

The European Landscape of AI and Data Regulation

Life sciences conference
Penningtons Manches
November 14, 2024

DE GAULLE
FLEURANCE
AVOCATS
NOTAIRES

LEGAL STEP

TO CHANGE



Summary

1. Definition of AI

2. AI as applied to health

3. Panoramic slide on overall European legal landscape around AI and data

4. AI Act's main features & Focus on the healthcare sector

5. The French example of the human warranty in the use of AI

6. Data legislations: Data Governance Act, Data Act, EHDS including TEHDaS program, interaction with other data spaces

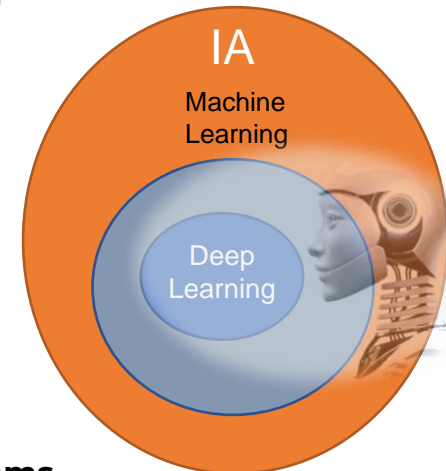
7. Focus on Secondary use of data

1. Definition of AI



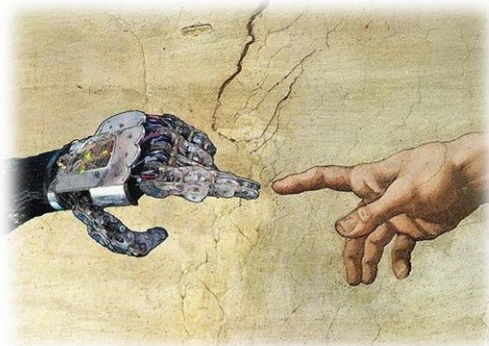
What is artificial intelligence?

- An old concept (1950s), after two "winters", a new and unprecedented boom thanks to the emergence of the availability of massive data (Big Data) and the acceleration in the speed of computing processors
- **Definition:** Science whose aim is to have a machine perform tasks that humans accomplish using their intelligence
- The academic table of AI fields identifies five:topics:
 - natural language processing
 - vision (or signal processing)
 - automatic learning
 - multi-agent systems
 - robotics
- One thing in common: AI is based on the use of algorithms



What is artificial intelligence?

- *AI not so intelligent?* AI applications are already ubiquitous in our daily lives but often remain "mono-tasking"
- **Weak AI** (or ANI, for *Artificial Narrow Intelligence*) versus **general or strong AI** (AGI, *Artificial General Intelligence*), capable of solving a variety of problems, like a human being... or even a **Super AI (ASI)** with capabilities superior to those of the human species (breaking point, "singularity", predicted by transhumanists)



In March 2016, **AlphaGo** (Google DeepMind) beat **Lee Sedol**, one of the world's best players → an AI victory that surpassed that of IBM's **Deep Blue** computer over world chess champion Garry Kasparov in 1997...



- Demystifying AI (as it is currently known) → 'automatic intelligence' or 'cognitive computing'

The technical, economic, ethical and societal challenges of AI

AI impacts the entire lifecycle of industrial products and services: R&D, manufacturing, installation, services, after-sales services, etc.

Examples of STRENGTHS

- **Improving R&D:** speeding up, new, more targeted applications, ...
- **Improved industrial quality and reliability:** e.g. fixing & enhancement action plans / customisation of products, ...
- **Supporting professionals:** enabling professionals to focus on "high added value tasks"
- **Flow management** for production and logistics centres...

Examples of WEAKNESSES

- Investment costs
- **Appropriation** of AI by professionals
- Other **HR impacts**
- **Lack of perspective** on the consequences of AI
- Data *sourcing* and qualification
- **Ethical issues**

Three major categories of players (1. data providers, 2. suppliers of AI technologies, products or services, 3. AI users) of varying size and degree of maturity, operating in a B2B and B2C universe

Objective: Find a new balance with the machine, between users, manufacturers, services providers and other AI players

2. AI as applied to health



Focus on the healthcare sector

AI impacts healthcare: diagnostics / care / training / patient care pathways

Examples of STRENGTHS

- Improvements in **medical research**: acceleration, new, more targeted therapies, etc.
- **Improved quality of care and patient management** : e.g., easier, more reliable diagnosis and prescription / personalized therapies
- **Support for healthcare professionals** : enabling them to refocus on “high value-added tasks”.
- **Flow management** for care centers (e.g. ER, procurement..)

Examples of WEAKNESSES

- Investment **costs for industry players, HC centers, public health authorities, etc.**
- Appropriation of AI** by healthcare professionals / liability risks
- Other **HR impacts**
- Lack of Rex** on the consequences of AI in healthcare in its current augmented capacity
- Sourcing** and **qualification of health data**
- **Ethical issues**

Ethical issues, risks and impacts for MD manufacturers

The patient's point of view

Personal data / Anonymization

Medical confidentiality vs. Scientific progress & open science

Prior consent vs. emergency situations?

Social fragmentation vs. a tool to compensate for lack of access to care

Repair vs. Transhumanism

Lack of human contact in the care process

The doctor's point of view

Blackboxes “ raise the question of the **physician's responsibility and autonomy** with regard to diagnostic/treatment decisions.

Implications for DM manufacturers' liability

To prevent doctors from becoming mere executors, **AI must be a tool, not a substitute** for humans

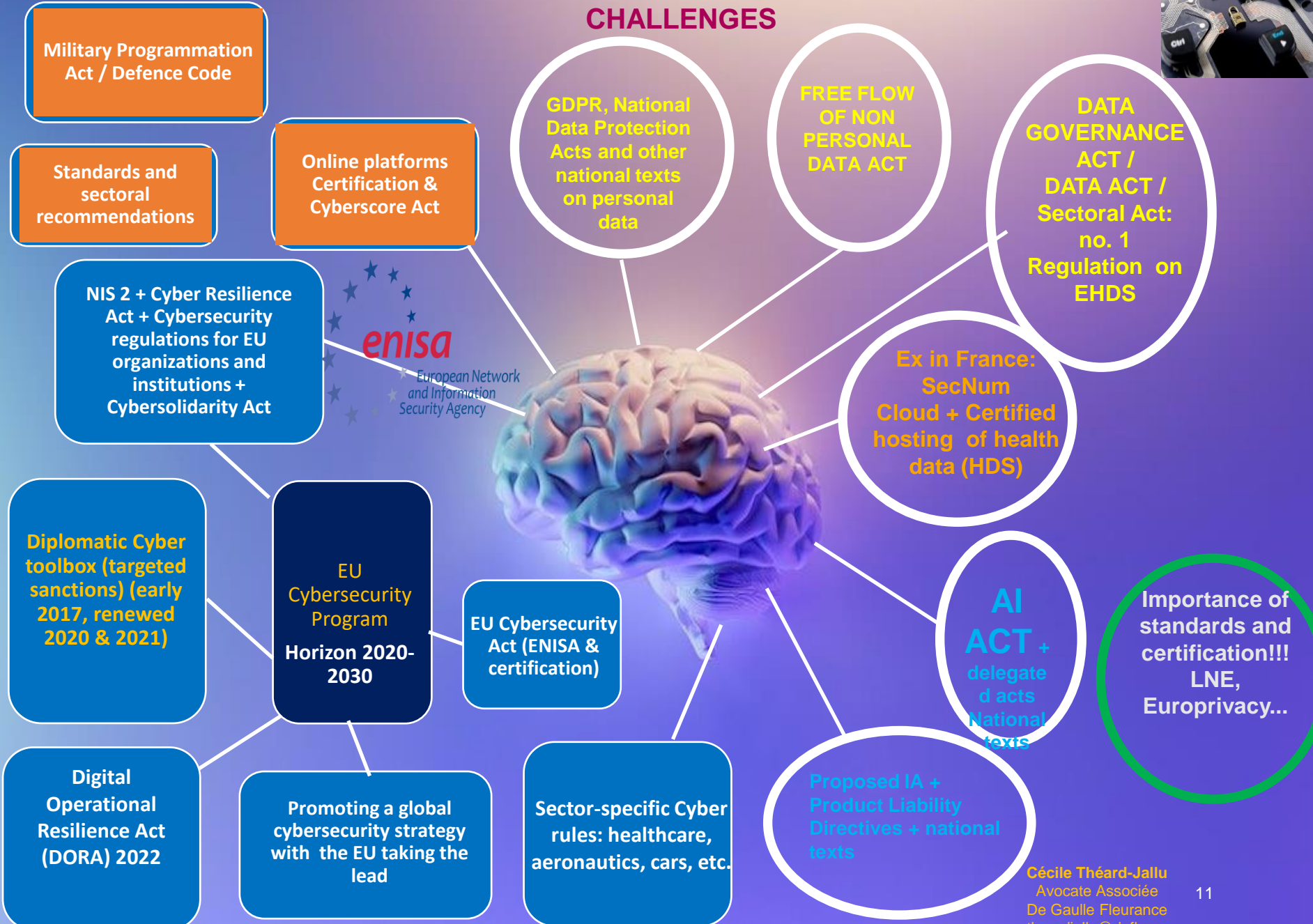
Need to understand the analysis process followed by AI:

