



Impact of International Privacy Regulations on Health Data Standards

Pierre-Yves Lastic, Secretary General, EFDPO

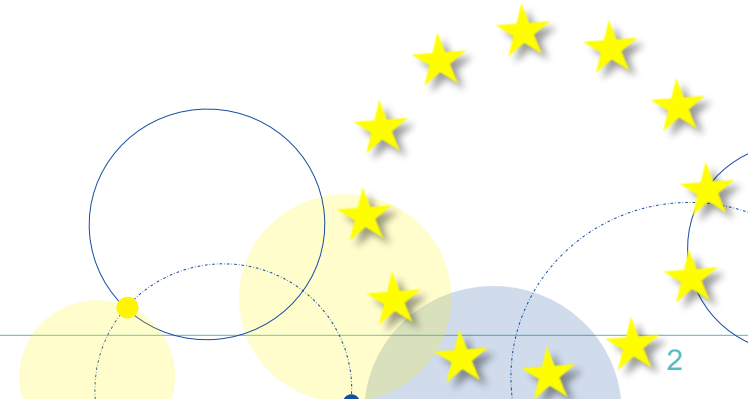


**EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS**



OVERVIEW

- Short presentation of EFDPO
- Evolution of International Privacy and Personal Data Protection Laws
- Digital Agenda of the European Union : New Data Regulations
- Impact on worldwide Health Data Standards



THE EUROPEAN FEDERATION OF
DATA PROTECTION OFFICERS
(EFDPO)



MEMBER ASSOCIATIONS

12 National Associations representing over 3900 DPOs



EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS



Spolek pro ochranu
osobných údajov



DAPRI
COMMUNITY



privacyofficers.at



Spolek pro ochranu
osobných údajů



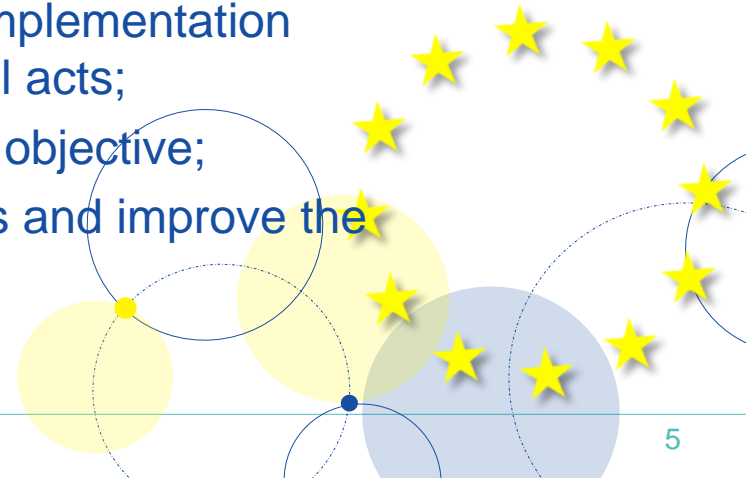
DATENSCHUTZ GESTALTEN

★ Associate members: Brazil, Croatia



MAIN OBJECTIVES

- Create a European network of national associations to exchange information, experience and methods;
- A continuous dialogue with the political sphere, business representatives and civil society to ensure a flow of information from the European to the national level;
- Proactively monitor, evaluate and shape the implementation of the GDPR and other European privacy legal acts;
- Keep the existing rules for DPOs as minimum objective;
- Promote high qualification standards for DPOs and improve the quality of training and professional practice.





WORKING GROUPS

- **Healthcare sector**
 - Health Data Certification for DPO and Privacy Officers
 - Analysis of (proposed) new regulations > position papers
 - Best Practices: Anonymization/Pseudonymization, Handling of Genetic Data, Artificial Intelligence in Healthcare & Biomedical Research
- **Cybersecurity**
 - Technology monitoring, best practices, training
- **Artificial Intelligence and personal data**
 - Analysis of proposed EU regulation (AI Act) and position paper
- **Art. 39 vs. national restrictions regarding legal counselling**
 - Respective roles of DPOs and lawyers

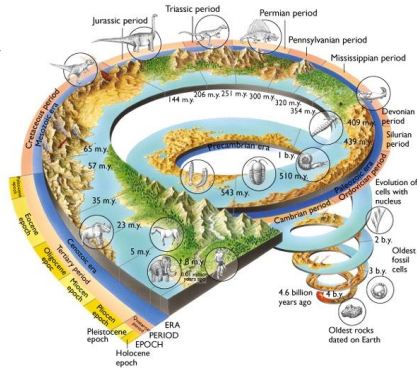


INTERNATIONAL PRIVACY AND PERSONAL DATA PROTECTION LAWS & REGULATIONS



A FEW DATES

- 1970: First data protection code in Hesse, Germany
- 1978: Federal Data Protection Act in Germany
"Loi informatique et liberté" in France
- 1980: OECD guidelines concerning the protection of privacy and transborder flows of personal data
- 1981: European Council Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
 - Remains the only international and universal legally binding instrument open to accession by any country, including non-member states
- 1995: Directive 95/46 EC on Personal Data Protection
- 1996: Health Insurance Portability and Accountability Act (HIPAA)
- 2000: Safe Harbor Privacy Principles of the U.S. Department of Commerce in consultation with the European Commission
- 2003: Japanese Privacy Act
- ■ ■ ■
- **2018: EU General Data Protection Regulation becomes applicable!**





THE 8 OECD BASIC PRINCIPLES

- **Collection Limitation**
 - data obtained by lawful and fair means and with the knowledge or consent of the data subject.
- **Data Quality**
 - Data should be accurate, complete and up-to-date
- **Purpose Specification**
 - Purpose or change of purpose must be declared before data collection
- **Use Limitation**
 - Use only for the declared purpose
- **Security Safeguards**
 - Protection against unauthorized access, destruction & disclosure
- **Openness**
 - Which data exist, who uses it, for which purpose
- **Individual Participation**
 - access & change right
- **Accountability**
 - Controller is accountable for complying



