AI.4.educators

AI.4.educators
Educating Educators on Artificial Intelligence (AI) – development of an AI training material and an AI educational program for educators

Project No: 2021-1-EL01-KA210-ADU-000034976

AI Legal Roadmap

Co-funded by the European Union

Table of Contents

Introduction to AI Legal Roadmap

The AI Legal Roadmap contains some basic information in the context of regulating AI in EU level.

The roadmap aims to present:

a) The EU's strategy in the field of AI
b) The legislative initiatives taken in order to regulate specifically the AI Sector in EU level and the Risk Based Approach that EU has adopted
c) The general EU's legal framework that affects (directly or indirectly) the AI systems, focusing on the Data Protection Legislation (GDPR)
d) Case studies of AI incidents and the legal issues arising

Key discussions and policy initiatives on EU level- The EU's strategy in the field of AI

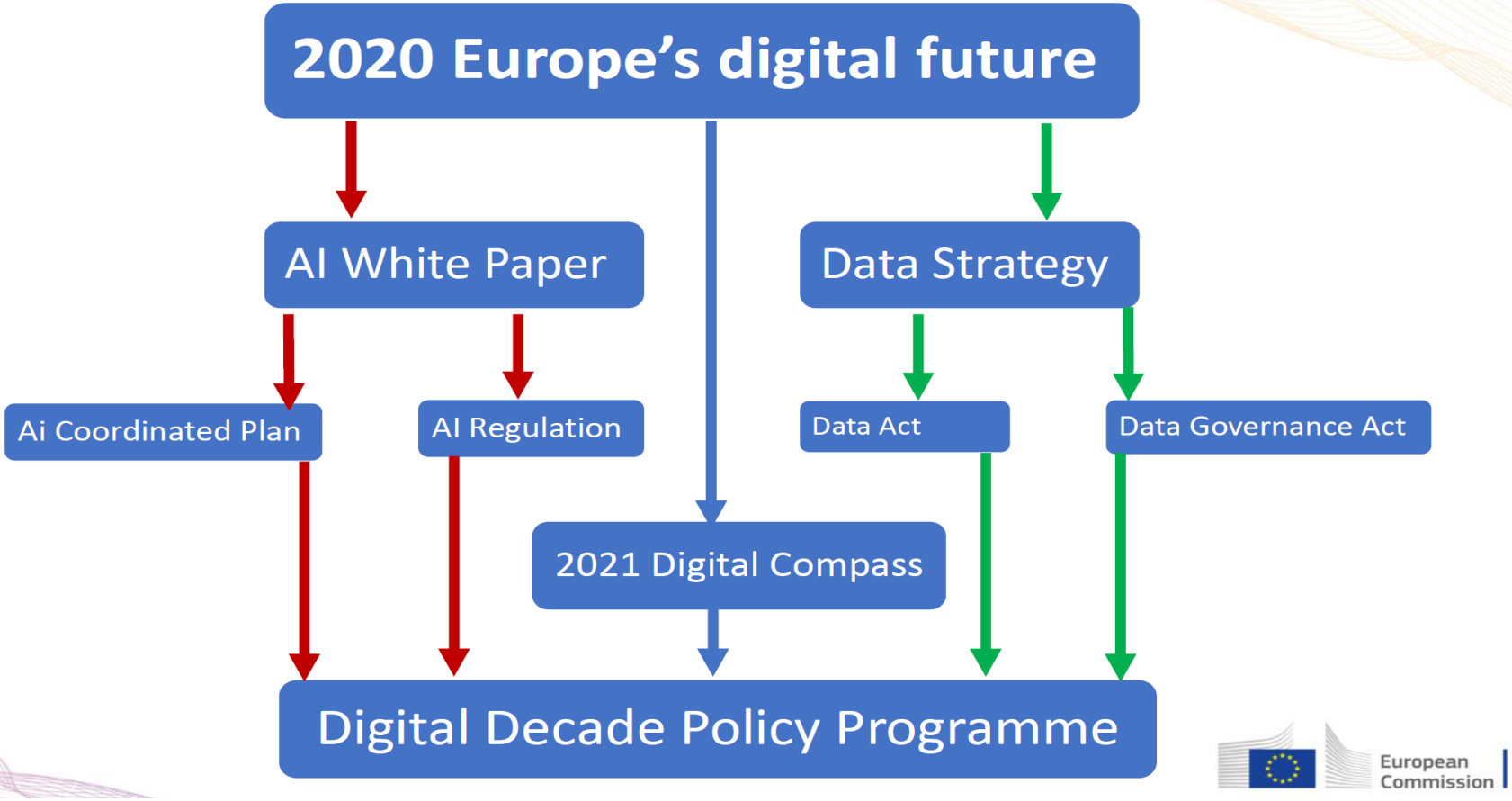
EU's Official Website https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#ecl-inpage-l6ov8brl

A European approach to artificial intelligence

"The EU's approach to artificial intelligence centers on excellence and trust, aiming to boost research and industrial capacity while ensuring safety and fundamental rights.
The way we approach Artificial Intelligence (AI) will define the world we live in the future. To help building a resilient, people and businesses should be able to enjoy the benefits of AI while feeling safe and protected.
The European AI Strategy aims at making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy . Such an objective translates into the European approach to excellence and trust (.pdf) through concrete rules and actions."

