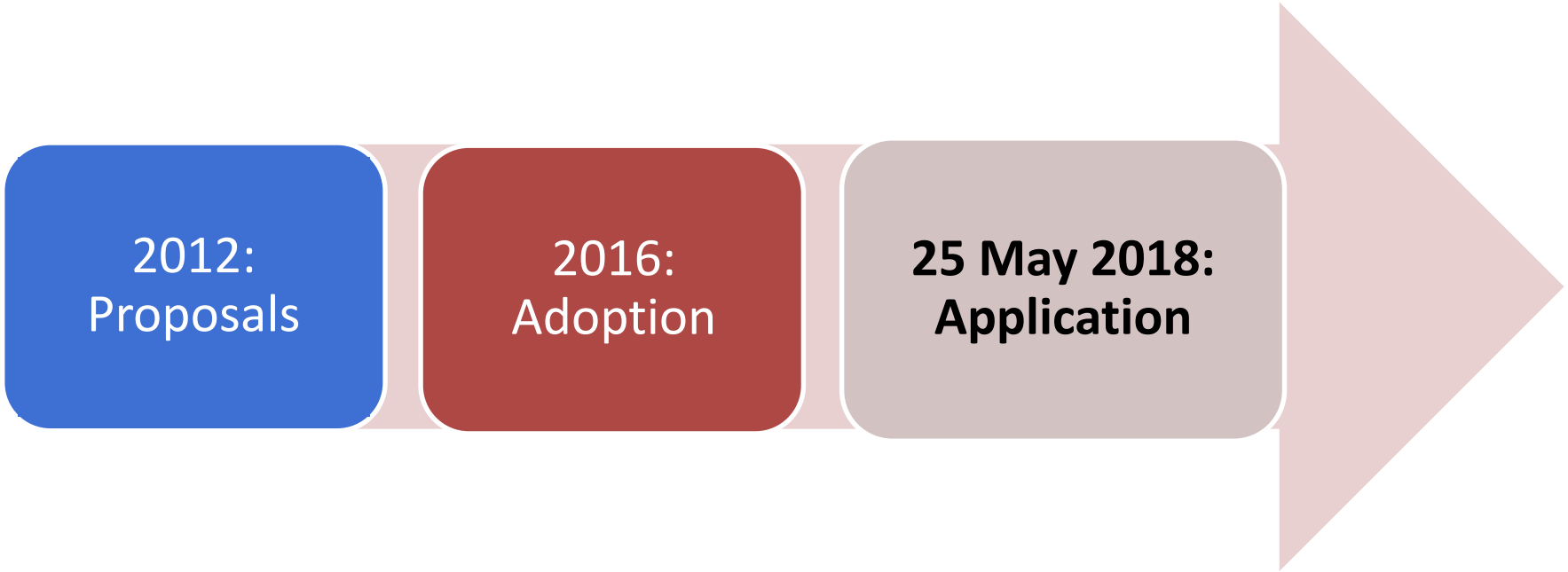
Ruxandra Draghia, MD, PhD

Disclaimer – this presentation contains description of GDPR and personal commentary, and does not reflect official positions of the European Commission or Merck &Co.

The EU Data Protection Reform Package: timeline

General Data Protection Regulation (GDPR)

2016-2018 was a transition period



What is the scope of this regulation?

GDPR **applies** to the **processing of personal data** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

GDPR **does not apply** to the processing of personal data:

- 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 common foreign and security policy;
- 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.
- generally, if the person is deceased.

Territorial scope

Possibly the biggest change to the regulatory landscape of data privacy in the European Union (EU) is the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the EU, **regardless of the company's location**.

It applies to clouds and datacenter providers and so do penalties ! [up to 20 million or 4% of annual turnover].

Controller and processor

Company X sells a medical device to consumers and uses Company Y to email consumers on their behalf and track use of the device, then with regard to such email activity data, Company X is the **data controller**, and Company Y is the **data processor**.

Distinction important for **compliance** - GDPR treats the **data controller as the principal party for responsibilities** such as collecting consent, managing consent-revoking, enabling right to access, etc. A data subject who wishes to revoke consent for his or her personal data therefore will contact the data controller to initiate the request, **even if such data lives on servers belonging to the data processor**. The data controller, upon receiving this request, would then proceed to request the data processor to remove the data from their servers.

Why did we need it - a harmonised and simplified framework

Evolution rather than revolution when compared to the previous directive: basic architecture and core principles are maintained (principles, legal bases, concept of personal data). Concept of personal data – not new.