CHRONOLOGY OF U.S. FEDERAL HEALTH PRIVACY LAWS

- **HIPAA – The Health Insurance Portability and Accountability Act of 1996**
 - Enacted in part to set the standards for medical/health information privacy.
 - Privacy Rule governs the use and disclosure of an individual’s health information.
 - Security Rule requires physicians, healthcare providers and health plans to protect health information in electronic form.
- **GINA – the Genetic Information Nondiscrimination Act of 2008**
 - Prohibits employers and health insurance companies from using genetic information to discriminate based on genetic predisposition to developing disease in the future.
- **HITECH - The Health Information Technology for Economic and Clinical Health Act of 2009**
 - Enacted as part of the American Recovery & Reinvestment Act (2009 Stimulus Bill).
 - Expands HIPAA’s Privacy and Security Rules; includes updated enforcement provisions, data breach notification provisions, and applies HIPAA directly to Business Associates.
- Interim Final Rule (Data Breach Provisions) August 2009
- Interim Final Rule (Enforcement Provisions) October 2009
- **Omnibus Final Rule March 2013**
 - HHS OCR issued its HITECH Final Rule modifying and implementing HIPAA’s Privacy, Security, Enforcement and Breach Notification Rules pursuant to HITECH.





THE APEC GUIDELINES

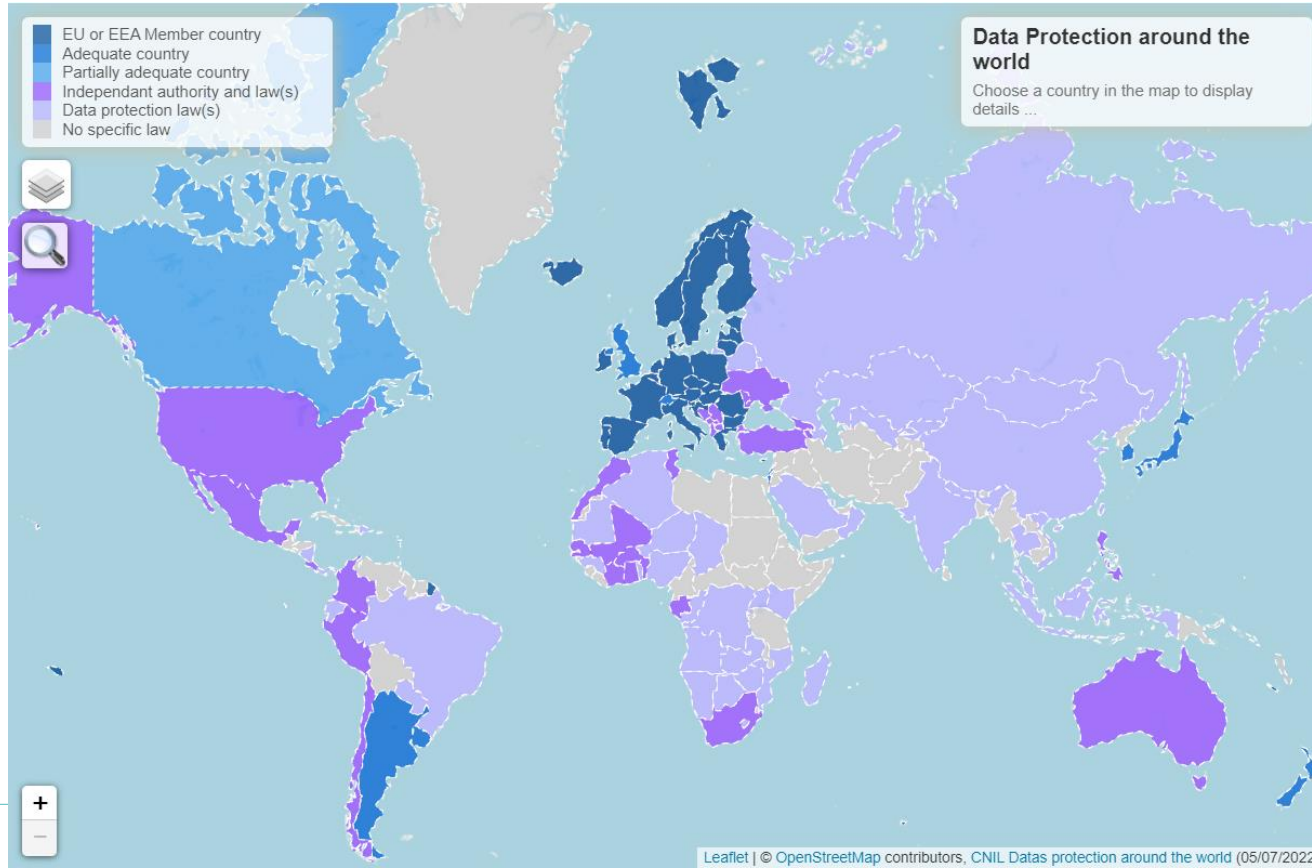
- **The Asia-Pacific Economic Cooperation published in 2005 a framework including**
 - principles based on the OECD guideline and
 - guidance for implementation
- **APEC information privacy principles**
 - Preventing Harm
 - Notice
 - Collection Limitations
 - Uses of Personal Information
 - Choice
 - Integrity of Personal Information
 - Security Safeguards
 - Access and Correction
 - Accountability
- **Implementation**
 - Domestic & International
- **The framework was updated in 2015, but is not yet considered providing sufficient protection by the EU**



**Asia-Pacific
Economic Cooperation**



WORLDWIDE PRIVACY FROM AN EU POINT OF VIEW





2030
DIGITAL
COMPASS

THE EUROPEAN WAY
FOR THE DIGITAL DECADE

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence

Artificial Intelligence Act
21 April 2021



A European Strategy for Artificial Intelligence

Presentation by Lucilla SIOLO

Director for Artificial Intelligence and Digital Industry, DG CNECT, European Commission

AI is good ...