EU's Official Website https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#ecl-inpage-l6ov8brl

EU's strategy in the field of AI at a glance



EU's strategy in the field of AI at a glance

Digital Compass

Skills

ICT Specialists: 20 million + Gender convergence
Basic Digital Skills: min 80% of population

Infrastructures

Connectivity: Gigabit for everyone, 5G in all populated areas
Cutting edge Semiconductors: double EU share in global production
Data – Edge & Cloud: 10,000 climate neutral highly secure edge nodes
Computing: first computer with quantum acceleration

Government

Key Public Services: 100% online
e-Health: 100% availability medical records
Digital Identity: 80% citizens using digital ID

Business

Tech up-take: 75% of EU companies using Cloud/AI/Big Data
Innovators: grow scale ups & finance to double EU Unicorns
Late adopters: more than 90% of European SMEs reach at least a basic level of digital intensity

European Commission

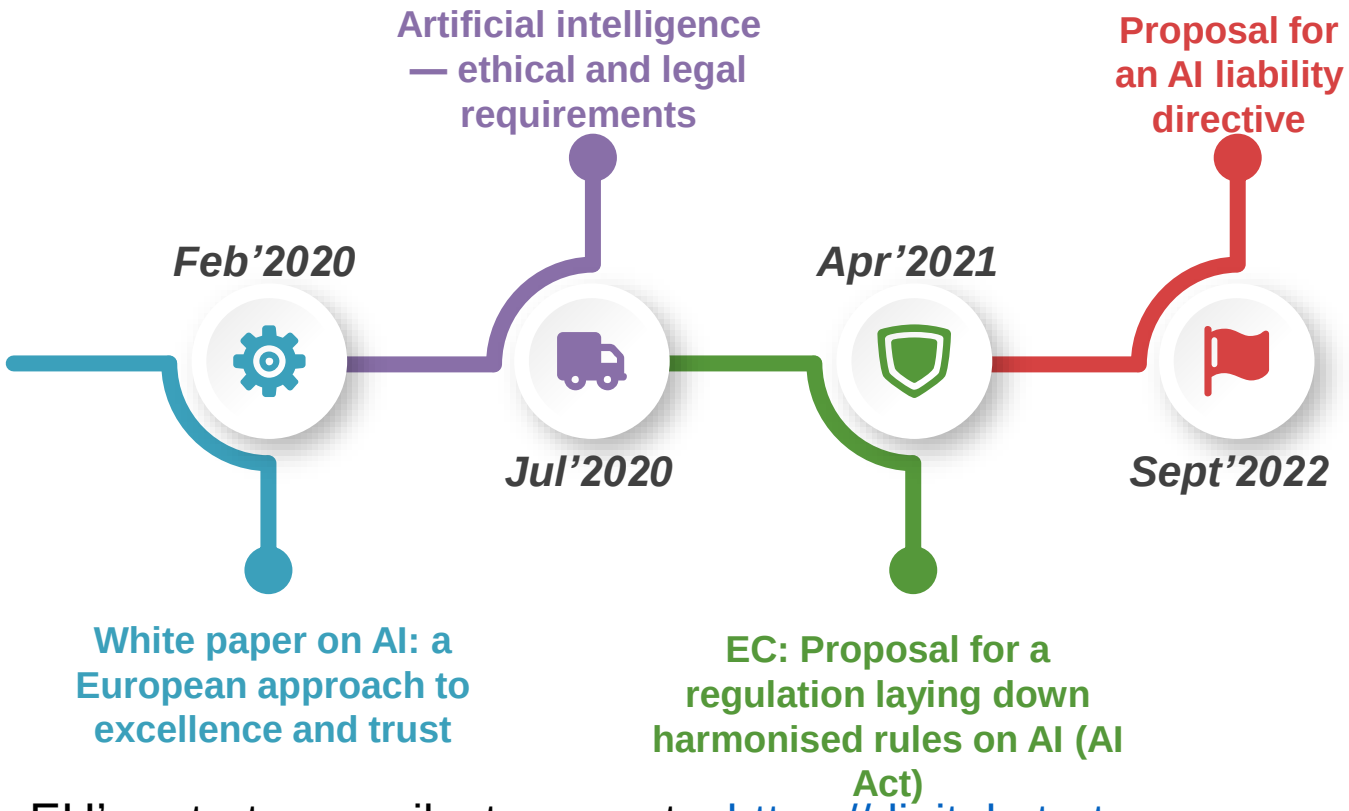
A European approach to excellence in AI

Fostering excellence in AI will strengthen Europe's potential to compete globally.

The EU will achieve this by:

- ✓Enabling the development and uptake of AI in the EU;
- ✓Making the EU the place where AI thrives from the lab to the market;
- ✓Ensuring that AI works for people and is a force for good in society;
- ✓Building strategic leadership in high-impact sectors.

EU Legislative Initiatives - Important Milestones



More info about the EU's strategy milestones at: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#ecl-inpage-l6ov8brl

A European approach to excellence in AI

EU focuses on the Access to high quality data which is an essential factor in building high performance, robust AI systems.

