Code of Practice on Secondary Use of Medical Data in European Scientific Research Projects

Anne BAHR, Ph.D, CIPP/E
Sanofi R&D Privacy Officer

SANOFI

Anne BAHR

R&D Privacy Officer

R&D
Based in France
Near Paris

Education

Ph.D. in Molecular Biology
CIPP/E certification

Professional experiences :

Academic Research (IGBMC, Strasbourg)

- 1994-1998: Wet lab
- 1998-2000: **Bioinformatics**

SANOFI group since November 2000

- **Bioinformatics (5 years)**
- R&D Privacy Officer France (2006)
- R&D Privacy Officer (2013 →)

- Ensure **compliance** with Data Privacy regulations across the **whole R&D organization**
  - Implement procedures
  - Assess all systems/ processing
  - Train departments
  - Manage relations with French SA
- Contribute to the management of the **GPO**
  - Manage communication tools (intranet, SharePoint, Connect, etc.)
  - Contribute to main activities (training material, policies, strategy, etc.)
- Manage the **R&D network**

Presentation Overview

- Personal Data Protection within the EU
  - **Definitions**
  - **Main principles**
- Code of Practice on Secondary Use of Medical Data in Scientific Research Projects
- Impact of the GDPR on the processing of R&D data
- Summary & Next Steps

Question 1 to the audience

How many of you know are in close connection with your company's R&D Privacy Officer*?

(*or person having equivalent responsibility)

SANOFI

Question 2 to the audience

How many of you feel not having enough information about privacy requirements?

SANOFI

Question 3 to the audience

How many of the represented companies* have joined Data Privacy and IS Security services?

(*Please one hand per company, then provide companies names)

SANOFI

Definition of Personal Data

SANOFI

Definition of Personal Data

- **Personal data** is "**any information relating to an identified or identifiable natural person** ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". *(Art. 2(a) of Directive 95/46/EC)*

Examples

- Name
- Address
- ID number
- Date of birth
- Photo
- Credit card numbers
- IP address
- Health records

Is Clinical Trial Data anonymous?

- Not really…
  - **For traceability reason, patient numbers match patients names at investigator's sites (i.e., hospital)**
  - **Data might contain many indirect identifiers**
    - Date of Birth, Weight, Height, Date of visit, etc.

- **Clinical Trial Data is Key-Coded (=Pseudonymised)**
  - **Are Personal Data**
  - **Are subject to privacy laws in Europe**
    - Specific categories in some countries

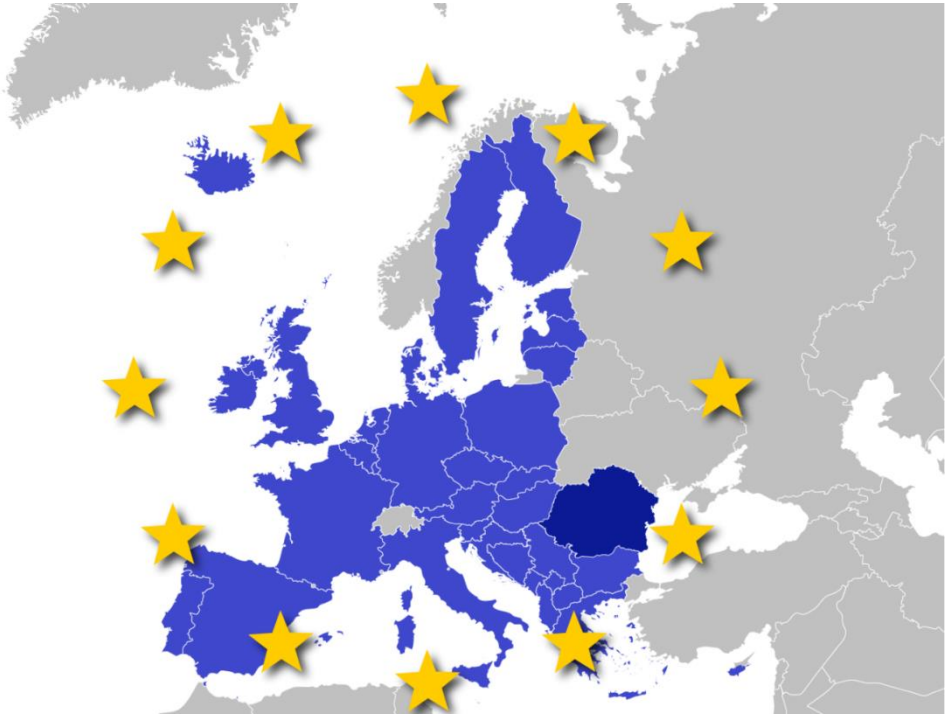
Current Personal Data Protection Framework