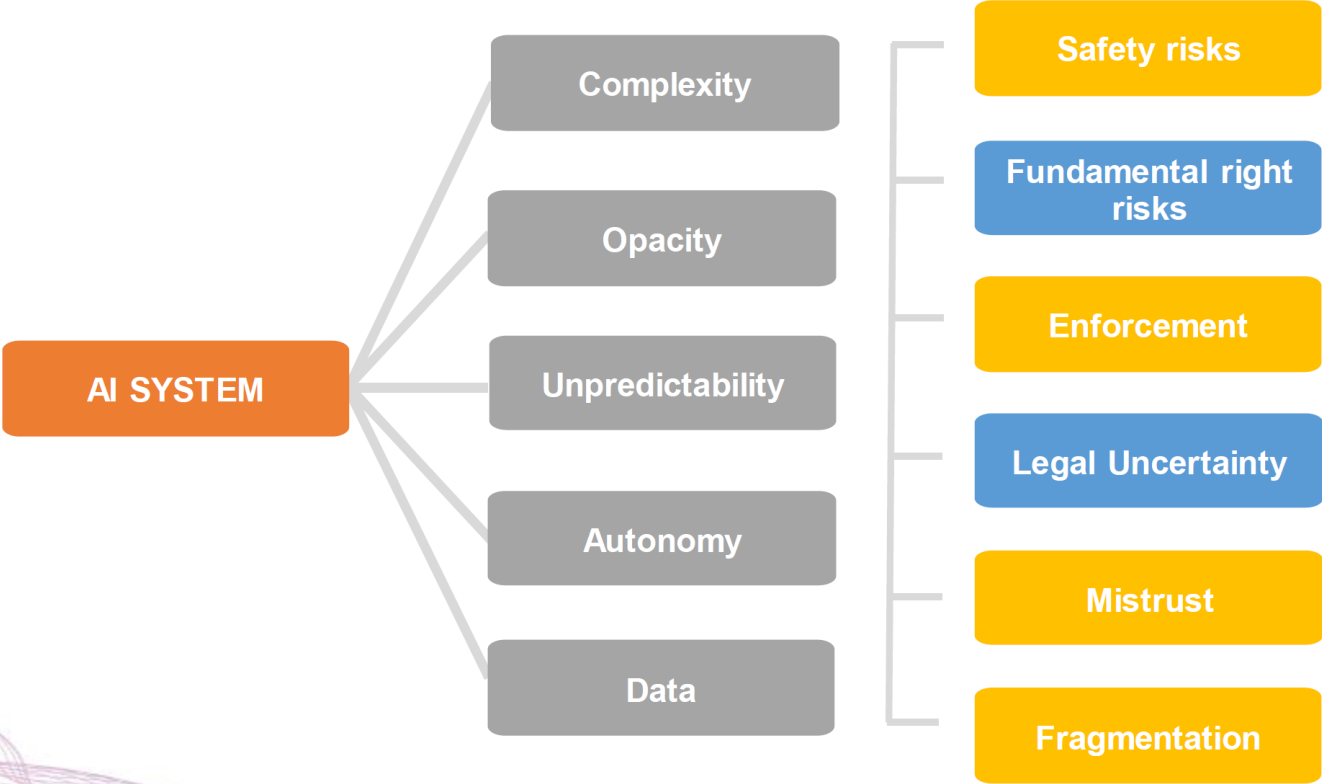
- For citizens
- For business
- For the public interest



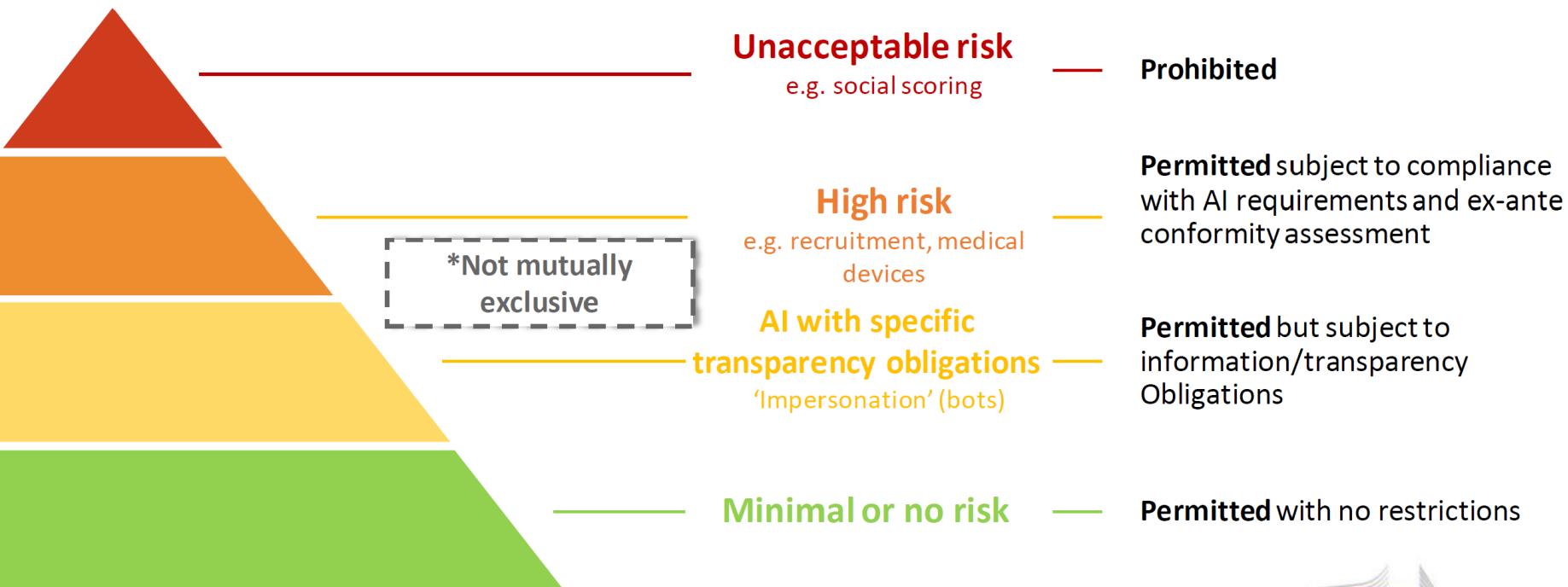
... but creates some risks

- For the safety of consumers and users
- For fundamental rights

Why does the EU regulate AI use cases?