- For validation of diagnosis/treatment by the physician (liability at stake)
- The patient must be informed of the use of AI (Code de la santé publique, Article L.1111-2 & R. 4127-35).
- Need to **control analysis steps and biases => from DM design and throughout its development & maintenance**

3. One panoramic slide on overall European legal landscape on AI and data



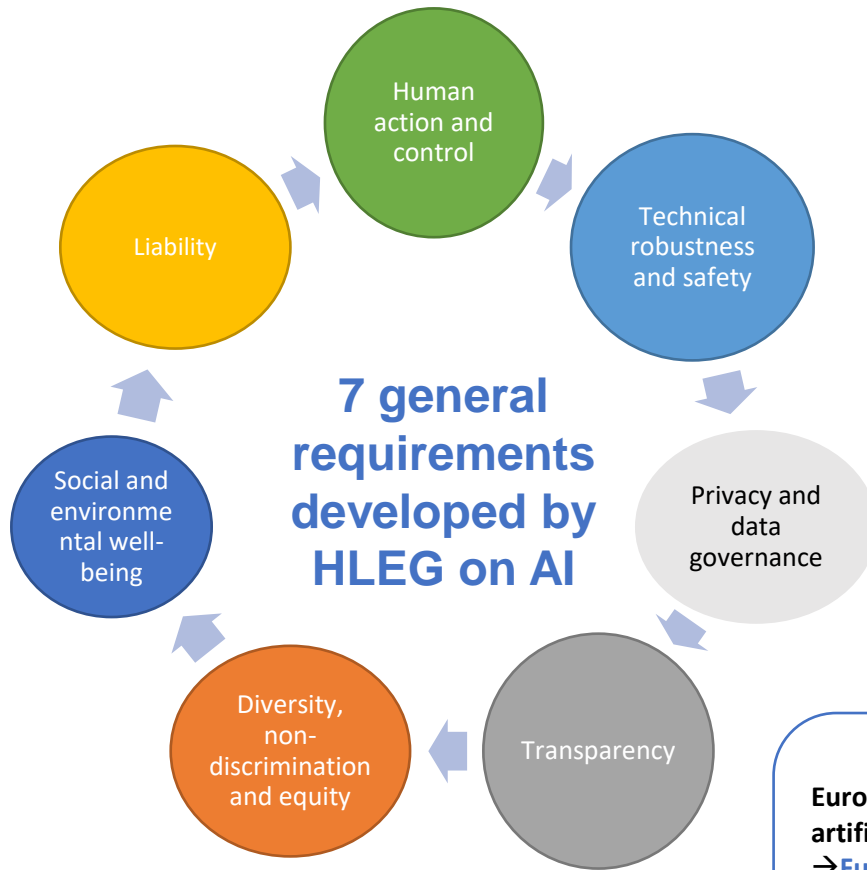
A LARGE SCOPE OF AI, DATA & CYBERSECURITY CHALLENGES



4. AI Act's main features



AI and ethics at European level



European guidelines for trustworthy AI (April 2019):

- Human autonomy and preservation of fundamental rights => **AI empowers people**
- AI developers should consider **technical and non-technical measures** to ensure implementation of these requirements
- The HLEG sees **healthcare as a key sector** in which AI can improve patient care and well-being, and optimize the work of healthcare professionals.

European Parliament resolution of January 20, 2021 on artificial intelligence :

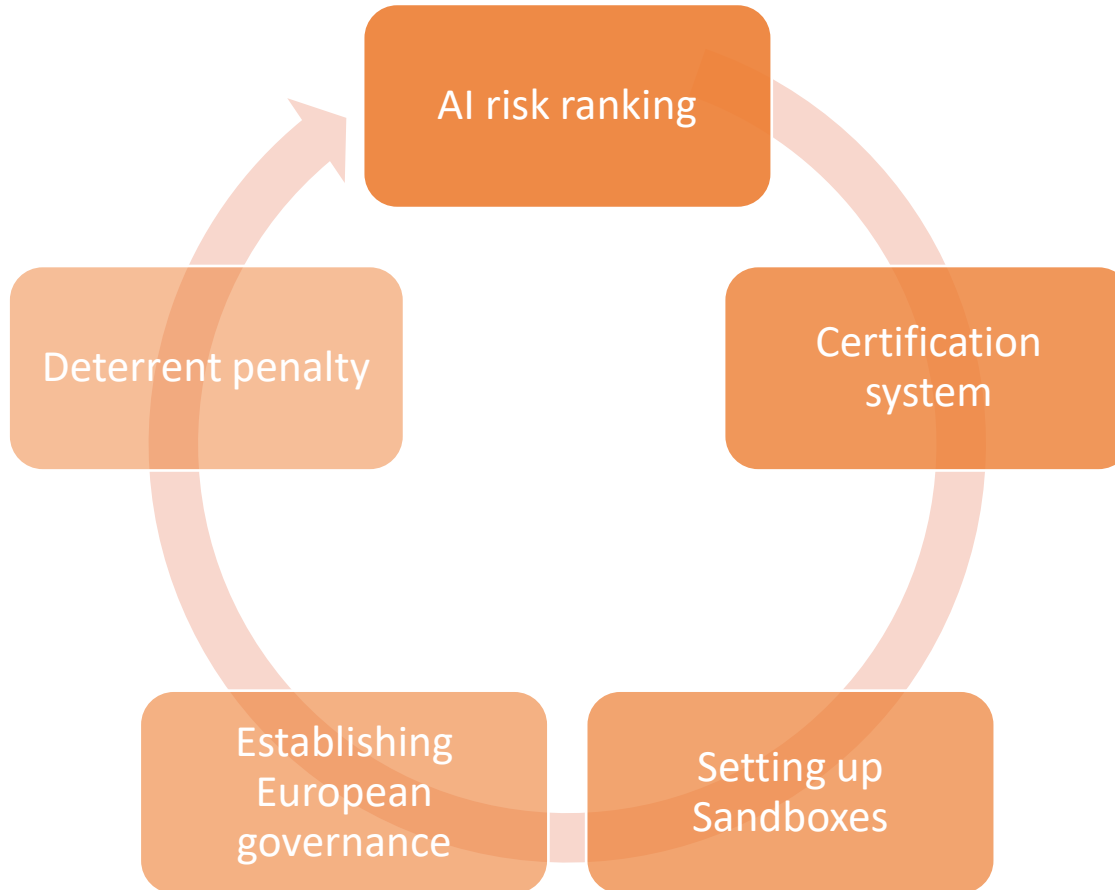
- **Fundamental rôle** that AI can play in the healthcare sector
- Call to **protect the patient** and leave room for the professional to deviate from the solution given by AI => AI remains a mere tool

“Artificial Intelligence Act”



November 2024 - De Gaulle Fleurance

“Artificial Intelligence Act”



Understanding the AI Act

A few regulatory definitions

AI: machine-based system designed to operate with different levels of autonomy, capable of adapting after deployment and which, for explicit or implicit purposes, deduces from the data it receives how to generate results such as predictions, content, decisions that can influence physical or virtual environments.

Developed using one or more of the following techniques: machine learning approaches, logic- and knowledge-based approaches, statistical approaches ...

Risk: the combination of the probability of occurrence of damage and the severity of that damage.

High-risk: Title II, Article 6

Recipients



Private and public players linked to AI systems. Free and open-source models are subject to restricted obligations.