SANOFI

1995 Directive on Personal Data

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (24 October 1995)

→ Unique Directive but variations in its local implementations



Scope of the Privacy Directive/ EU local laws

- Applies to the **processing** of **personal data**
  - **Processing = collecting, recording, consulting, holding, using, ... data**
- Processing **sensitive** data is forbidden → requires **authorization**
  - **Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life**
  - **In some countries: SSN, Biometric data, Genetic data**
- Does not apply to **anonymous** data
- **Forbids the flow** of personal data from EU **to third countries** not ensuring an adequate level of protection
  - e.g., USA, China, Japan (**authorization** required)

Privacy Directive Principles

- Fairly and lawfully processed
- Limited and **defined purposes**
- Adequate, relevant and **not excessive**
- Accurate and up-to-date
- **Not kept** for **longer** than necessary
- Processed in line with the rights of data subjects
- Secure
- Not transferred to other countries without adequate protection

→ Principles implemented differently in local laws

How to comply with all local laws in multi-national Collaborative Research Projects?

→ Code of Practice on Secondary Use of Medical Data in Scientific Research Projects

SANOFI

Why developing a Code of Practice?

- Develop a unique - common across the EU - framework to reuse clinical (health) data
  - **Acceptable for EU collaborative research projects, IMI office, Privacy SA, Patients associations, Ethics Boards, …**
  - **Not a binding document as such (yet): A guidance to be used by IMI projects to address multi-partners multi-countries issues for complying with Personal Data Protection regulations**
  - **Provides EU harmonized operational solutions for being compliant with the EU Privacy directive**
    - Does not plan for all local exception
  - **Provides an harmonized solution to start from in multi-partners multi-countries, to be completed by applicable laws specificity where required**
- Published on IMI eTRIKS project website and on IMI Office website

Content of the Code

- **Collection**, **Use** and **Transfer** of Personal Medical Data
- **De-identification** and Protection of Anonymised Data
- **Information**, **Consent** and **Withdrawal**
- Human Biological **Samples**
- Data **Security** & Involvement of Data **Processors**
- Data **Retention**
- Data **Disclosure**

- Know more about the Code? Read our Article!
  - **Code of practice on secondary use of medical data in European scientific research projects - Anne Bahr & Irene Schlünder - International Data Privacy Law 2015 - *doi: 10.1093/idpl/ipv018* *(free access)***

Secondary Use of Medical Information under the Directive (Rule 20 of the Code)

- Personal medical data already lawfully collected for research purposes (e.g., data arising from clinical trials) **can be re-used** in another research project if:
  - **The initial consent covers the possibility of re-use, or,**
  - **The data have been de-identified and the initial consent does not explicitly forbid the planned secondary use, or,**
  - **Permitted by an applicable law**

Impact of the GDPR on the processing of R&D data

→ **Requires many clarifications from the EDPB**

SANOFI

Definition of Personal Data in the GDPR is nearly the same

Art. 2(a) of the Directive

- **Personal data** is "**any information relating to an identified or identifiable natural person** ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference **to an identification number** or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

Art. 4 of the GDPR

- **Personal data** is "**any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference **to an identifier such as a name, an identification number, location data, an online identifier** or to one or more factors specific to the physical, physiological, **genetic**, mental, economic, cultural or social identity **of that natural person**"

Processing Health Data
[Article 9 and 83]

- Processing of personal data concerning health is prohibited
  - **Not applicable if processing is necessary for scientific research purposes**
  - **If technical and organisational measures implemented to ensure the respect of data minimisation**
    - Pseudonymisation or anonymisation
- Union or Member State law may provide for derogations…
- Legal basis is still needed

Legal Basis for Research
[Recital 45, 47 & Article 6(1)]

- **Consent** for one or more **specific** purposes
- Necessary for the performance of a **task carried out in the public interest**
  - **Processing should have a basis in Union or national law.**
- Necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party
  - **Only if the interests or the data subject are not overriding and aligned with expectations**

Consent
[Recital 33 & Article 7]

- Data subjects should be allowed to give their consent to **certain areas of scientific research**
- Data subjects should have the **opportunity to give their consent only to certain areas of research**.
- The consent for data protection must be **clearly distinguishable** from any other matters.