In this context EU has taken the following legislative Initiatives

- The EU Cybersecurity Strategy ,
- The Digital Services Act and the Digital Markets Act ,
- The Data Governance Act provide the right infrastructure for building such systems.

A European approach to excellence in AI

Data Governance Act

- Access to and re-use of sensitive public data.
- Emergence and of new neutral data players in Europe.
- Allow Europeans to gain more control over their data.
- A safe environment for those willing to share data

Data Act

- Ensuring fairness in the allocation of economic value among actors of the data economy
- fair data access, processing and use in business-to-business (B2B) context
- fair, reliable and transparent data access and use in business-to-government (B2G) context

European Commission

European proposal for a legal framework on AI

In April 2021, the Commission presented its AI package, including:

- Its Communication on fostering a European approach to artificial intelligence ;
- An update of the Coordinated Plan on Artificial Intelligence (with EU Member States) ;
- Its proposal for a regulation laying down harmonised rules on AI (AI Act) and relevant Impact assessment .

European proposal for a legal framework on AI

AI Regulation

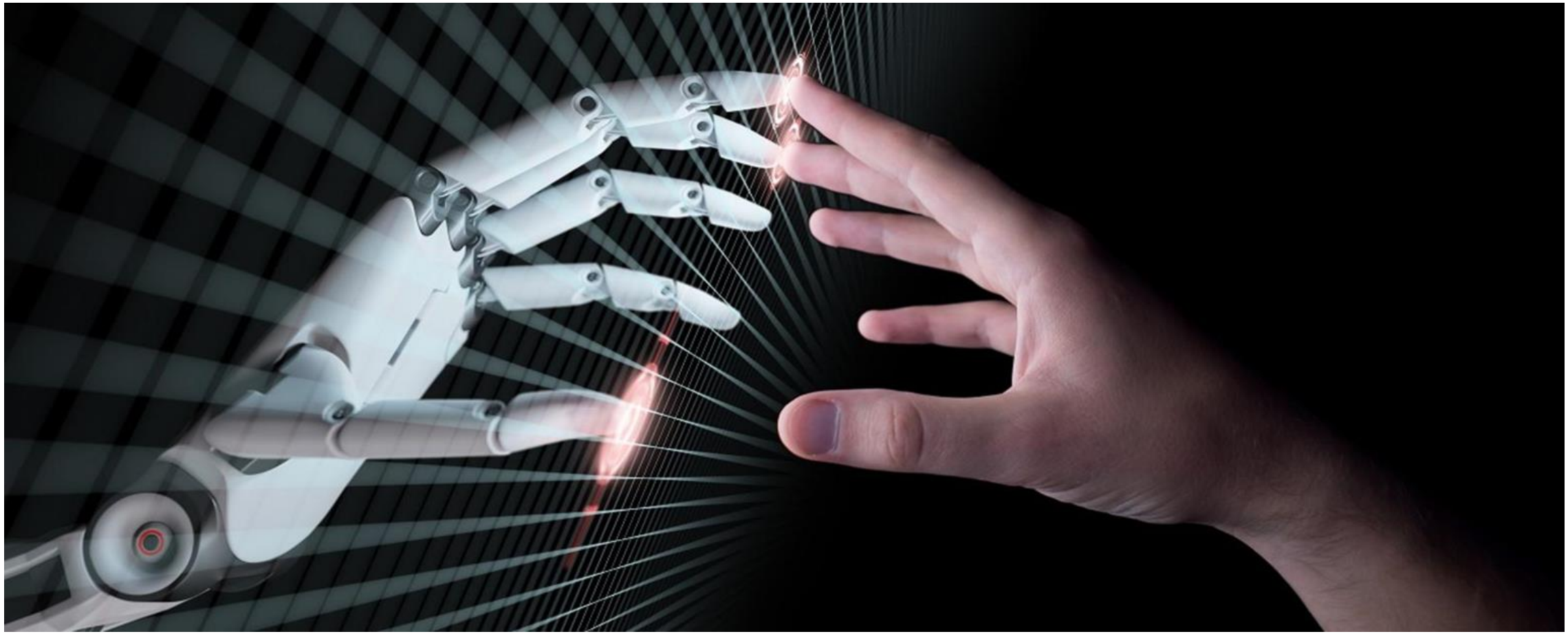
- Definition of AI
- A risk-based approach
- Light but effective requirements
- Enforcement
- Governance

AI Coordinated Plan

- Accelerate investments
- Act on strategies
- Align policy
- Strategic sectors

European Commission

EU Proposal for an Artificial Intelligence Regulation (AI Act)