Suppliers, established in the EU or in a third country, who market or commission AI systems **in the EU.**



Users of AI systems located in **the EU.**



Suppliers and users of AI systems located in a third country, when the **results generated by the system are used in the EU.**



The regulation **will not apply** to AI systems used **for military, defense or national security purposes, and during the research and innovation phase of AI systems except real-life testing.**

Objectifs



Preventing AI-related **risks** to health, safety and fundamental rights, while preserving democracy, the rule of law and the environment



Providing for obligations on AI system operators to mitigate the various types of risk



Harmonize the regulatory framework for AI at EU level to IA Act will be mandatory **24 months** after entry into force (but 6, 12 or 36 months for certain principles) - Codes of good practice: 9 months

Risk categories defined by the IA Act

Unacceptable risk → Prohibited

These AIs are **contrary to EU values** because they violate fundamental rights.

Ex: social rating, exploitation of people's vulnerabilities...

High risk → Authorized (subject to conditions)

These AIs have a **negative impact on people's safety** or fundamental rights (protected by the EU Charter of Fundamental Rights).

Specific transparency risks → Authorized (subject to conditions)

For certain AI systems, **specific transparency requirements** are imposed. (e.g. chatbots)

Minimal risk → Authorized without restriction

These AI systems can be developed and used in accordance with existing legislation, **without any additional legal obligations.**

+ Systemic risks associated with general-purpose AI models

Obligations under the AI Act

ACTIONS TO BE TAKEN BY OPERATORS

- **Transparency** (notify users that they are interacting with an AI, apply markings to deep fakes, etc.)
 - Respect for **copyright**
- Implementation of **regulatory compliance** (data protection impact analysis, collaboration with the AI Office, obligation to inform if content is generated by automated means...)

For systems at systemic risk

- Assessment of **energy efficiency**
- Implementation of **cybersecurity** measures
- Risk assessment and mitigation to **report serious incidents**

For high-risk AI systems

- **Conformity** assessment and **CE marking** (physical marking on products, digital marking on digital systems where possible)
 - **Quality** and **risk management**
 - **Registration on EU databases**
- Identification (and integration if technically possible) of measures to ensure **human control**

PENALTIES

Thresholds

- **35million euros or 7% of sales** for violations of prohibited AI practices
- **15million euros or 3% of sales** for breaches of other obligations under AI legislation
- **7.5 million euros or 1% of sales** for providing inaccurate information.

Sanctioning authority:

Competent national authority designated by each Member State

NB: For each category of infringement, the threshold will be the lower of the two amounts for SMEs and the higher of the two amounts for other companies.

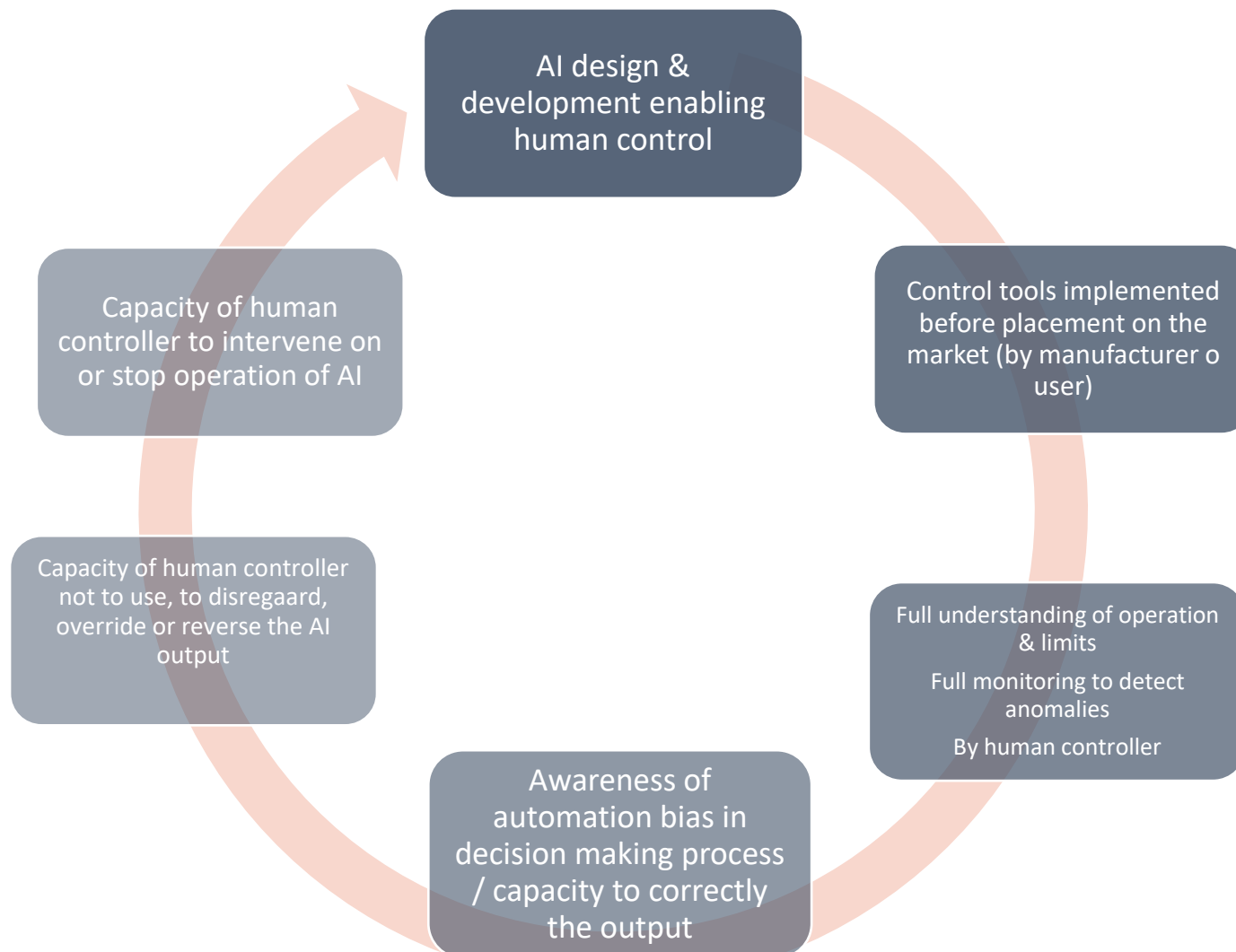
Actions to be taken under the IA Act

Proactive → AI action plan → Technical and organizational measures:

- Implementation of an IT compliance tool
- Audit of internal and external activities, risk analysis, impact analysis, compliance analysis, identification of sources of value (data sets, etc.).
- Review, design & evolution of contracts / documentation
- Risk management policies (including high-risk AI) / incident management
- Adaptation of insurance policies
- Training (GDPR intellectual property, liability risks, ethics, AI human guarantee...)
- Standardization & certification

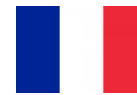
Defining a global AI strategy

« Artificial Intelligence Act » “Human oversight” – Article 14



November 2024 - De Gaulle Fleurance

Human guarantee for AI-enabled MDs



Human guarantee - **3 levels of supervision** must be implemented:

1. **Human-In-the-Loop (HIL)** : human intervention for each decision made by the AI tool
2. **Human-On-the-Loop (HOL)** : human intervention in AI tool design
3. **Human-In-Command (HIC)** : ability to supervise the overall activity of the AI system.