- One single set of data protection rules for the EU (Regulation)
- One interlocutor and one interpretation (one-stop-shop and consistency mechanism)
- Creating a level playing field (territorial scope)
- Cutting red tape (abolishment of most prior notification and authorisation requirement), **including as regards international transfers**

Sensitive data
Health data
Genetic data
Pseudonymization
Anonymization

Principles of processing:

- Fair and lawful processing
- Purpose limitation
- Data minimization
- Rules on further processing
- Data retention
- Data accuracy
- Accountability

Legal bases for processing health data

- Relationship Art.6 (consent) and Art.9 (health, research)

- Explicit consent – ***clear affirmative action***
- Conditions for consent
- Consent for research – ***consent to specific areas of research***
- Based on national or EU law (Art. 9)
- Art. 9(4) – further conditions, including limitations on processing health data [Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health]

Article 9 – processing of genetic data, biometric data…, data concerning health is prohibited unless…..

- processing relates to personal data which are manifestly made public by the data subject….
- processing is necessary for reasons of **substantial public interest**….
- processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services**…
- 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**…
- processing is necessary for archiving purposes in the ***public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) …..***

Rules for research

Research – a privileged purpose subject to clear requirements - Art 9(2)(j) – law

Further processing for archiving purposes in the **public interest, scientific or historical research purposes or statistical purposes** shall, in accordance with Article 89(1), **not be considered to be incompatible with the initial purposes** ('purpose limitation');

Personal data may be stored for **longer periods** insofar as the personal data will be processed solely for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures … in order to safeguard the rights and freedoms of the data subject ('storage limitation');

Art 89 – safeguards for research processing, such as data minimization, pseudonymization, ***anonymization [anonymous data falls outside the scope of GDPR]***

Art 89(2) – restrictions to rights via Member State laws

An updated set of rights for individuals

Clearer rights for data subjects

- Transparency, clear, accessible language
- Right of information [….provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation … is likely to render impossible or seriously impair the achievement of the objectives of that processing….]
- Right of access
- Right to object
- Right not to be subject to automated decision making
- New right: right to portability; communication of data breach to data subject [within 72 hours]

Specific issues of use personal data in EU health research regarding the application of the GDPR

- Member States have the right to maintain or introduce further conditions, limitations (Art. 9(4)) – we want harmonization!
- Principles: further processing of personal data (Art. 5(1)(b) versus 'data limitation' (Art. 5(1)(c)) – as justified!
- Withdrawal of the consent by the data subject at any time (Art. 7(3))

Research - Horizon 2020 Societal Challenge 'Health, demographic change and wellbeing'

- Encourages the use of European infrastructures for storing, curation and processing of data, such as HBM4EU of IPChem information platform of chemical monitoring data, or Biobanking and Biomolecular Research Resource Infrastructure (BBMRI) for biological data.
- Provides for data management plans for projects, including those with multiple project partners in European countries and in international settings.
- Code of conduct under elaboration of BBMRI according to Article 40 of the GDPR.

Measures are foreseen to ensure compliance with the GDPR rules and principles

- Discussion with the concerned EU bodies/Member States and ***Scientific/Research societies*** about the need and possibilities for establishing coherent and harmonized guidelines.
- Coordinated actions for appropriate safeguards, e.g. European and International Thematic Research Networks.
- Harmonisation of standards for pseudonymisation/anonymisation.

Safe Harbour

Max Schrems

European Court of Justice

Privacy Shield

Edward Snowden

Transparency
Diversity
Credibility
Inclusion
Continued Research

Can we ever work together ?

- Currently, less than 10% of US businesses are prepared for GDPR!!!!! But, we can do it…..
- Transfer of personal data about EU citizens to the US - mechanisms for doing so:
  1. Binding Corporate Rules (BCRs)
  2. Privacy Shield – self-certification [applicable only to companies that are subject to the jurisdiction of the US Federal Trade Commission (FTC) or the Department of Transportation (DOT), but not many US banks or telecoms companies]: PrivacyShield.gov
  3. Model Contracts
  4. Explicit consent of the data subject
  5. Necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject – think twice!!!!
  6. If the transfer is necessary for issues of public interest, including public health research.

Conclusions

- GDPR underlines obligations for entities that process personal data in a risk-based approach
- GDPR creates **new exemptions for research**, specifically:
  - Broad consent to certain areas of research, harmonized safeguards, exemption from the right to be forgotten
  - GDPR exempts research from the principles of storage limitation and purpose limitation thus allows researchers to reasonably further process personal data beyond the purposes for which they were first collected.
  - Research by itself constitutes a legitimate basis for processing without a data subject's consent.
  - GDPR allows researchers to process sensitive data, such as biometric, health or genetic data.
  - GDPR allows in limited circumstances and with pre-requisite measures (pseudonymization) to transfer personal data to third countries considered not to provide an adequate level of protection.
  - To benefit from these exemptions, researchers must implement appropriate safeguards, and apply recognized ethical standards, lowering the risks for the rights of individuals.

Thank you very much for your attention!

Questions, comments?