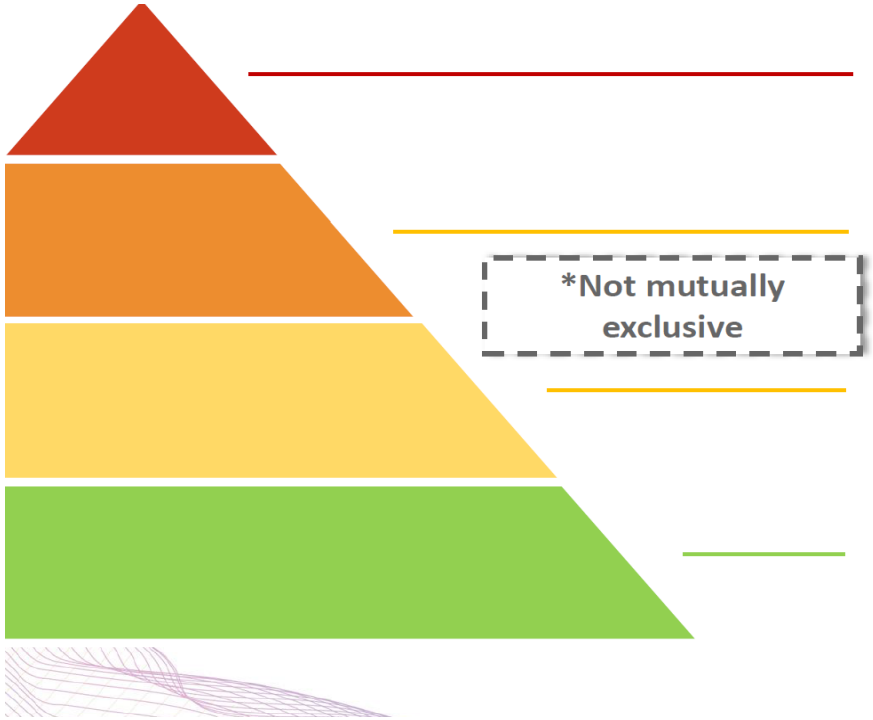


EU Proposal for an Artificial Intelligence Act (Definition)

‘Artificial intelligence system’ (AI system) means a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions , influencing the environments with which the AI system interacts;

EU Proposal for an Artificial Intelligence Act (Categories of AI Systems – Risk based approach)

EU categorizes the AI Systems in the following Categories:



Unacceptable risk
e.g. social scoring
— **Prohibited**

High risk
e.g. recruitment, medical devices
— **Permitted** subject to compliance with AI requirements and ex-ante conformity assessment

'Transparency' risk
'Impersonation' (bots)
— **Permitted** but subject to information/transparency obligations

Minimal or no risk
— **Permitted** with no restrictions

European Commission

EU Proposal for an Artificial Intelligence Act (Prohibited Systems)

Subliminal manipulation resulting in physical/ psychological harm

Example: An **inaudible sound** is played in truck drivers' cabins to push them to **drive longer than healthy and safe**. AI is used to find the frequency maximising this effect on drivers.

Exploitation of children or mentally disabled persons resulting in physical/psychological harm

Example: A doll with an integrated **voice assistant** encourages a minor to **engage in progressively dangerous behavior** or challenges in the guise of a fun or cool game.

General purpose social scoring

Example: An AI system **identifies at-risk children** in need of social care **based on insignificant or irrelevant social 'misbehavior'** of parents, e.g. missing a doctor's appointment or divorce.

Remote biometric identification for law enforcement purposes in publicly accessible spaces (with exceptions)

Example: All faces captured live by video cameras checked, in real time, against a database to identify a terrorist.

EU Proposal for an Artificial Intelligence Act (High Risk AI Systems 1/2)

AI systems deployed in the following sectors are deemed to be high-risk to safety or fundamental rights:

- Critical infrastructure where the AI system could put people's life and health at risk;
- Educational and vocational settings where the AI system could determine access to education or professional training;
- Employment, worker management and self-employment; (such as Recruitment AI systems)

EU Proposal for an Artificial Intelligence Act (High Risk AI Systems 2/2)

AI systems deployed in the following sectors are deemed to be high-risk to safety or fundamental rights:

- Essential private and public services, including access to financial services such as credit scoring systems;
- Law enforcement;
- Migration, asylum and border control, including verifying the authenticity of travel documents;
- The administration of justice.

EU Proposal for an Artificial Intelligence Act (High Risk AI Systems – Main Obligations 1/2)

- Creating and maintaining a risk management system for the entire lifecycle of the system;
- Testing the system to identify risks and determine appropriate mitigation measures, and to validate that the system runs consistently for the intended purpose, with tests made against prior metrics and validated against probabilistic thresholds;
- Establishing appropriate data governance controls, including the requirement that all training, validation, and testing datasets be complete, error-free, and representative;
- Detailed technical documentation, including around system architecture, algorithmic design, and model specifications;

EU Proposal for an Artificial Intelligence Act (High Risk AI Systems – Main Obligations 2/2)

- Automatic logging of events while the system is running, with the recording conforming to recognized standards;
- Designed with sufficient transparency to allow users to interpret the system's output;
- Designed to maintain human oversight at all times and prevent or minimize risks to health and safety or fundamental rights, including an override or off-switch capability.