EU Guidelines

Practical measures for implementing the human guarantee:

- **Evaluate** the **level of involvement of AI systems** during diagnosis and treatment and ensure that (i) **patients** are **informed beforehand** and (ii) the **healthcare professional** is properly **trained** and is the one who **makes the final decision**.
- Promote the exercise of a **second human medical** eye at the request of a patient or healthcare professional (possibly through telemedicine).
- Implement **targeted and random verification procedures** to anticipate, manage and control the possibilities offered by AI tools with the creation of **independent internal and external control bodies**.
- **B-to-B and B-to-C impact, throughout the lifecycle of the AI-based product and the care pathway**



“Artificial Intelligence Act”

New rules for providers of high-risk AI systems

Step 1



A high-risk AI system is developed

Step 2



It needs to undergo the conformity assessment and comply with AI requirements
For some systems a notified body is involved

Step 3



Registration of stand-alone AI systems in an EU database

Step 4



A declaration of conformity needs to be signed and the AI system should bear the CE marking. The system can be placed on the market

If substantial changes happen in the AI system's lifecycle, go back to Step 2

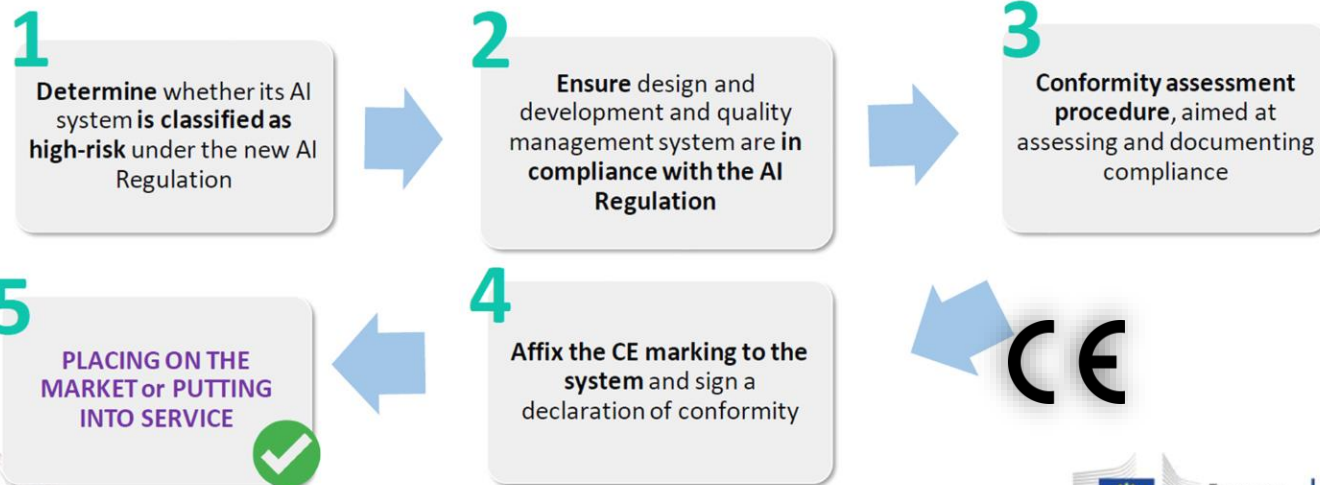
Source : <https://lestempsselectriques.net/index.php/2021/04/22/proposition-de-reglement-de-lia-de-la-commission-europeenne-entre-le-trop-et-le-trop-peu/>

“Artificial Intelligence Act”

Obligations concerning the design of high-risk AIs

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**:



Source : <https://www.ceps.eu/wp-content/uploads/2021/04/AI-Presentation-CEPS-Webinar-L.-Sioli-23.4.21.pdf>

Applicability of the

“Artificial Intelligence Act”

AI suppliers if they commission AI in the European Union

AI users located in the European Union

AI providers and users located in third countries who would use AI results in the EU



Cons. 28

• *In line with the aims of EU harmonization legislation to facilitate the free movement of products on the internal market and to ensure that only products that are safe and compliant in other respects are placed on the market, it is important to duly prevent and mitigate safety risks that may be associated with a product as a whole due to its digital components, including AI systems. **For example, increasingly autonomous robots, whether in the manufacturing industry or in personal care and support services, should be able to operate and perform their functions safely in complex environments. Similarly, in the healthcare sector, where the stakes for life and health are particularly high, increasingly sophisticated diagnostic systems and systems supporting human decisions should be reliable and accurate.***

Cons. 37

• *With regard to autonomous AI systems, i.e. high-risk AI systems (...), they should be classified as high-risk if, in view of their intended purpose, they present a high risk of causing harm to health.*

Cons. 45

• ***The European Common Data Spaces created by the Commission and the facilitation of public interest data sharing** between companies and with government will be key to providing reliable, accountable and non-discriminatory access to high-quality data for training, validating and testing AI systems. For example, **in healthcare, the European Health Data Space will facilitate non-discriminatory access to health data and the training of AI algorithms using these datasets, in a privacy-friendly, secure, fast, transparent and trustworthy manner, and with appropriate institutional governance.***



Art. 13

- The information [in the instructions for use in a digital format of high-risk AI systems] shall include (...) any known or foreseeable circumstances relating to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may result in **risks to health** and safety or to fundamental rights.

Art. 14

- The design and development of high-risk AI systems allow, in particular by means of appropriate human-machine interfaces, effective control by physical persons during the period of use of the AI system. Human control aims to prevent or minimize **risks to health**, safety or fundamental rights.

Art. 53

- Any **significant risk to health**, safety and fundamental rights identified during the development and testing [in AI regulatory sandboxes] of these systems will result in immediate mitigation measures and, failing that, suspension of the development and testing process until such mitigation is effective.

5. AI in health: the French example of the human warranty in the use of AI



AI and human guarantees in France



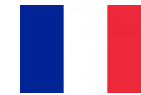
Comité consultatif national d'éthique (CCNE), opinion no. 130 of May 29, 2019:

Humans must remain the sole decision-makers

➤ 12 recommendations based on the following key questions:

- I. Ensuring the autonomy of humans and enabling them to make choices and appropriate decisions (**information, accessibility, training, periodic monitoring** of the effectiveness of existing legal tools for data protection, contours and feasibility of the requirement for individual consent)
- II. **Human guarantees** for the accountability of players + **the need for an independent supervisory authority**
- III. **AI training for healthcare professionals / ethics training for data professionals**
- IV. **the human-to-human link must prevail**
- V. Ensuring both individual freedom and solidarity
- VI. **promote the sharing of knowledge and data through the development of shared, interconnected national databases**

Human guarantee for AI-enabled DMs



Bill on bioethics, No. 2187, submitted on Wednesday 24 July 2019

- I. - When algorithmic processing of massive data is used for preventive, diagnostic or therapeutic acts, the healthcare professional who **communicates the results of these acts informs the person of this use and the methods of action of this processing.**

- II. – The adaptation of the parameters of a treatment mentioned in I for preventive, diagnostic or therapeutic actions concerning a person is **carried out with the intervention of a healthcare professional and may be modified by the latter.**
- Traceability** of the actions of a treatment mentioned in I and of the data used by it is ensured, and the resulting information is **accessible** to the healthcare professionals concerned.



Article L4001-3 of the French Public Health Code (in force)

- I.- Any healthcare professional who decides to use, for an act of prevention, diagnosis or treatment, a medical device incorporating algorithmic data processing learned from massive data **must ensure that the person concerned has been informed and, where appropriate, warned of the resulting interpretation.**
- II. -The healthcare professionals concerned are **informed of the use of this data processing.** The patient data used in this processing and the results obtained are **accessible** to them.
- III.- Designers of the algorithmic processing mentioned in I above **must ensure that users can understand how it works.**
- IV.- A decree issued by the Minister of Health, after consultation with the Haute Autorité de Santé and the Commission Nationale de l'Informatique et des Libertés, establishes the nature of the medical devices mentioned in I and their conditions of use.

Amendment no. 177 by M. Milon in the Senate on Feb. 3, 2021:

“II.- A human guarantee principle applies to algorithmic processing. The implementation of this principle is ensured in particular by the manufacturer under the conditions provided for in the context of the marketing of algorithmic processing.”



The bioethics law's obligation to provide information



- What emerges from L. 4001-3 of the CSP:
 - *Mainly information obligations*
 - *the text requires that the person concerned has “been informed and, where appropriate, warned of the resulting interpretation” (CSP, art. L. 4001-3, I)*
 - *“the healthcare professionals concerned are informed of the use of this data processing. Patient data used in this processing and the results obtained are accessible to them” (CSP, art. L. 4001-3, II)*

Data legislations: Data Governance Act, Data Act, EHDS including TEHDaS Program, interaction with other data spaces

A European Strategy for Data



The European data strategy of February 2020: a **single market** to ensure **Europe's competitiveness** on the international stage.