A risk-based approach to regulation



Most AI systems will not be high-risk (Titles IV, IX)



New transparency obligations for certain AI systems (Art. 52)

- ▶ **Notify humans** that they are **interacting with an AI system** unless this is evident
- ▶ Notify humans that emotional recognition or biometric categorisation systems are applied to them
- ▶ Apply **label to deep fakes** (unless necessary for the exercise of a fundamental right or freedom or for reasons of public interests)

Possible voluntary codes of conduct for AI with specific transparency requirements (Art. 69)

- ▶ No mandatory obligations
- ▶ Commission and Board to encourage drawing up of codes of conduct intended to foster the **voluntary application of requirements to low-risk AI systems**

High-risk Artificial Intelligence Systems (Title III, Annexes II and III)



Certain applications in the following fields:

1 SAFETY COMPONENTS OF REGULATED PRODUCTS

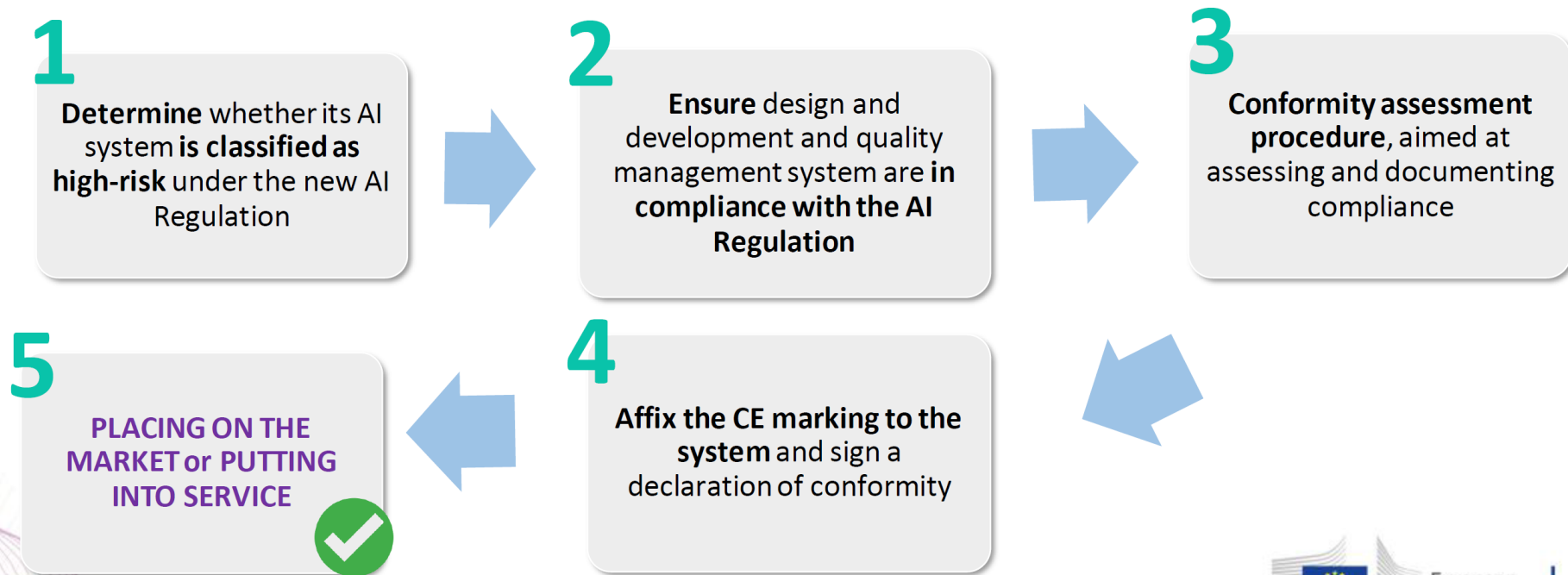
(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation

2 CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING FIELDS

- ✓ Biometric identification and categorisation of natural persons
- ✓ Management and operation of critical infrastructure
- ✓ Education and vocational training
- ✓ Employment and workers management, access to self-employment
- ✓ Access to and enjoyment of essential private services and public services and benefits
- ✓ Law enforcement
- ✓ Migration, asylum and border control management
- ✓ Administration of justice and democratic processes

CE marking and process (Title III, chapter 4, art. 49.)

CE marking is an indication that a product complies with the requirements of a relevant Union legislation regulating the product in question. In order to affix a CE marking to a high-risk AI system, a provider shall undertake **the following steps**:



Requirements for high-risk AI (Title III, chapter 2)

Establish and implement **risk management** processes
&
In light of the **intended purpose** of the AI system

Use high-quality **training, validation and testing data** (relevant, representative etc.)