EU Proposal for an Artificial Intelligence Act (High Risk AI Systems – Main Obligations at a glance)

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**

EU Proposal for an Artificial Intelligence Act (High Risk AI Systems)

New rules for providers of high-risk AI systems

Step 1	Step 2	Step 3	Step 4	
A high-risk AI system is developed	It needs to undergo the conformity assessment and comply with AI requirements For some systems a notified body is involved	Registration of stand-alone AI systems in an EU database	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*

EU Proposal for an Artificial Intelligence Act (Limited and Lower Risk AI Systems)

Providers should be encouraged to create codes of conduct

Providers should be encouraged to apply additional requirements (Vonutary)

Providers should ensure that natural persons are informed that they interract with an AI System

EU Proposal for an Artificial Intelligence Act (Fines)

Non-compliance with prohibited uses and data governance obligations is punishable with a fine of up to **€30M** or 6 percent of worldwide annual turnover (whichever is higher);

For high-risk AI applications, the ceiling is **€20M** or 4 percent of turnover

The supply of incorrect, incomplete, or misleading **information to national competent bodies is subject to a fine of up to €10M** or 2 percent of turnover.

AI and Data Protection Legislation

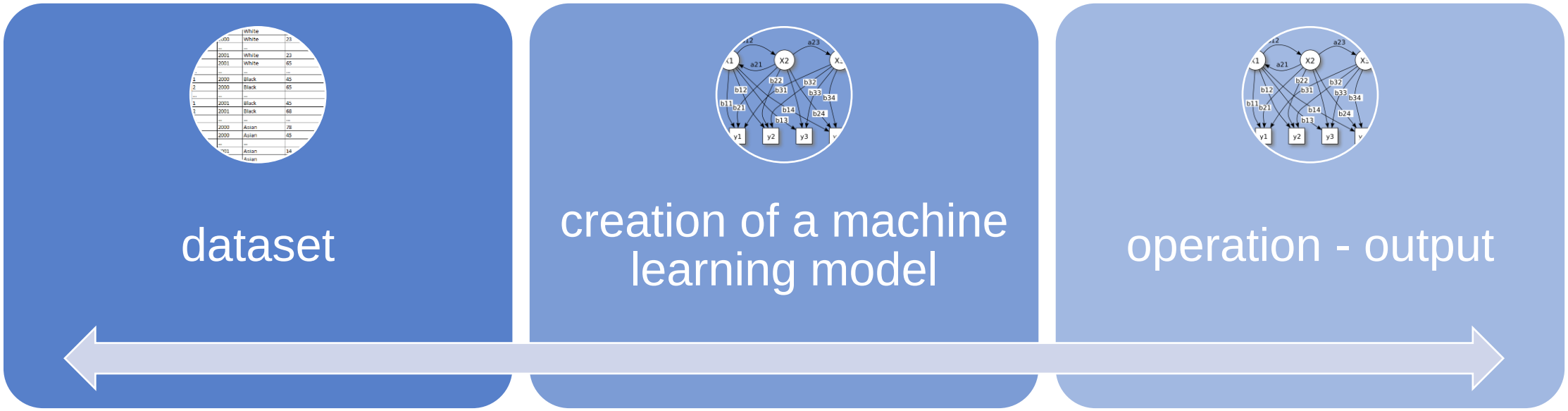
Data Protection Legislation and AI Systems

Data Protection Legislation's requirements affect the AI Systems in their whole lifecycle:

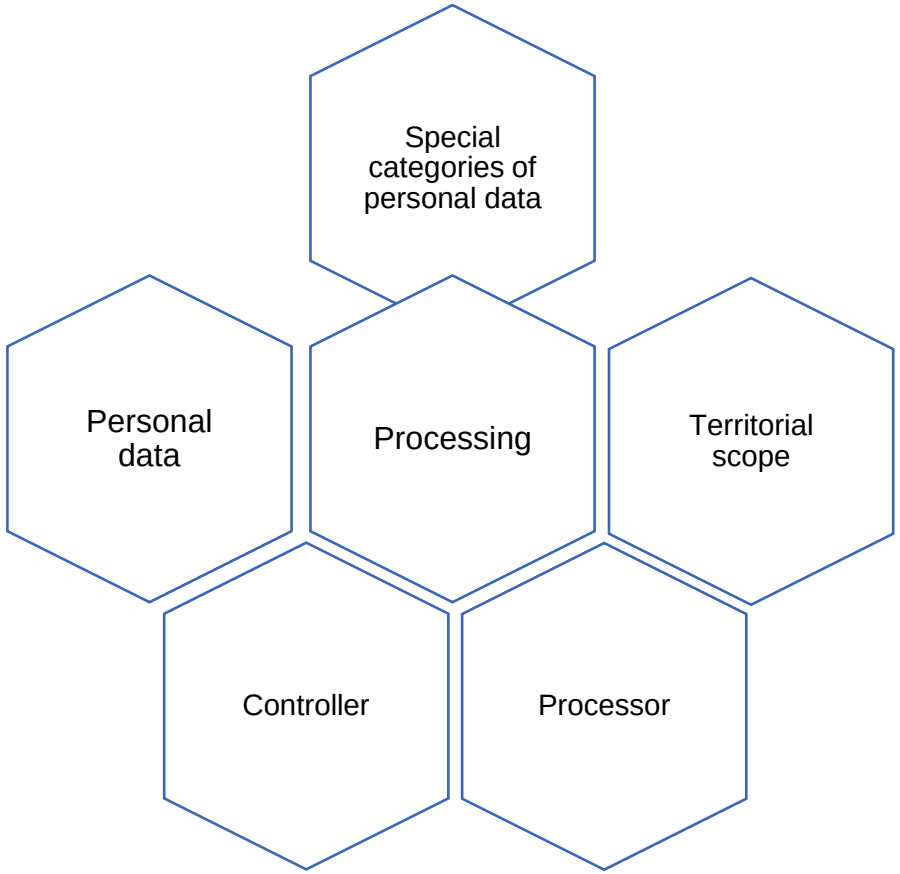
a) Step 1: Collecting and using a training dataset (For the training of an algorithm a big volume of data is needed).
b) Step 2: Creation of the AI System (The Use of Personal Data for this purpose, shall follow the Data Protection Legislation's requirements).
c) Step 3: Use of the AI System (specific requirements apply to the automatic decision making procedure).