→ Creation of common European data spaces in key sectors. In total, 15 are planned :

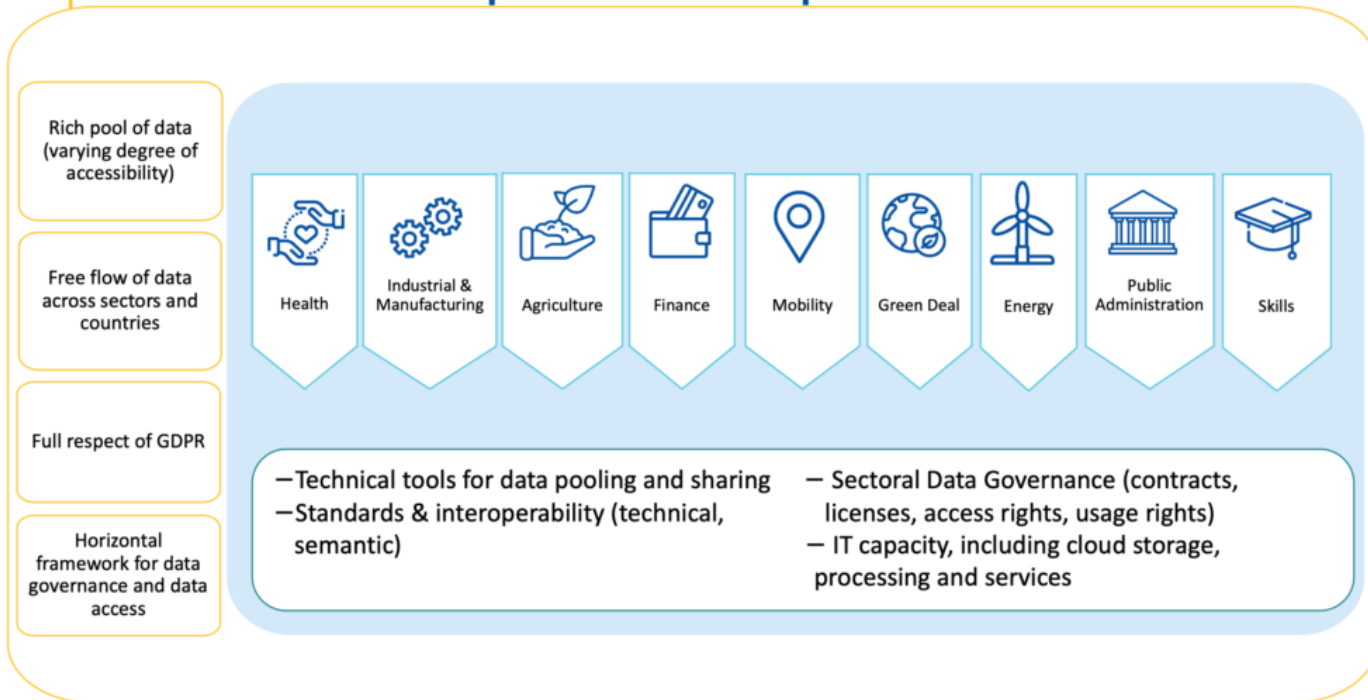


And more...
spaces

<https://digital-strategy.ec.europa.eu/en/policies/data-spaces>

A European strategy for data

Common European data spaces



Source : Europa

' Today we are defining a truly European approach to data-sharing. Europe needs **an open but sovereign single market for data**. Our regulation, coupled with the right investments and key infrastructure, will help Europe lead the world in data. ' Thierry Breton – EU Commissioner for Internal Market

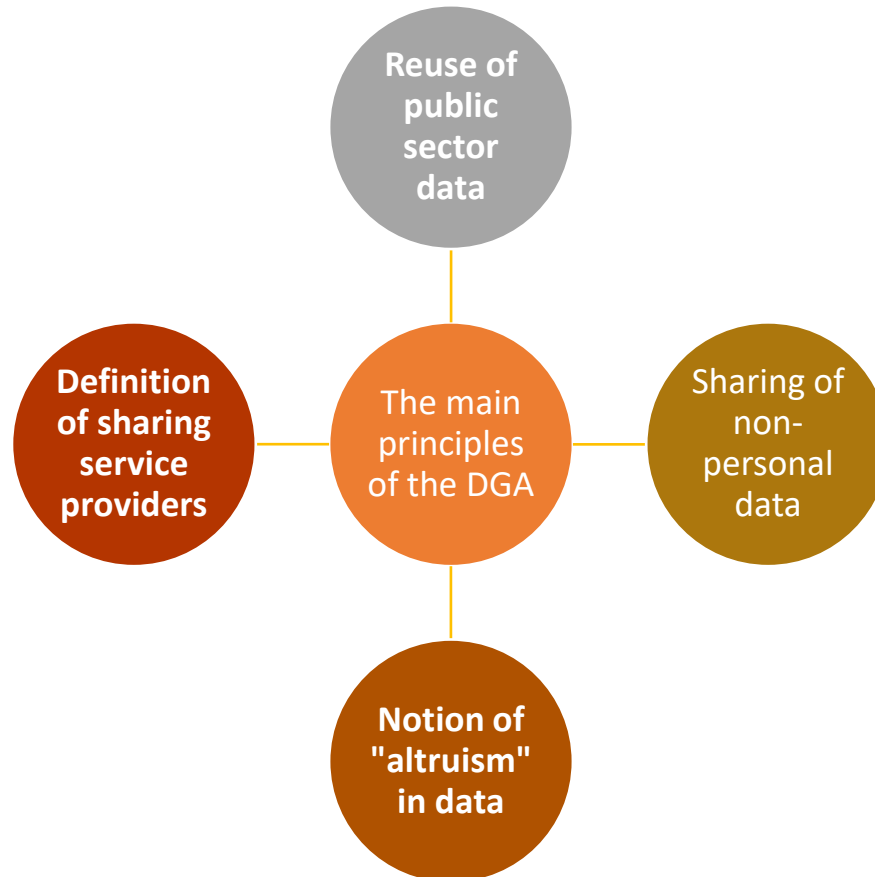


Data Governance Act (DGA)

Regulation (EU) 2022/868 of May 30, 2022 – Effective: September 24, 2023

- **Chapter III DGA:** Requirements applicable to data intermediation services
- **Data Intermediation Services (DIS):** Services aimed at establishing commercial relationships for data sharing among an indefinite number of data holders and users using technical, legal, or other means (see DGA rec. 28)
- **Context :**
 - Data intermediation services will play a **key role in the European data economy**
 - The EU plans to create several European data spaces
 - Bilateral or multilateral data sharing on a common platform, effective pooling of data.
 - Objective: **To create new data-centric ecosystems** independent of existing actors, enabling nondiscriminatory access to the data economy for SMEs, startups, etc.
 - Use Cases: Development of new products/services, scientific research, civil society initiatives.
- **The DGA will encourage the interconnection between European data spaces:**
 - Considering (2): "The tool is inspired by the principles of management and reuse of data developed for research data. The FAIR data principles state that data should be **Findable, Accessible, Interoperable, and Reusable in principle.**"
 - Article 27: "The committee performs the following tasks: [...] (d) **assist the Commission in improving data interoperability** as well as data sharing services across different sectors and domains by leveraging existing European, international, or national standards."
- **Applies to:**
 - ❖ *Public sector bodies (but not public enterprises)*
 - ❖ *Data intermediaries (neutral third parties facilitating the negotiation of data flow between the data source and data users who may be individuals or businesses)*
 - ❖ *Organizations recognized as altruistic in terms of data (i.e., persons or companies voluntarily and freely making their data available for use in the public interest)*

DGA: main topics



DGA: Notion of “altruism” when it comes to data



Data altruism: the provision of personal data voluntarily by data subjects with their consent, or of non-personal data by legal entities.

→ is aimed at the re-use of data for purposes of general interest, defined as including healthcare, the fight against climate change, improved mobility, but also support for scientific research and technological development, including those financed by private funds.


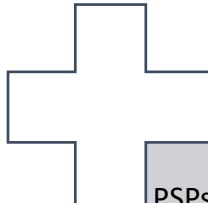
Registration as “altruistic data organization recognized in the Union”.

Not for profit

High transparency requirements

Safeguards to protect the rights and interests of data subjects and companies

Effective technical means for withdrawing or modifying consent and providing information on data use



PSPs facilitate the aggregation and exchange of large quantities of relevant data, via commercial, legal and technical matchmaking services.

Type of PSP: data cooperatives

PSPs may only act as intermediaries in transactions, and may not use the data exchanged for any other purpose.