Establish **documentation** and design logging features (traceability & auditability)

Ensure appropriate certain degree of **transparency** and provide users with **information** (on how to use the system)

Ensure **human oversight** (measures built into the system and/or to be implemented by users)

Ensure **robustness, accuracy** and **cybersecurity**

Overview: obligations of operators (Title III, Chapter 3)



Provider obligations

- ▶ Establish and Implement **quality management** system in its organisation
- ▶ Draw-up and keep up to date **technical documentation**
- ▶ **Logging** obligations to enable users to monitor the operation of the high-risk AI system
- ▶ Undergo **conformity assessment** and potentially re-assessment of the system (in case of significant modifications)
- ▶ Register AI system in EU database
- ▶ Affix CE marking and sign declaration of conformity
- ▶ Conduct **post-market monitoring**
- ▶ **Collaborate** with market surveillance authorities

User obligations

- ▶ Operate AI system in accordance with **instructions of use**
- ▶ Ensure **human oversight** when using of AI system
- ▶ **Monitor** operation for possible risks
- ▶ **Inform the provider or distributor about any serious incident** or any malfunctioning
- ▶ **Existing legal obligations** continue to apply (e.g. under GDPR)

Lifecycle of AI systems and relevant obligations



Design in line with requirements



Ensure AI systems **perform consistently for their intended purpose** and are in **compliance with the requirements** put forward in the Regulation

Conformity assessment



Ex ante conformity assessment

Post-market monitoring



Providers to **actively and systematically collect, document and analyse relevant data** on the reliability, performance and safety of AI systems throughout their lifetime, and to **evaluate continuous compliance of AI systems with the Regulation**

Incident report system



Report serious incidents as well as malfunctioning leading to breaches to fundamental rights (as a basis for investigations conducted by competent authorities).

New conformity assessment



New conformity assessment in case of **substantial modification** (modification to the intended purpose or change affecting compliance of the AI system with the Regulation) by providers or any third party, including when changes are **outside the “predefined range”** indicated by the provider for **continuously learning AI systems**.



DATA ACT (DA) & DATA GOVERNANCE ACT (DGA)

- DGA and DA are key pillars of the EU's digital strategy
 - The DA proposed in February 2022 aims at making more data available for re-use by setting rules on who can access and use data and under what conditions
 - The DGA seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data.

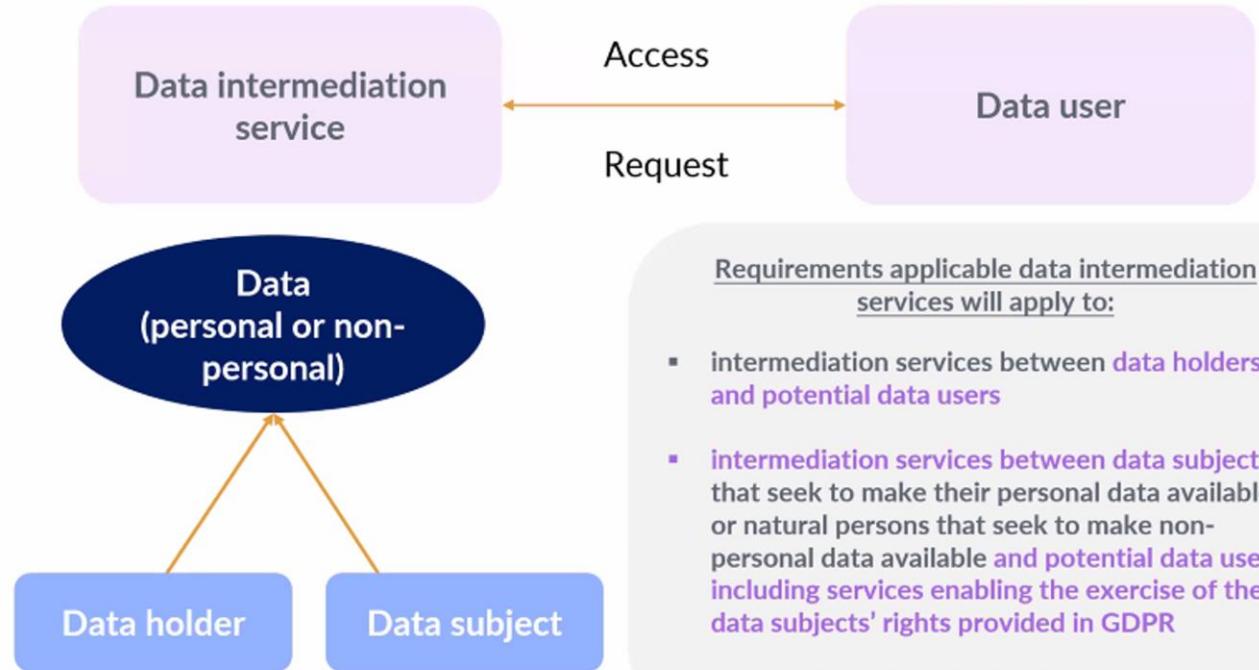


DGA: DATA INTERMEDIATION SERVICES (1/2)

4. Data intermediation services (art. 10 to 15)

Definition:

"a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data"



Requirements applicable data intermediation services will apply to:

- intermediation services between **data holders and potential data users**
- **intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available and potential data users, including services enabling the exercise of the data subjects' rights provided in GDPR**
- **services of data cooperatives**



DGA: DATA INTERMEDIATION SERVICES (2/2)

REQUIREMENTS AND OBLIGATIONS

Positive obligations (what the service provider shall do)	Negative obligations (what the service provider shall not do)
Provide intermediation services through a separate legal entity	Not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users
<p>Facilitate the exchange of data in the format in which it is received (unless conversion to another format is required to enhance interoperability within and across sectors or if requested by the data user or required by European law or to ensure harmonisation with international or European standards)</p> <p>May provide additional specific tools and services to facilitate the exchange of data (e.g. temporary storage, curation, anonymisation tool, etc.) <u>but only for this purpose</u></p>	<p>The data collected for the purpose of the provision of the data intermediation service (such as date, time, geolocation data, duration of activity and connections to other persons) shall be used only for the development of that data intermediation service, which may entail the use of data for the detection of fraud or cybersecurity, and shall be made available to the data holders upon request</p> <p>The commercial terms shall not be made dependent upon whether the data holder or data user uses other services provided by the same data intermediation services provider or a related entity</p>
Ensure that the procedure for access to its service is fair, transparent and non-discriminatory	
Have procedures in place to prevent fraudulent or abusive practices	
Ensure reasonable continuity in the event of its insolvency and have mechanisms to ensure that users can access, transfer or retrieve their data	
<u>Take appropriate measures to ensure interoperability with other data intermediation services</u>	
Inform data holders of any unauthorised transfer, access or use of the non-personal data that it has shared	