Data Protection Legislation and AI Systems

Data Protection Legislation's requirements affect the AI Systems through their whole lifecycle



Data Protection Legislation and AI Systems – Definitions of Data Protection Legislation (1/



Data Protection Legislation and AI Systems – Step 1 Collecting and using a training dataset (1/3)

According to Data Protection Legislation, any process of Personal Data shall respect the following principles:

- Purpose limitation
- Data minimization
- Storage limitation

Data Protection Legislation and AI Systems – Step 1 Collecting and using a training dataset (2/3)

Purpose limitation

The principle of purpose limitation is designed **to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use**

Data minimization

The principle of “data minimisation” means that **a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose**.

Storage limitation

The principle of “storage limitation” means that even if you collect and use personal data fairly and lawfully, **you cannot keep it for longer than you actually need it**.

Data Protection Legislation and AI Systems – Step 1 Collecting and using a training dataset (3/3)

So, In case there is a need to use personal data, among other data, in order to train the AI System:

The principles of

- ✓ data minimization,
- ✓ storage limitation and
- ✓ purpose limitation,

Impose strict requirements as long as it concerns the lawfulness of the training dataset.

Step 2: Creation of the AI System: Processing for purpose other than that for which the personal data have been collected

In the context of the development of an AI System we may need to process personal data.

But is it legal to use the collected personal data for a purpose other than that for which they have been collected?

The Data Protection Legislation sets some prerequisites:

a) The Data Subject consents to the process, or

b) The data process is based on EU or Member State specific law, or

c) There is a compatibility of purposes

Step 2: Creation of the AI System: Processing for purpose other than that for which the personal data have been collected

Based on Consent

-Distinguishable from the other matters - Action
- Controller shall be able to demonstrate the consent
- Withdrawal at any time
- Necessary for the performance of that contract

Based on Union or Member State law

Compatibility of purposes

-Link between the purposes.
- The context in which the personal data have been collected.
– The nature of the personal data.
- Appropriate safeguards, which may include encryption or pseudonymisation.
- Possible consequences.

Step 2: Creation of the AI System: Obligations regarding the Data Protection Principles and the Data Subject's Rights

Principles

- lawfulness
- fairness
- transparency
- integrity and confidentiality
- Privacy by Design, Privacy by Default
- ACCOUNTABILITY

Rights of the data subject

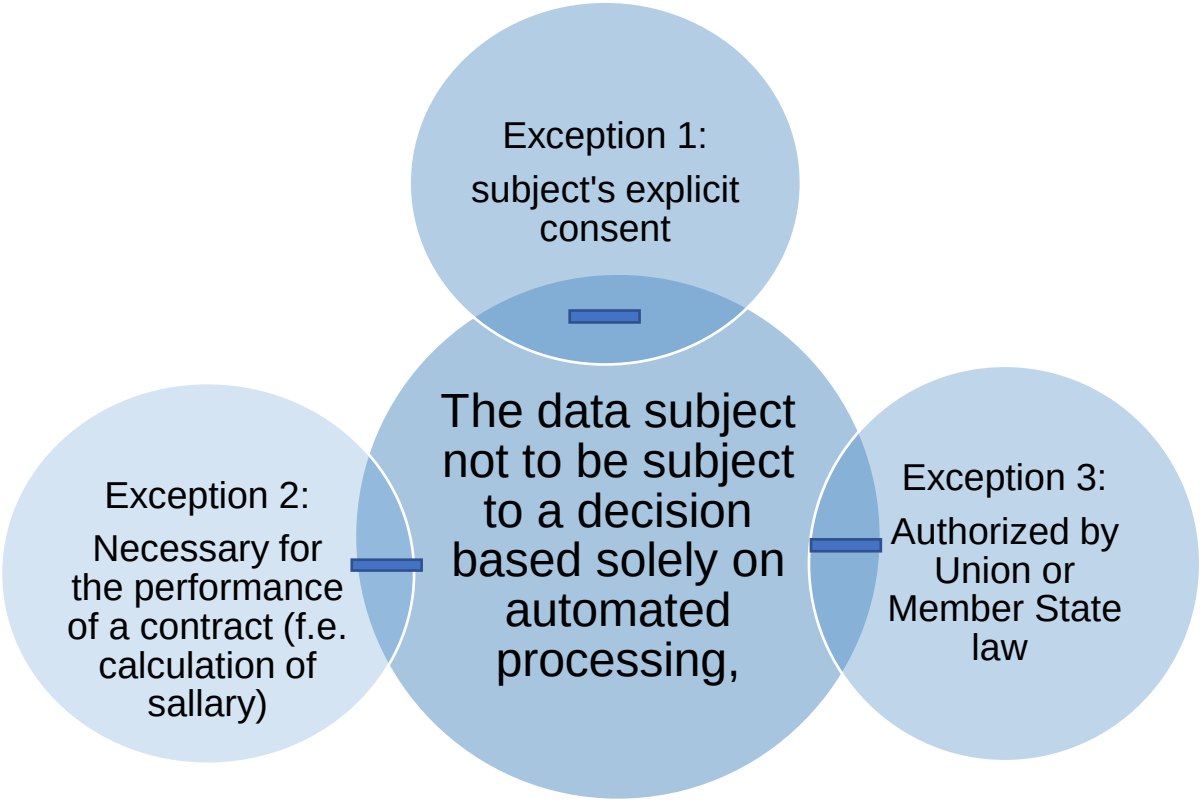
- Transparent information
- Access
- Rectification and erasure
- Right to data portability
- Right to object under conditions
- Right to object ''marketing profiling''