→ An opportunity to better recognise broad consent

→ May require “à la carte” consent

Pseudonymisation & Scope
[Recital 26 & Article 4(5)]

- **Definition** of pseudonymisation (**NEW**)
  - *Personal data which can **no longer be attributed to a specific data subject without the use of additional information**, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*

- Pseudonymised data are in scope/ **are personal data**
  - If a re-identification key exists, or,
  - If an individual can be singled-out (**NEW**)

- Anonymised data are NOT in scope/ **are NOT personal data**

Secondary use/ Further processing
[Recital 50 & 156, Article 5(1)(b)]

- Personal data **can be further processed** if **compatible** with initial purposes (**NEW**)
  - **Further processing for scientific research purposes is deemed compatible**
  - **If assessed that cannot be done with anonymized data**
  - **If appropriate safeguards exist (for instance, pseudonymisation)**

→ Hospital records to be used in studies and research projects?

→ Clinical trials data to be further used without being fully anonymised?

Information of data subjects must include:
[Art 13]

- the identity and the contact details of the controller, incl. (NEW) contact details of the data protection officer
- the purposes of the processing and (NEW) the legal basis of the processing
- (NEW) where applicable, the legitimate interests pursued by the controller
- the recipients of the personal data
- the transfer of personal data to a third country
- (NEW) the intended transfer of personal data to an international organisation inc. the existence or absence of an **adequacy decision** by the Commission, **or** reference to the **appropriate safeguards** and the means to obtain a copy
- (NEW) the period for which the personal data will be stored
- the right to access, rectify, (NEW) restrict access, (NEW) object to the processing, erase personal data and the right to (NEW) data portability, (NEW) the right to withdraw consent, (NEW) the right to lodge a complaint to a supervisory authority

Exemption for Information when data where **not collected directly** [Art 14(5)(b)]

- No obligation to provide information if it proves **impossible or would involve a disproportionate effort**, in particular for **processing for scientific research purposes**
  - **Does not apply to data collected directly**

- In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including **making the information publicly available**

→ Legal basis for Big Data Projects if advertised

Right to erasure/ Right to be forgotten
[Art 21(6)]

- The data subject has the **right to object to processing of personal data processed for scientific research** purposes unless the processing is necessary for the performance of a task carried out for reasons of public interest
  - **The right to object apply to research, but not when for public interest**

→ This may be an issue for secondary use of clinical trial data

Summary & Next Steps

SANOFI

Summary

- 4 possible legal basis for research
  - Specific Consent / Compatible with initial Consent / Public Interest* / Legitimate Interest
- No information if it requires disproportionate effort
  - Requires making the information publicly available
- Pseudonymised data (e.g. CT data) are personal data
  - As long as a key exist or a patient can be singled-out
- Anonymized data are NOT personal data
- Requires data minimization
- Broad consent is valid
  - Requires options to consent only to some parts
  - Requires additional information to be valid

Next Step:

BD4BO – CSA, an IMI project on Data Privacy

SANOFI

IMI – Joining forces from public and private bodies

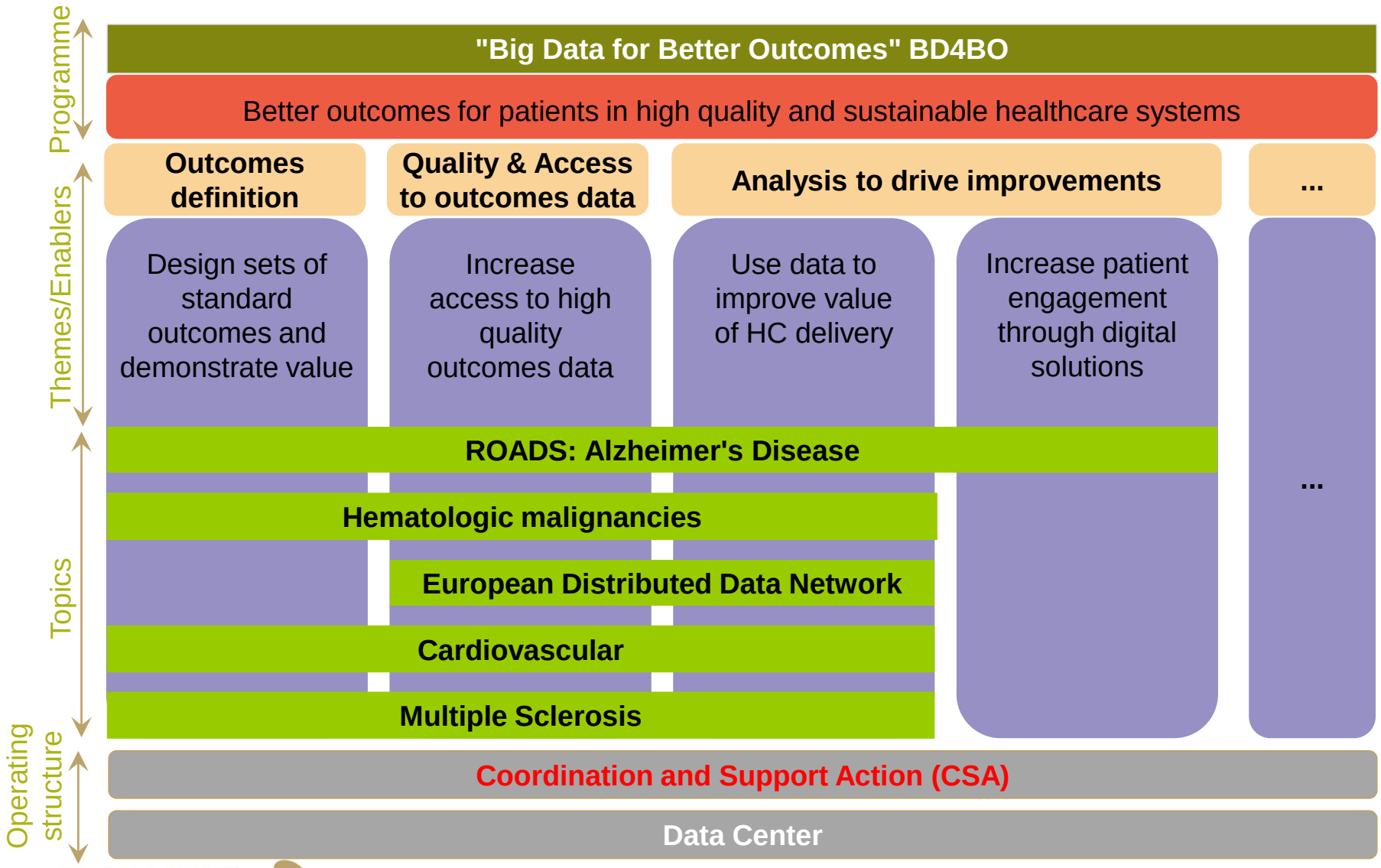
Innovative Medicines Initiative:
Joining Forces in the Healthcare Sector

IMI1 & IMI2
2008 - 2024

The biggest public/private partnership in Life Science aiming to:

- Make drug R&D processes in Europe more **innovative** and **efficient**
- Enhance Europe's **competitiveness**
- Address key **societal challenges**

"Big Data for Better Outcomes" programme



BD4BO - CSA - WP4 Deliverables

- Minimum standards/ **ICF templates** for the use of clinical data and human samples for:
  - **Clinical studies/ other studies / donation of human biological samples**

- **Guidance documents**
  - **to facilitate work with ICF and with Big Data**
  - **dealing with related common data protection issues**

- **Training and educational guidance** for BD4BO, IMI/ IMI2 projects, non-IMI related addressees (e.g. patients, Ethics Committees)

Thank you for you attention

Questions?

Anne.BAHR@Sanofi.com

SANOFI

Status of the Code and Next Steps

- **Final draft** (dated August 27th, 2014) prepared with the 2 experts
  - **Submitted to the EDPS (as an IMI guidance/ tool) in Aug. 2014**
  - **Submitted to the CNIL (→ Art29WP) in Dec. 2014 + Belgian DPA**

- **Article** (published in Sep. 2015)

  → Both to be submitted directly to the Art.29 WP

- EFPIA to work on an industry-wide **CoC** based on this code

- EFPIA / IMI launched a "Coordination and Support Action (CSA) for the Big Data for Better Outcomes (**BD4BO**) program" including data privacy topics ("Advice and requirements on legal, ethics, regulation, data privacy considerations").