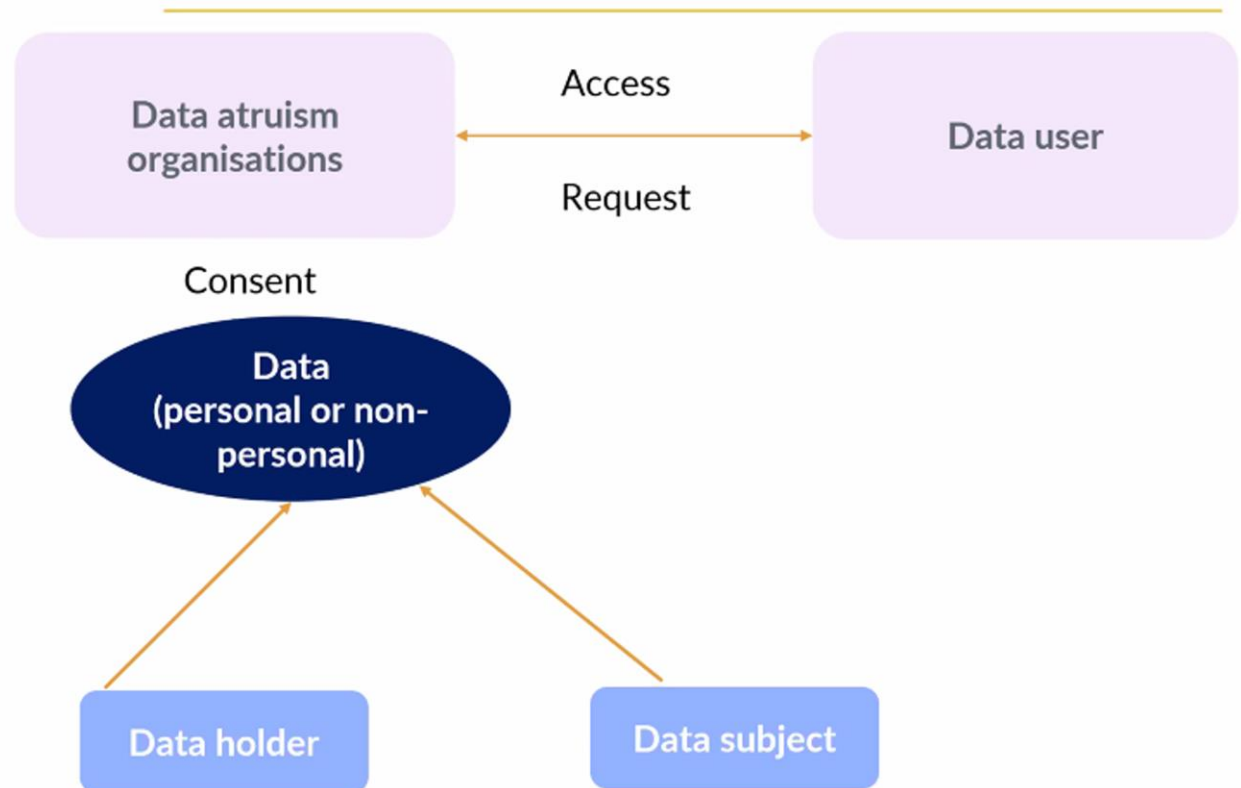


DGA: DATA ALTRUISM

5. Data altruism (art. 16 to 25)

Definition:

"the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest"





EUROPEAN HEALTH DATA SPACE

- **Putting people in control of their own health data, in their country and cross-border**
 - Thanks to the EHDS, people will have immediate, and easy access to the data in electronic form, free of charge. They can easily share these data with other health professionals in and across Member States to improve health care delivery. Citizens will be in full control of their data and will be able to add information, rectify wrong data, restrict access to others and obtain information on how their data are used and for which purpose.
 - Member States will ensure that patient summaries, ePrescriptions, images and image reports, laboratory results, discharge reports are issued and accepted in a **common European format**.
 - Interoperability and security will become mandatory requirements. **Manufacturers of electronic health record systems will need to certify compliance with these standards.**
- **To ensure that citizens' rights are safeguarded, all Member States have to appoint digital health authorities.**
 - These authorities will participate in the cross-border digital infrastructure (MyHealth@EU) that will support patients to share their data across borders.



EUROPEAN HEALTH DATA SPACE

- **Improving the use of health data for research, innovation and policymaking**
 - The EHDS creates a strong legal framework for the **use of health data for research, innovation, public health, policy-making and regulatory purposes**. Under strict conditions, researchers, innovators, public institutions or industry will have access to large amounts of high-quality health data, crucial to develop life-saving treatments, vaccines or medical devices and ensuring better access to healthcare and more resilient health systems.
 - **The access to such data by researchers, companies or institutions will require a permit from a health data access body, to be set up in all Member States. Access will only be granted if the requested data is used for specific purposes, in closed, secure environments and without revealing the identity of the individual.** It is also strictly prohibited to use the data for decisions, which are detrimental to citizens such as designing harmful products or services or increasing an insurance premium.
 - The health data access bodies will be connected to the new decentralised EU-infrastructure for secondary use (HealthData@EU) which will be set up to support cross-border projects.

IMPACT ON WORLDWIDE HEALTH DATA STANDARDS



INTEROPERABILITY

- Developing best practices for the use of **Artificial Intelligence** in clinical trials is a must, just as CDISC did help set up rules for eCRF and ePRO.
- Data sharing will need to follow the **Data Governance Act** as well as **GDPR**
- Use of data from the **European Health Data Space**, for example for Real World Evidence Studies will require interoperability within existing Health Data Standard, e.g. CDISC & HL7
- The new **common European health data standard** with most certainly build upon these existing standards, but with increased security and confidentiality requirements.