Step 2: Creation of the AI System: Additional obligations imposed by Data Protection Legislation

- In case the process of personal data is likely to result in a high risk to the rights and freedoms of natural persons, a Data Protection Impact Assessment shall be conducted.
- If the risk cannot be minimized, a prior consultation with the component Data Protection Authority is needed.
- The “Privacy by Design” and “Privacy by Default” principles are applicable. According to these principles technical and organizational security measures shall be taken.

Step 3: Use of the AI System

Decision without human intervention?



Always needed:

Measures to safeguard rights and freedoms

+

Always needed:

The right to obtain human intervention - express point of view and contest the decision

Step 3: Use of the AI System – Transparency and Accountability

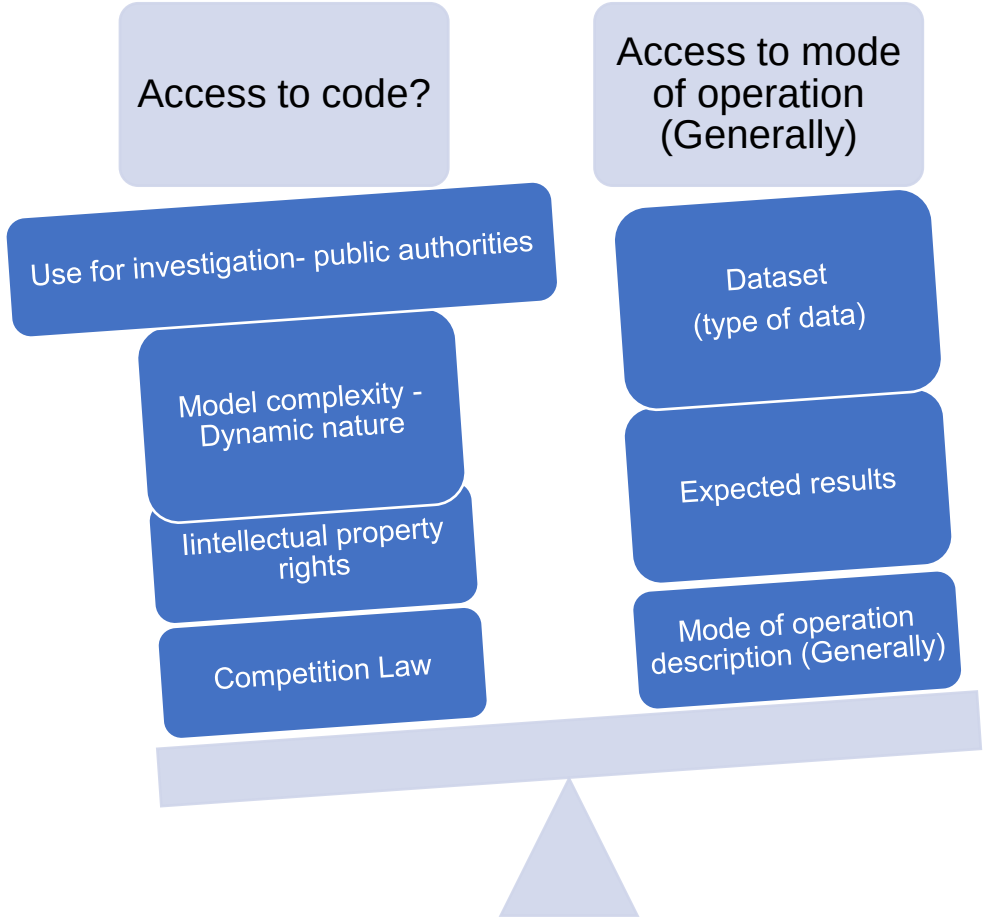
According to Data Protection Legislation there are obligations related to:

- ✓ The Principle of Transparency and Accountability, and
- ✓ The Right of transparent information.

Access to the code? Or General information related to the mode of AI's system operation?