The following cannot be PSPs:

- cloud service providers
- data brokers or advertising agencies
- data consulting firms

Data Act (DA)

Regulation (EU) 2023/2854 of December 13, 2023 – Effective January 11, 2024

Objectives

- ❑ Address the challenges and unlock the opportunities offered by data in the EU
- ❑ Focus on equitable access, user rights, and the protection of personal data
- ❑ Address the following obstacles:
 - ↳ **Lack of clarity regarding** the use and access to data from connected products
 - ↳ **Difficulties for SMEs** to negotiate balanced data-sharing agreements with more powerful market players
 - ↳ **Obstacles to transitioning to competitive and trustworthy cloud (Cloud) or edge (Edge) services** in the EU
 - ↳ **Limited ability to combine data** from different sectors

Means

- ❑ Implement **safeguards against illegal data transfer**
- ❑ **Facilitate B2B and B2C data sharing**
- ❑ **interoperability standards for data reuse** across sectors
- ❑ **Ease the transition between cloud and edge services**
- ❑ Enable public sector organizations and EU institutions **to use data held by companies in cases of exceptional data need**

The DA will also **encourage the interconnection** between European data spaces:

- “**Plan the development of interoperability standards** for data intended for **reuse across sectors**, with the aim of removing barriers to data sharing between common European data spaces specific to certain domains, in accordance with sector-specific interoperability requirements, and between other data not part of a specific common European data space.”
- Article 2 (19): ““Interoperability,” the ability of at least two data spaces or communication networks, systems, products, applications, or components to exchange and use data in order to perform their functions.”

- **1. Strengthening users' rights**
 - Obligation for data holders to make the data generated by them on users available to users free of charge
- **2. New data sharing requirements from companies to governments**
 - In certain exceptional circumstances (e.g.: a health crisis or natural disaster) companies may be required to share their data with public institutions, including governments, free of charge
 - Compensation may be requested by the data holder if it is requested in a preventive manner
- **3. Supporting SMEs in B2B data transfers**
 - EU Commission's target: unfair contractual clauses, i.e., those imposed unilaterally on an SME by a more powerful party in a data sharing contract between companies
- **4. Easier switching between cloud and edge services**
 - Minimum rules to enable switching between cloud and edge services
 - new contractual, commercial and technical requirements
 - Obligation to set various measures to prevent governments outside the EU from illegally accessing data stored in EU clouds
- **5. A horizontal basis for future data spaces**
 - Sectoral acts destined to supplement the Data Act
 - Beginning by the health data space, due to be presented in April 2022?

European Health Data Space (EHDS)



Regulation adopted on **April 24, 2024**

- Will enter into force **20 days** after its publication in the Official Journal of the European Union (expected in the autumn)
- Implementation within a timeframe of **2 to 8 years**



OBJECTIVES

- Help individuals take control of their own health data
- Support the use of health data to improve care, research, innovation, and the development of health policies
- Enable the EU to fully exploit the potential offered by a safe and secure exchange, use, and reuse of health data within the EU

MAIN PROVISIONS

- The proposal is subject to the **GDPR** and the EU Data Protection Regulation by EU institutions, organs, and agencies (**EUDPR**).
- Developments on the **rights of individuals concerned** with the use and reuse of health data.
- Implementation of a European platform '**MyHealth@EU**' (primary use) and '**Healthdata@EU**' (secondary use).
- Dedicated framework for the **processing of health data for the two described uses** (primary and secondary).

Article 42: 'Organizations responsible for access to health data and holders of unique data may receive royalties for making electronic health data available for secondary use purposes.'

The provided text distinguishes two types of data usage:

- (1) Primary use of electronic health data:** *"The processing of electronic health data of a personal nature for the provision of health services aimed at assessing, maintaining, or restoring the health status of the physical person to whom these data relate, including the prescription, dispensing, and provision of medications and medical devices, as well as for relevant social security, administrative, or reimbursement services."*
- (2) Secondary use of electronic health data:** *"The processing of electronic health data for the purposes stated in Chapter IV of this regulation. The data used may include electronic health data of a personal nature initially collected within the framework of a primary use, but also electronic health data collected for the purposes of secondary use."*

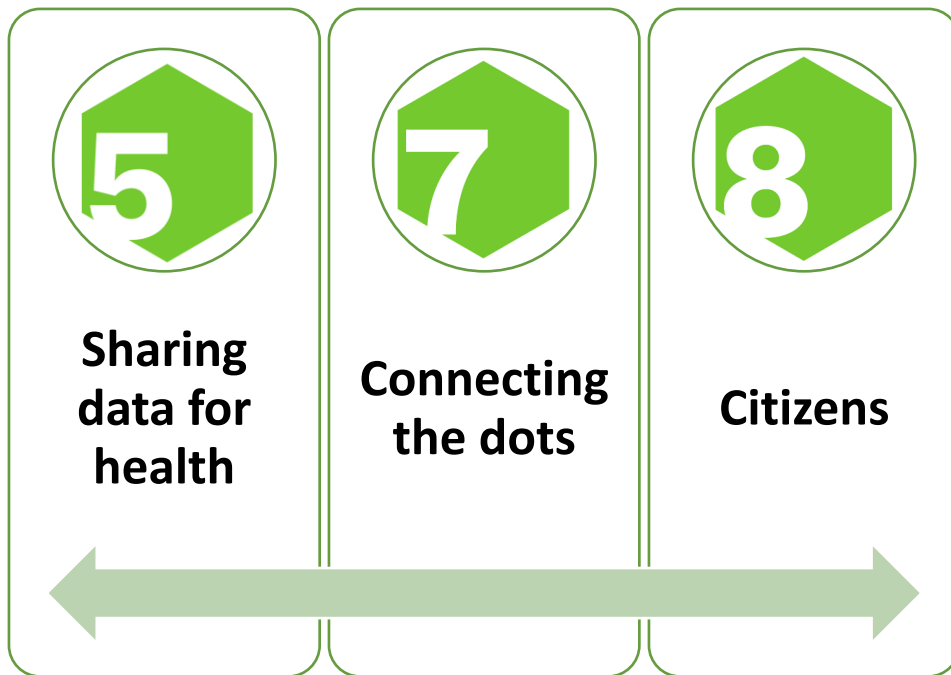


- **Why?**
 - To regulate the reuse of health data for purposes other than initial care
 - Value of this activity according to the EU Commission:
 - €25 billion today
 - Expected €50 billion in 2032
- **What to expect about the coming EU Health Data Space Act?**
 - First sectoral Act combined with DGA + DA
 - Requirements of cross frontier interoperability and pan European infrastructure
 - **Improve efficiency in care and scientific research => “Free the health data market”**
 - Individuals’ rights on ‘primary’ use
 - **Individuals should have the right to access a minimum set of ‘primary’ health data**, including vaccination, electronic prescriptions, images, laboratory results, discharge reports, and others – using a free of charge access service
 - Individuals will also have the right to restrict access to such data or share it with third parties free of charge
 - ‘Secondary use’ for personalized medicines
 - **Secondary use** includes health records, social data, administrative data, genetic and genomic data, public registries, clinical studies, research questionnaires, and biomedical data such as biobanks
- The list of **allowed uses** includes informing regulatory decisions and supporting public authorities in carrying out their tasks, as well as in education, scientific research, developing innovative solutions for public interests, and training algorithms with medical applications
- Some purposes to be explicitly **forbidden**, such as informing decisions against individuals with legal effects, including insurance premiums, commercial advertising, and selling data to third parties
- **What’s next?**
 - Several articles yet to be specified through secondary acts (delegated or implementing acts)
 - Establishment of a *“European Digital and Health Data Committee”*

Source:

<https://www.euractiv.fr/section/economie/news/leak-lespace-europeen-des-donnees-de-sante-pour-liberer-les-donnees-de-sante/>

TEHDaS Packages concerning the reuse of health data



5. Develops options for **governance models** for the exchange and **secondary use of health data** between European countries, based on transparency, trust, citizen empowerment and a common good. Provides recommendations for European countries on **planning national legislation to enable cross-border** exchange and secondary use of health data.

7. Provides options for the **technical interoperability** of the **secondary use of health data** in the European Health Data Space. Encourages the participation of future users of the European Health Data Space, such as researchers and policymakers, and of the technical implementers, such as companies and institutions, in co-designing the services.

8. Seeks to obtain a **better understanding of citizens' attitudes** towards sharing their health data. Identifies ways to inform people about the use of their health data and raise awareness of the benefits that the **secondary use of data** offers.