Key Actors

Acts only on instruction of the DC

Determine purpose and means

The person who's data is processed

Processor

Data Controller

Data Subject

Recipient

Other 3rd-parties having access to data

Regulator

Art29WP

Transfer of Personal Data: 1) to a third-party

- Requires a “processing Agreement” stipulating in particular that
  - **The processor shall act only on instructions from the controller**
  - **The processor shall implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing**
  - **The processor, as well as any person acting under his authority, must not process personal data except on instructions from the controller, unless he is required to do so by law**

→ Privacy clauses developed by Isabelle Cadiau (see latest drafts here)

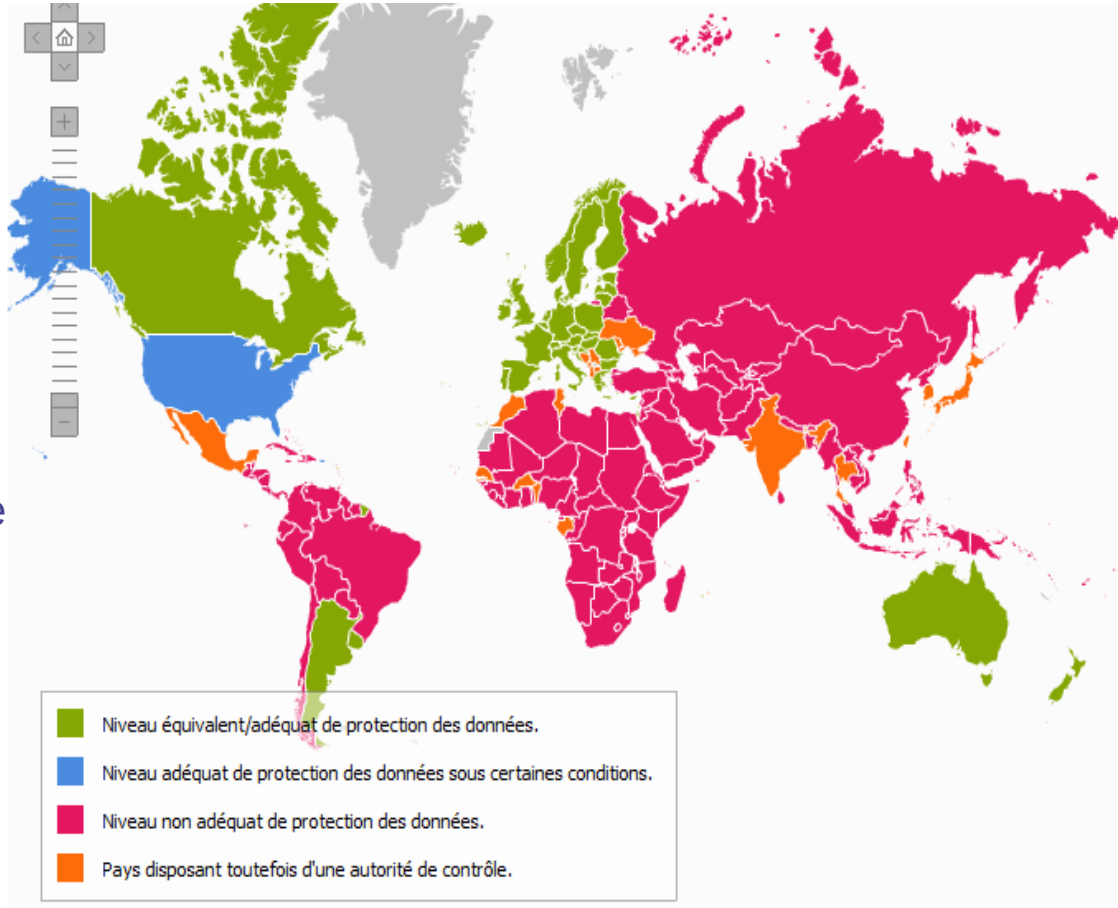
- NOTE: Member States shall provide Security requirements
  - **Processor MS law applies on security measures!**

Transfer of Personal Data: 2) to a third-country

- **Within** the EEA (all EU countries + Iceland, Liechtenstein and Norway)
  - **Free transfer**

- To a country with **adequate level** of data protection
  - **Permitted if "adequacy" recognized by the European Commission**

- To a **country with no** adequate level of data protection
  - **Particular safeguards to be implemented (standard contractual clauses, binding corporate rules, consent, ~~US safe harbor~~)**



Safe Harbor → Standard Contractual Clauses to be implemented

- SCC reflect provisions of the Data Privacy Directive:
  Principle aim = **ensure that EU Privacy Directive principles are maintained when data is transferred outside the EU**

- Two types of contracts (all documents available here)
  - **Controller to Controller or Controller to Processor**

- The GPO shall take care of the applications/ collaboration notified to it
  - **Replace SH → SCC for 5 application for R&D**
  - **SCC in place with Cognizant, QSI, Indigene (on-going for Medidata)**

- **IS** or **Legal** must ensure that all external vendors/ CROs processing PD outside of the EU have signed the SCC
  - **Inform the GPO of those who have not**
  - **Implement the SCC**

U.S. ★ EU
SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE

Binding Corporate Rules

SANOFI

U.S. EU SAFE HARBOR
U.S. DEPARTMENT OF COMMERCE

What is it ?