Step 3: Use of the AI System

Still a matter of Discussion:



Data Protection Legislation and AI Systems – The Critical issues at a glance

Dataset

- Purpose limitation
- Data minimization
- Storage limitation
- Purpose other than that for which the personal data have been collected

Lawfulness of processing

- Transparency
- Accountability
- Fairness
- Privacy by design-by default
- Transparent information and access
- Risk and Impact Assessment

Operation - output

- The data subject not to be subject to a decision based solely on automated processing
- Algorithmic decision-making and fairness:
- Bias
- Ethical Issues

Case studies of AI accidents and Liability Issues

Accidents in wich AI Systems are involved

AID AI INCIDENT DATABASE English ★93 Subscribe

Incident ID	Title	Description	date	Alleged Deployer of AI S...	Alleged Developer of AIS...	Alleged Harmed or Nea
Search 363 records...	Search 363 records...	Search 363 records...	Search 363 records...	Search 363 records...	Search 363 records...	Search 363 records...
Incident 1	Google's YouTube Kids App Presents Inappropriate Content	YouTube's content filtering and recommendation algorithms exposed children to disturbing and inappropriate videos.	2015-05-19	YouTube	YouTube	Children
Incident 2	Warehouse robot ruptures can of bear spray and injures workers	Twenty-four Amazon workers in New Jersey were hospitalized after a robot punctured a can of bear repellent spray in a warehouse.	2018-12-05	Amazon	Amazon	Warehouse Workers
Incident 3	Crashes with Maneuvering Characteristics Augmentation System (MCAS)	A Boeing 737 crashed into the sea, killing 189 people, after faulty sensor data caused an automated manuevering system to repeatedly push the plane's nose downward.	2018-10-27	Boeing	Boeing	Airplane Passengers, Airplane Crew
Incident 4	Uber AV Killed Pedestrian in Arizona	An Uber autonomous vehicle (AV) in autonomous	2018-03-18	Uber	Uber	Elaine Herzberg, pedestrians

MENU

The incident database is accessible in the following web page https://incidentdatabase.ai/

The liability Issue

<u>The issue of Liability in case of an accident caused by an AI System:</u>

Who is liable?

- The User?
- The Seller/Manufacturer?
- The Developer?

EU Strategy in the context of liability issue

- In its White Paper on Artificial Intelligence, the Commission undertook to promote the uptake of artificial intelligence and to address the risks associated with certain of its uses.
- The Commission proposed a legal framework for artificial intelligence which aims to address the risks generated by specific uses of AI through a set of rules focusing on the respect of fundamental rights and safety.
- In the Report on Artificial Intelligence Liability, the Commission identified the specific challenges posed by artificial intelligence to existing liability rules.
- In October 2020, the European Parliament adopted a legislative own-initiative resolution, based on Article 225 TFEU, on civil liability for AI and requested the Commission to propose legislation.

EU Strategy in the context of liability issue

- On 28 September 2022, the Commission delivered on the objectives of the White Paper and on the European Parliament's request with the Proposal for an Artificial Intelligence Liability Directive (AILD).
- The purpose of the AI Liability Directive proposal is to improve the functioning of the internal market by laying down uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems.
- The proposal addresses the specific difficulties of proof linked with AI and ensures that justified claims are not hindered.

AI Liability Directive proposal – Why?

Current liability rules, in particular national rules based on fault, are not adapted to handle compensation claims for harm caused by AI-enabled products/services.

Under such rules, victims need to prove a wrongful action/omission of a person that caused the damage.

The specific characteristics of AI, including autonomy and opacity, make it difficult or prohibitively expensive to identify the liable person and prove the requirements for a successful liability claim

AI Liability Directive proposal – Goals

The AI initiative will:

- Ensure that victims of AI-enabled products/services are equally protected as victims of traditional technologies.

- Reduce legal uncertainty regarding the liability exposure of businesses developing or using AI.

- Prevent the emergence of fragmented AI-specific adaptations of national civil liability rules.

AI Liability Directive proposal – Summary

Under the proposed new AI Liability Directive, the presumption of causality will apply only if claimants can satisfy three core conditions:

a) The fault of an AI system provider or user has been demonstrated, or at least presumed to have been so by a court;

b) It can be considered reasonably likely, based on the circumstances of the case, that the fault has influenced the output produced by the AI system or the failure of the AI system to produce an output; and

c) The claimant has demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage.

Conclusion (1/2)

- The EU's approach to artificial intelligence centers on excellence and trust, aiming to boost research and industrial capacity while ensuring safety and fundamental rights.

- In this context, the legal initiatives focus in two pillars:

a) Boost AI Research: Access to high quality data which is an essential factor in building high performance, robust AI systems (The Data Governance Act, the Digital Services Act and the Digital Markets Act)

b) Regulate AI (AI Act, AI Liability Directive)

Conclusion (2/2)

Taking into account that the legislative procedure hasn't finished yet, the main obligations related to the development and use of AI Systems are coming, by now, from the Data Protection Legislation and particularly from the General Data Protection Regulation (679/2016) and the Directive 680/2016.

AI.4.educators

AI.4.educators
Educating Educators on Artificial Intelligence (AI) – development of an AI training material and an AI educational program for educators

Project No: 2021-1-EL01-KA210-ADU-000034976

AI Legal Roadmap

Co-funded by the European Union