Focus on Secondary use of data

Secondary use in industrial contracts: some food for thoughts



Questions about the combination between secondary use and GDPR, specifically:



- 1 In which cases does GDPR apply to data sharing and reuse projects? What about national law?
- 2 Who are the parties involved in these projects? What is the role distribution? For what purposes?
- 3 Who is responsible for ensuring compliance with GDPR? At what level?
- 4 What guarantees should be put in place to ensure this compliance with GDPR?
- 5 How are rights and contractual obligations translated, and what procedures of control *ex ante* and *ex post*? (Add contractual specifications)
- 6 Under what economic model?
- 7 How to continue to protect and enhance investments including intellectual property (IP)?
- 8 What role does cross-border certification play?
- 9 How to ensure flexibility and comprehensive coverage while structuring contracts (contract engineering)?

November 2024 - De Gaulle Fleurance

A prerequisite: the verification of legality

CNIL • CNIL File, April 8, 2024

The example of the DPIA: Ensure that the processing is lawful - In the case of data reuse, perform the necessary tests and checks.

Reusing health data requires, first and foremost, verifying the **lawfulness of the processing** in light of current law, notably the GDPR.

Example: A data controller might want to reuse data they collected for an original purpose (e.g., providing a service to individuals) in order to create a database for the purposes of training an AI system.

→ **COMPATIBILITY TEST** with the initial purpose ONLY IF the processing does not rely on the consent of the data subject (or EU or national law).

→ **NO COMPATIBILITY TEST** if secondary purposes are planned and made known to the data subjects at the time of collection and transparently, or for scientific research if it respects rights and guarantees (e.g., anonymization) (Article 89 GDPR), or for statistical purposes

PUBLIC DATABASE

- Control by the data controller of the lawful nature of the publication
- The data controller must ensure the lawfulness of the content (e.g., non-compliance with GDPR: Article 5.1.a + crime of concealing an offense under Article 321-1 of the Penal Code).

Recommendations to re-users => to be reflected in the contract in the form of guarantees:

- ✓ Mention the **source of the database in addition to its description.**
- ✓ The creation/distribution of the database must not obviously result from a **crime or misdemeanor, nor have been subject to a conviction or public sanction.**
- ✓ There must be **no clear doubt** about the **lawfulness** of the database (ensure that the collection conditions are sufficiently documented).
- ✓ **Check whether or not the database contains sensitive personal data** (including health data); if yes, it is clearly not usable.

DATABASE ACQUIRED FROM A THIRD PARTY (brokers...)

- (1) For the third party sharing personal data:**
- **Ensure the lawfulness of the transmission**

Case 1: Data collected to be shared for the purpose of creating a database for AI training

= The third party must ensure **the compliance of the data transmission process for which they are responsible.**

Case 2: The third party did not originally collect the data for this purpose

= The third party must ensure that the data transmission pursues a compatible purpose = **COMPATIBILITY TEST**

- (2) For the re-user:**

→ **A series of verifications of the initial data controller's processes**



Recommendation : Recommendation: Conclusion of an agreement between the initial data holder and the re-user to allow the latter to ensure the legality of their own processing. For this, the CNIL recommends indicating in the contract:

- ✓ **The source, the context, the legal basis, and the impact assessment**
- ✓ **The information provided to the individuals Les garanties**
- ✓ **The guarantees**

Consent or compatibility test

Why ?

- **Analysis** of large quantities of data
- Discovery of **patterns** and **trends**
- **Prediction** and **decision making**



Examples

- **Epidemiology:** data analysis, early epidemic detection, tracking of spread...
- **Improvement of care**
- **Research & development & innovation**

BEST PRACTICES

COMPATIBILITY TEST

- ✓ **Link between the initial purpose and the subsequent processing purpose**
- ✓ **Context** in which data was collected
- ✓ **Type and nature** of the data (sensitivity)
- ✓ Possible **consequences** of the subsequent processing
- ✓ Existence of appropriate **safeguards** (encryption, pseudonymization)

CNIL. "CNIL IA sheet"

1. **Define the purpose of the processing** (collect new consent if necessary)
2. **Qualify the roles of the actors** (data controller...)
3. **Ensure the legality of the processing** (appropriate legal basis, explicit and granular consent from patients, legitimate interest of the data controller)
4. **Conduct a Data Protection Impact Assessment (DPIA)**
5. **Data protection** (minimization, anonymization, pseudonymization...)
6. **Selection and management of data** (process only relevant data)
7. **No open data for health data** (public database)

Guidelines – Reuse of Health Data January 2022

CNIL.

Data Processor

- **Definition.** The Data Processor processes personal data on behalf of the Data Controller
- **Role.** The Data Processor follows the instructions of the Data Controller and cannot, in principle, use the data for its own purposes (GDPR) / must delete or return them at the request of the Data Controller.

CONDITIONS

1 Written authorization from the data controller

- ✓ **Compatibility test:**
 1. Check if the reuse is compatible with the initial purpose of the collection
 2. Consider the relationships between the parties, the type of data, and the potential consequences for the data subjects
- ✓ Implement **safeguards**, such as anonymization
- ✓ **No prior and general authorization**

2 The processor becomes the data controller of the reused data

- ✓ Ensures compliance of the processing with the **GDPR**
- ✓ Ensures the purpose of the processing and its **legal basis**
- ✓ Provides the concerned individuals with **all information** on the indirect collection of data
- ✓ Defines an appropriate **data retention period**
- ✓ Collects only the data necessary to meet the initially set purpose (**minimization**)
- ✓ Allows the concerned individuals to **exercise their rights**
- ✓ Implements all necessary **security measures**




Best Practices


- ✓ Compliance with **confidentiality standards (GDPR)**
- ✓ **Explicit consent** (anticipated during collection)
- ✓ **Data Protection Impact Assessment (DPIA)**
- ✓ **Anonymization** of health data as much as possible
- ✓ **Transparency and accountability**




CNIL. Reuse of personal data (Guidelines 01/22)

 **Controller must conduct a "compatibility test" before granting approval as per art. 6(4)**


- Controller must determine whether such further processing is compatible with the initial purpose
- If test not satisfied, Controller must refuse the re-use of the data. If test satisfied, Controller is free to give or withhold consent

 **Controller must inform data subjects**


- In particular, whether it is possible to object
- If Processor already holds the contact data of the data subjects, original Controller may delegate this action to Processor for the targeted secondary processing

 **No prior and general authorization**


- The "compatibility test" must be carried out for a specific processing operation, taking into account the purposes and characteristics of each processing operation for which Processor wishes to re-use the data.

 **Processor, as the new Controller, must ensure compliance of the processing**

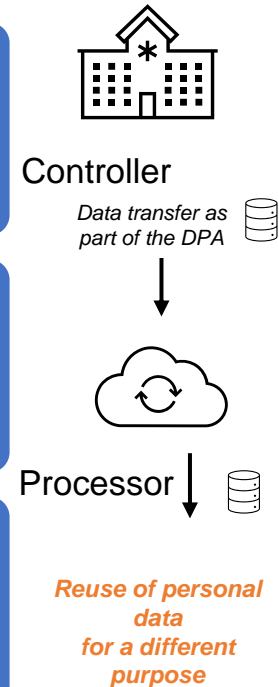
- By reusing data, Processor of original data controller becomes responsible for the secondary processing
- As the new Controller, must also ensure that the further processing serves a well-defined purpose

 **Authorization shall be in writing**

- Original controller's authorization must be in writing, including possibly in electronic format
- Oral form is not compliant with GDPR

 **In particular, Processor must:**

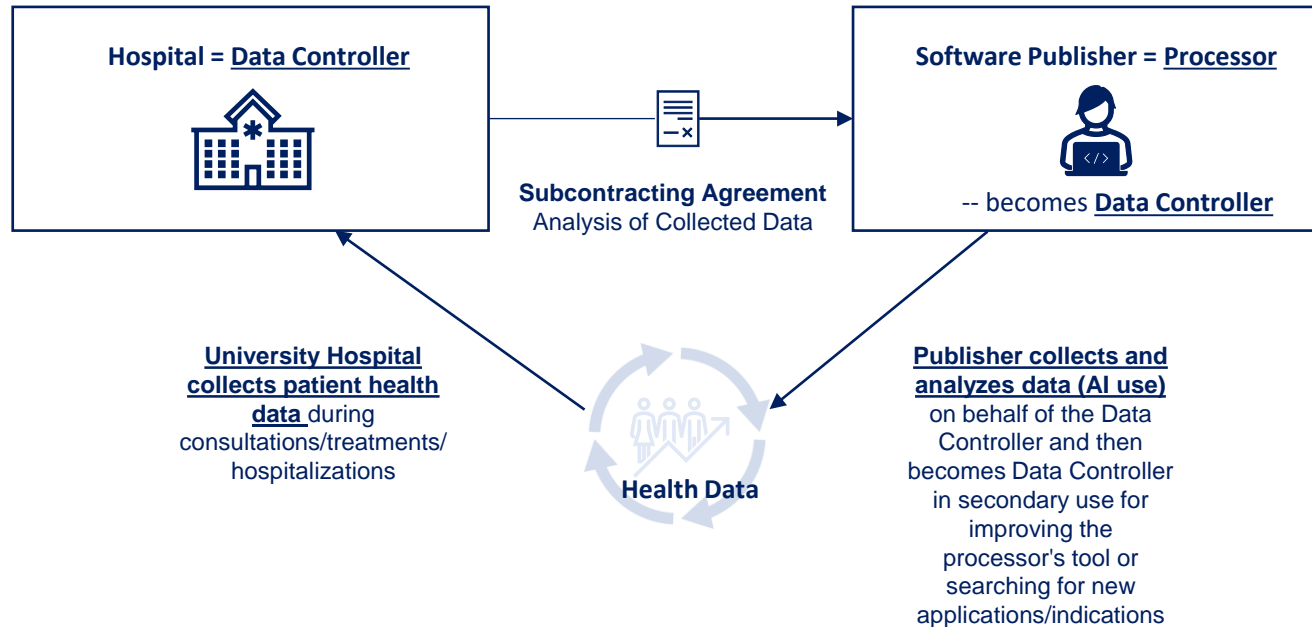
- provide data subjects, with applicable exceptions, with information about the indirect collection when not already provided by original data controller
- define an appropriate data retention period
- Ensure minimization



Use case

Use case 1.

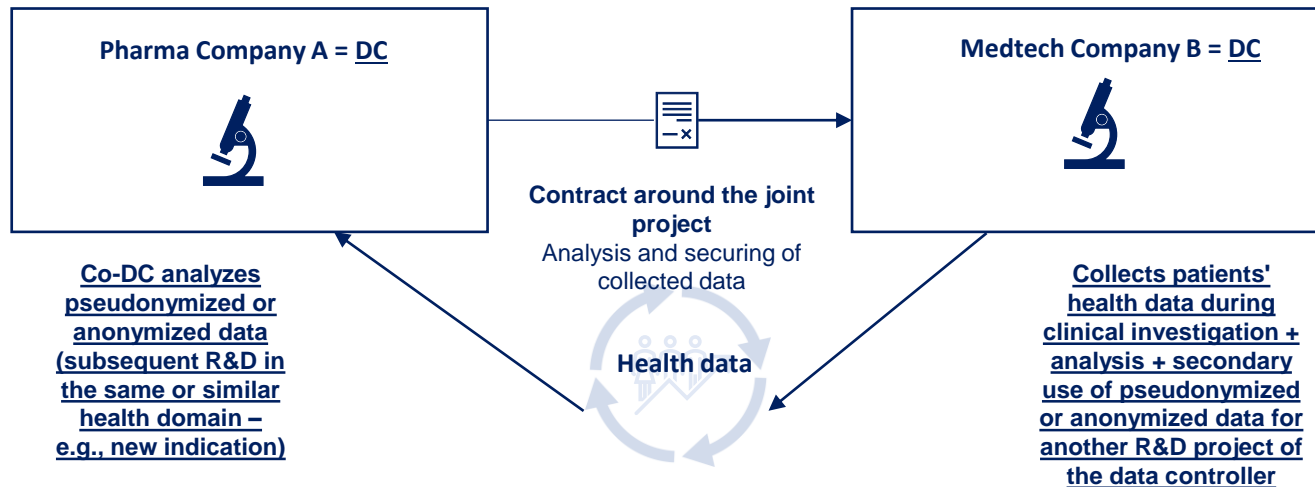
A hospital (DC) collaborates with a software publisher (P) for the management of health data. In the context of secondary use, the publisher becomes the DC as it uses the data for its own purposes, such as research and development.



Use case

Use case 2.

Two companies (e.g., pharma and medtech) collaborate to develop a new drug delivery technology. Medtech is the promoter of clinical investigation generating data, but with an RCT agreement. Then, secondary use for the specific purposes of each party (e.g., R&D vs. statistics).



- ✓ Respect for **confidentiality standards** (GDPR)
- ✓ **Explicit patient consent**: the RCT promoter must inform patients of the new purpose of the processing
- ✓ Data Protection **Impact Assessment (DPIA)**
- ✓ **Pseudonymization** or better anonymization of patient data to minimize re-identification risks
- ✓ **Transparency** towards patients regarding the use of their data
- ✓ **Implement appropriate security measures** to protect data against any cyberattacks/unlawful access
- ✓ Etc.



Cécile Théard-Jallu
Partner



Co-Chair of the Healthcare and Life Science Law Committee of the International Bar Association
Co-Chair of the IBA Annual World Life Sciences Conference



Leading individual in Legal 500 EMEA 2024 in Industry focus: Healthcare and life sciences and Data Privacy



Biography

Cécile Théard-Jallu specializes in commercial law & contracts, healthcare regulations, innovative technologies, data protection and database projects as well as intellectual property. She has developed a strong experience acting for both international groups and SMEs, particularly in the fields of health & life sciences, agrifood, insurance, mobility and digital technologies. She is also active for actors in the New Space industry.

She helps clients through the definition and implementation of their innovation strategies with a particular focus on regulations relating to healthcare products and activities (including research, development, market access, marketing, promotion, manufacturing, vigilance and end of life of drugs, medical devices & cosmetics, telemedicine/telecare, protection and valuation of health data -including secondary use deals-, digital twins, 3D printing, IoT, platforms, social robots, artificial intelligence, web3 & metaverse, VR, blockchain, 5G/6G, smart healthy cities, and connected mobility around the patient pathway...).

She works on complex contractual operations, including R&D, clinical research and consortia, technology transfers, licensing, or technological mutation projects, with or without public funding. Furthermore, she advises clients on the engineering, design, negotiation and implementation of their commercial, computer, technological or industrial contracts.

As a data protection specialist, Cécile Théard-Jallu is certified with Europrivacy -a GDPR compliance certification program endorsed by the European Commission in October 2022- and has been helping clients implement this program in France and at an international level. Selected as an expert for France for the European project TEHDAS 1 aimed at building the regulation of the future European Health Data Space, she

helps private and public actors implement the GDPR, the French Data Protection Act, related guidelines as well as the European legal arsenal governing the digital market (Data Governance Act, Data Act, European Health Data Space Act, IA Act, etc.).

Co-chair of the Healthcare & Life Sciences Law Committee and member of the Technology Law Committee of the International Bar Association (IBA), she also cochairs the IBA Annual World Life Sciences Conference, which has celebrated its 10th anniversary in 2024.

She has recently started developing the Firm's practice in the New Space / Space Tech domain, including for healthcare and agri-food actors, representing the Firm as a member of Space Cooperative Europe, i.e. the European Space Agency (ESA)'s accelerator for agrifood SMEs as well as co-leading the legal group of ESA's new working program on the future European Space Data Space.

She teaches data law and AI law as part of the "DU AI & Health" and "DU Generative AI & Health" diplomas of the University of Burgundy.

In addition to the Paris Bar, Cécile Théard-Jallu holds a Master 2 "DESS" diploma in Business Law and a D.J.C.E. (Business Counsel Training) diploma from the Universities of Cergy-Pontoise and Montpellier, 1995.

Listed in Best Lawyers 2024 in:

- Biotechnology and Life Sciences
- Information Technology Law
- Outsourcing



Ranked Lawyer in Chambers Europe 2024 in Pharma/Life Sciences / Regulatory



Thank you for your attention



Cécile Théard-Jallu
Partner
De Gaulle Fleurance
+33 6 07 26 93 43
ctheardjallu@dgfla.com

9, rue Boissy d'Anglès, 75008 Paris - France | Tél. : +33 (0)1 56 64 00 00 Fax: +33 (0)1 56 64 00 01

contact@dgfla.com - www.degaullefleurance.com

De Gaulle Fleurance & Associés - SAS au capital de 40 000 euros - RCS Paris 439 534 835 - Toque K 35
Confidentiel / Privileged and confidential - N° TVA intracommunautaire FR00439534835

**DE GAULLE
FLEURANCE**

**AVOCATS
NOTAIRES**

LEGAL STEP

TO CHANGE