BEST PRIVACY PRACTICES

- **Privacy Impact Assessments** in Clinical Research
 - Mandatory in the EU for clinical studies, use of genetic data, Artificial Intelligence or new technologies (e.g. wearables, connected devices, etc.)
- Privacy by Design
 - Data Minimization principle
 - Standard Protocol Text Bricks
 - Anonymization & Pseudonymization in practice (PHUSE example)
 - Handling of Genetic Data
 - Use of Artificial Intelligence in Data Management, Analysis and Reporting



GDPR CHECKLIST TO FEED YOUR PIA

1. **General/Global Checks:**
 - Relevant policies & procedures, e.g. standardized content for Patient Informed Consent, Cybersecurity policies, Record Keeping policies
2. **Study specific checks:**
 - GDPR compliance of Protocol, Case Report Forms, Data Management Manual, etc.
3. **Risk Assessment and mitigation plans**



PIA, templates February 2018 edition

Contents

Foreword.....	2
1 Study of the context: templates.....	4
1.1 Overview of the processing.....	4
Description of the processing under consideration.....	4
Sector-specific standards applicable to the processing.....	4
1.2 Data, processes and supporting assets.....	4
Data description, recipients and storage durations.....	4
Description of the processes and supporting assets.....	4
2 Study of the fundamental principles: templates.....	5
2.1 Assessment of the controls guaranteeing the proportionality and necessity of the processing.....	5
Explanation and justification of purposes.....	5
Explanation and justification of lawfulness.....	5
Explanation and justification of data minimization.....	6
Explanation and justification of data quality.....	6
Explanation and justification of storage durations.....	6
Assessment of the controls.....	6
2.2 Assessment of controls protecting data subjects' rights.....	7
Determination and description of the controls for information for the data subjects.....	7
Determination and description of the controls for obtaining consent.....	8
Determination and description of the controls for the rights of access and to data portability.....	8
Determination and description of the controls for the rights to rectification and erasure.....	10
Determination and description of the controls for the rights to restriction of processing and to object.....	11
Determination and description of the controls applicable to processors.....	11
Determination and description of the controls on transfer of data outside the European Union.....	12
Assessment of the controls.....	12
3 Study of data security risks: templates.....	13
3.1 Assessment of security controls.....	13
Description and assessment of controls implemented for treating the risks related to data security.....	13
Description and assessment of general security controls.....	15
Description and assessment of organizational controls (governance).....	18
3.2 Risk assessment: potential privacy breaches.....	20
Analysis and assessment of risks.....	20
Assessment of the risks.....	20
4 Validation of the PIA: templates.....	21
4.1 Preparation of the material required for validation.....	21
Elaboration of the synthesis regarding compliance with [GDPR] of the controls selected to ensure compliance with the fundamental principle.....	21
Elaboration of the synthesis regarding compliance with good security practices of controls implemented for treating the risks related to data security.....	22
Mapping of risks related to data security.....	23
Elaboration of action plan.....	24
Documentation of the advice of the person in charge of "Data Protection" aspects.....	24
Documentation of the views of data subjects or their representatives.....	24
4.2 Formal validation of the PIA.....	25
Documentation of the validation.....	25

Please note: these templates may have to be adapted, and should be used as a complement to the guide "PIA, methodology".

CNIL 1

1 Study of the context: templates

1.1 Overview of the processing

Description of the processing under consideration

Description of the processing ¹	Clinical Trial Protocol
Processing purposes	id.
Processing stakes	id.
Controller	id.
Processor(s)	id.

Sector-specific standards applicable to the processing²

Standards applicable to the processing	Consideration
Clinical Trials Regulation	EU Legal Obligation
CNIL MR-001	France Legal Obligation

1.2 Data, processes and supporting assets

Data description, recipients and storage durations

Data types	Recipients	Storage duration
Clinical Trial Protocol	IT Policies	Clinical Trials Regulation
	Access Rights SOP	Records Mgt Policy

Description of the processes and supporting assets

[insert a diagram of data flows and a detailed description of the processes carried out]

Processes	Detailed description of the process	Data supporting assets
Clinical Trial Protocol		
Clinical Development Standard Operating Procedures		

2 Study of the fundamental principles: templates

2.1 Assessment of the controls guaranteeing the proportionality and necessity of the processing

Explanation and justification of purposes

Purposes	Legitimacy
Clinical Trial Protocol	Health Authority Authorization Ethics Committee Approval

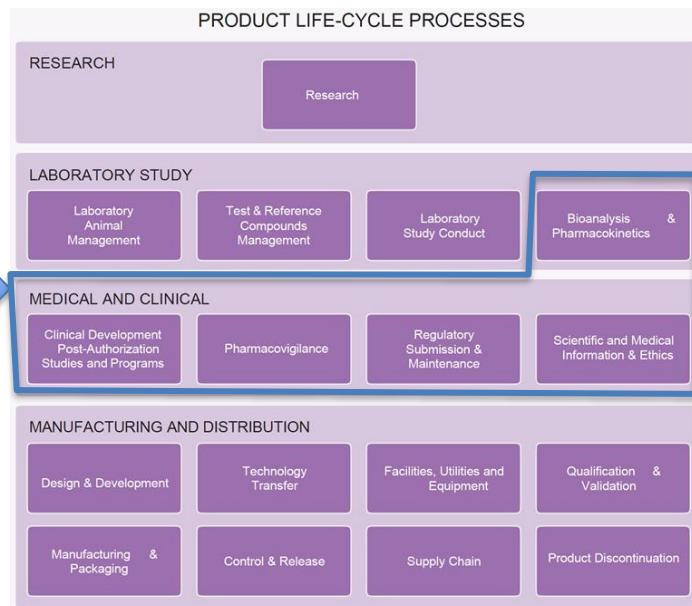
Explanation and justification of lawfulness