- Safe Harbor is the name of an agreement between the United States Department of Commerce and the European Union that regulated the way that U.S. companies could export and handle the personal data of European citizens.

Context

On **Oct 6th 2015** : invalidation of the US Safe Harbor by the CJEU ("Safe Harbor decision").

- Transfers of personal data from the EEA Sanofi affiliates to the USA still taking place in conformity with Safe Harbor certification are deemed unlawful.
- All types of data are concerned

U.S. EU SAFE HARBOR
U.S. DEPARTMENT OF COMMERCE

- **Consequences and actions taken within Sanofi:**
  - **Oct 9th & 13th, 2015 : Request to check and list the contracts already executed on a Safe Harbor basis (in process at the corporate level with the database MisContrat and CNIL Declarations)**
    - information sent to the Legal Steering Committee (LSC) members and Local Privacy Officers (LPO)
  - **From Oct 6th, 2015 , to use only the "EU Commission Model Clauses" as the legal basis for transfer**
  - **Nov 26th, 2015: generic email and amendment to the current contracts provided , sent to the LSC members and French Data protection Committee members**
- **Next steps:**
  - **End of January 2016 : WP 29 will issue recommendations**
  - ***Germany* : clarification needed about the legality of the BCR and EU Clauses**

Binding Corporate Rules

What are Binding Corporate Rules designed to achieve?

- **Binding Corporate Rules (BCRs) are designed to allow multinational companies to transfer personal data from the European Economic Area (EEA) to their affiliates located outside of the EEA in compliance with the 8th data protection principle and Article 25 of Directive 95/46/EC.**

- **Binding corporate rules should not be considered as the only or the best tool for carrying out international transfers but only as an additional one**
  - Other existing instruments : standard contractual clauses
  - *Until October 5th 2015 the Safe Harbor*

It's a kind of "codes of conduct for international transfers"

Binding Corporate Rules

- **BCR within Sanofi (28 October 2009)**
  - Current scope :
    - **Employee data; Clinical-trial and pharmacovigilance data.**
    - List of Sanofi affiliates having signed the BCR as of October 31st, 2014 Available on Internet / Intranet
  - New scope to be defined
    - KOL, HCP, vendors …
- **Formalities :**
  - Authorization from CNIL (French DPA) must still be obtained for each application

BD4BO - CSA at a glance

The Coordination and Support Action will:

- Drive Health Outcomes strategy of the BD4BO program
- Integrate knowledge and disseminate findings
- Design approaches to ensure sustainability of projects in the program
- Ensure consistency and quality across projects
- Bring and share expertise across all diseases and themes

Coordination and Support Action (CSA)
Key themes to be addressed

EFPIA participants of Work Package 4

- Bayer (lead)
- Sanofi (co-lead)
- Boehringer Ingelheim
- Celgene
- Eli Lilly
- GSK
- Janssen
- Novartis
- UCB

Data Retention
[Article 5(1)(e)]

- Personal data must be **kept for no longer than is necessary** for the purposes

- Personal data may be **stored for longer periods** for **scientific research** purposes + appropriate technical and organisational of Art. 89

→ Legal basis for keeping clinical trials data much longer than today

Inspired from the ***Welcome Trust*** draft GDPR assessment document

Processing for research purposes
[Art 89 & Recital 156]

- **Technical and organisational measures** must be in place in particular in order to ensure the respect of the principle of data **minimisation**.
  - **These measures may include pseudonymisation (Anonymization to be used where possible)**

- Union or Member State law **may provide for derogations** from the rights referred to in Articles 15 (access), 16 (rectification), 18 (restriction of processing) and 21 (opposition), if:

- **Member States should provide for appropriate safeguard** to the processing of personal data for scientific research purposes

→ Cross-border research projects will face challenges for complying with different approaches