Lawfulness criteria	Applicable	Justification
The data subject has given consent ³ to the processing of his or her personal data for one or more specific purposes	✓	Data/Study Dependant
Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract		
Processing is necessary for compliance with a legal obligation to which the controller is subject	✓	
Processing is necessary in order to protect the vital interests of the data subject or of another natural person		
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller		
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child ⁴	✓	

LINKING PIA WITH QUALITY DOCUMENTS

PIA, templates		February 2018 edition
Contents		
Foreword		2
1 Study of the context: templates		4
1.1 Overview of the processing		4
Description of the processing under consideration		4
Sector-specific standards applicable to the processing		4
1.2 Data, processing and supporting assets		4
Data description, recipients and storage durations		4
Description of the processes and supporting assets		4
2 Study of the fundamental principles: templates		5
2.1 Assessment of the controls guaranteeing the proportionality and necessity of the processing		5
Explanation and justification of purposes		5
Explanation and justification of finalities		5
Explanation and justification of data minimization		6
Explanation and justification of data quality		6
Explanation and justification of storage durations		6
Assessment of the controls		6
2.2 Assessment of controls guaranteeing data subjects' rights		7
Determination and description of the controls for information for the data subjects		7
Determination and description of the controls for obtaining consent		8
Determination and description of the controls for the rights of access and to data portability		8
Determination and description of the controls for the rights to rectification and erasure		10
Determination and description of the controls for the rights to restriction of processing and to object		11
Determination and description of the controls applicable to processors		11
Determination and description of the controls on transfer of data outside the European Union		12
Assessment of the controls		12
3 Study of data security risks: templates		13
3.1 Assessment of security controls		13
Description and assessment of controls implemented for treating the risks related to data security		13
Description and assessment of general security controls		15
Description and assessment of organizational controls (governance)		18
3.2 Risk assessment: potential privacy breaches		20
Analysis and assessment of risks		20
Assessment of the risks		20
4 Validation of the PIA: templates		21
4.1 Preparation of the material required for validation		21
Elaboration of the synthesis regarding compliance with (GDPR) of the controls selected to ensure compliance with the Fundamental principles		22
Elaboration of the synthesis regarding compliance with good security practices of controls implemented for treating the risks related to data security		22
Mapping of risks related to data security		23
Elaboration of action plan		24
Documentation of the advice of the person in charge of "Data Protection" aspects		24
Documentation of the view of data subjects or their representatives		24
4.2 Formal validation of the PIA		25
Documentation of the validation		25

Please note: these templates may have to be adapted, and should be used as a complement to the standard "PIA methodology".



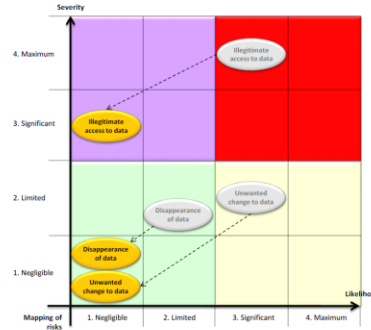


MEASURE RISKS & IMPROVE MITIGATION

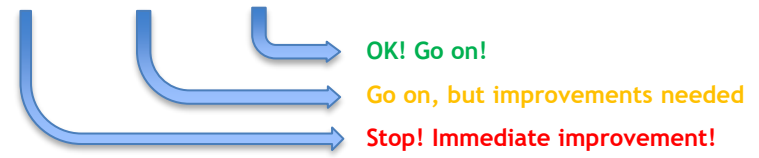
Elaboration of the synthesis regarding compliance with good security practices of controls implemented for treating the risks related to data security

Controls implemented for treating the risks related to data security	Assessment
Controls bearing specifically on the data being processed	
Encryption	○○●
Anonymization	○○●
Data partitioning (in relation to the rest of the information system)	○○●
Logical access control	○○●
Traceability (logging)	○○●
Integrity monitoring	○○●
Archiving	○○○
Paper document security	○○○
General security controls regarding the system in which the processing is carried out	
Operating security	○○●
Clamping down on malicious software	○○●
Managing workstations	○○●
Website security	○○●
Backups	○○●
Maintenance	○○○
Security of computer channels (networks)	○○●
Monitoring	○○●
Physical access control	○○○
Hardware security	○○●
Avoiding sources of risk	○○●
Protecting against non-human sources of risks	○○●
Organizational controls (governance)	
Organization	○○●
Policy (management of rules)	○○●
Risk management	○○●
Project management	○○○
Management of incidents and data breaches	○○●
Personnel management	○○○
Relations with third parties	●○○
Supervision	○○●

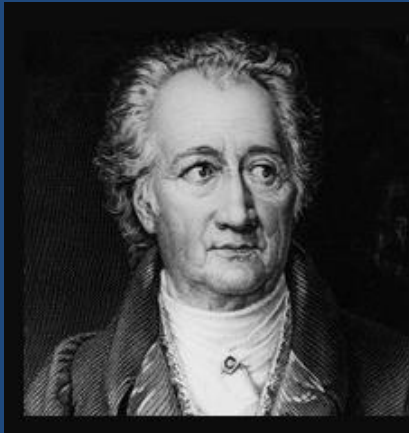
Mapping of risks related to data security



Caption
Symbol : ●●● ●○○ ○●○ ○○●
Meaning : Non applicable Unsatisfactory Planned improvement Acceptable



- Many challenges ahead in which the CDISC community
- has an important role to play!



Knowing is not enough; we must apply. Willing is not enough; we must do.

~ Johann Wolfgang von Goethe

Thank you for your attention!

pylastic@outlook.com (Information Management & Privacy in Life Sciences)

pierre-yves.lastic@udpo.eu (Privacy in France)

pierre-yves.lastic@efdpo.eu (Privacy in Europe & the World)



**EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS**