AI ACT : HOW IS EU REGULATING AI TO PRESERVE HUMAN RIGHTS

Data Privacy Day 2024

30.01.2024

samuel.renault@list.lu

LUXEMBOURG
INSTITUTE OF SCIENCE
AND TECHNOLOGY
LIST

AGENDA

1 AI Act : overview & current state of development

2 Links & parallels between AI Act & GDPR

3 AI related risks as foreseen by the Act

4 Obligations for developers & users

#1 AI ACT

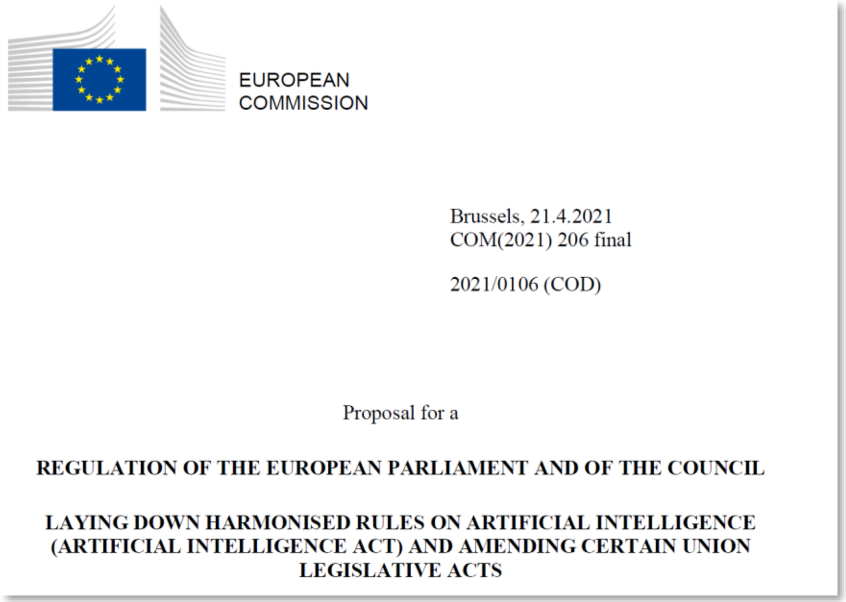
Overview & current state of development

WHAT IS THE AI ACT ?

A bill of law (regulation) under definition

Issued by EU Commission on April 21st 2021 [1]
Discussions at EU council 2021 → 2022
Parliament amendments May 2023 [2]
Trilogue : June → Dec 8th 2023

Vote expected in 2024
Entry into force expected in 2026



EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

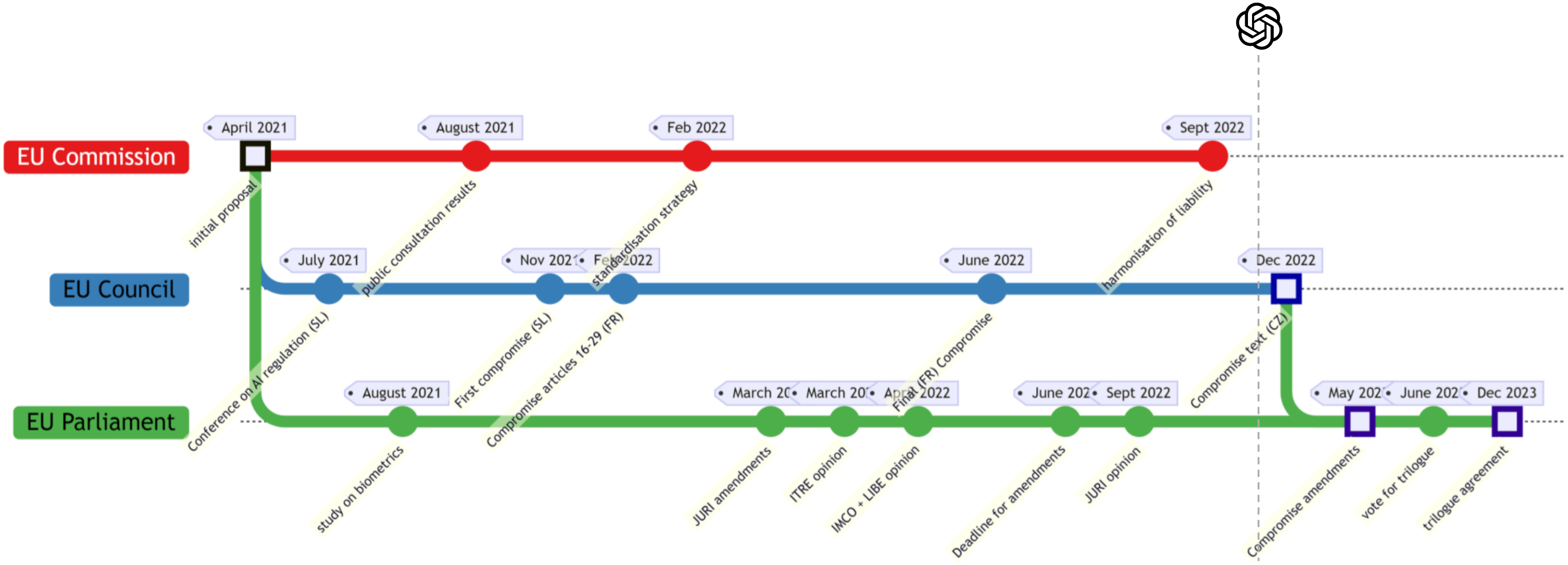
2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

AI ACT DEVELOPMENT



Source: https://artificialintelligenceact.eu/developments/

DISCLAIMER

This content is based on the draft text

Does not exhaustively reflect what will be the final version

Guidelines on implementation to come (art 58a)

Work in progress

DEFINITIONS

AI system

[…] machine-based system designed to operate with **varying levels of autonomy** and that may exhibit **adaptiveness after deployment** and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as **predictions, content, recommendations, or decisions that can influence physical or virtual environments**. .

general purpose AI model

[…] AI model, including when trained with a large amount of data using self-supervision at scale, that **displays significant generality** and is **capable to competently perform a wide range of distinct tasks** regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications.

This does not cover AI models that are used before release on the market for research, development and prototyping activities.

#2 LINKS BETWEEN AI ACT & GDPR

A COMPARATIVE VIEW OF AI ACT & GDPR

Shared characteristics

GDPR		AI Act
	EU regulations	
	Potential worldwide applicability if EU citizens are impacted	
EU Data Prot° Board	EU coordination	EU AI office
	Purpose-based	
	Accountability principle	
	Code of conduct & certification through notified bodies	
20 M€ / 4 % WAT	(significant) enforcement fines	35 M€ / 7% WAT
	Focus on protecting citizens' rights	
	Collaboration with authorities in case of incidents	
	Importance of risks management / impact analysis	

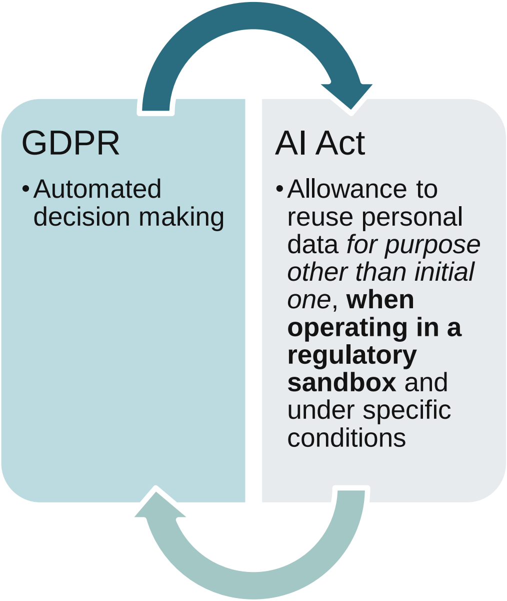
A COMPARATIVE VIEW OF AI ACT & GDPR

Some differences

GDPR	AI Act
Creation of new rights for citizens	No new rights created
Applicable to all when personal data are collected and processed	Applicable as soon as an AI system is put on the market
New role in organisations : data protection officer	No specific role required in organisations
	Explicit room for innovation (regulatory sandbox)
	EU database of AI systems, providers, conformity assessment operators (notified bodies)

A COMPARATIVE VIEW OF AI ACT & GDPR

Noticeable interdependencies



GDPR

- Automated decision making

AI Act

- Allowance to reuse personal data *for purpose other than initial one*, **when operating in a regulatory sandbox** and under specific conditions

#3 AI RELATED RISKS

AI RISKS CATEGORIES

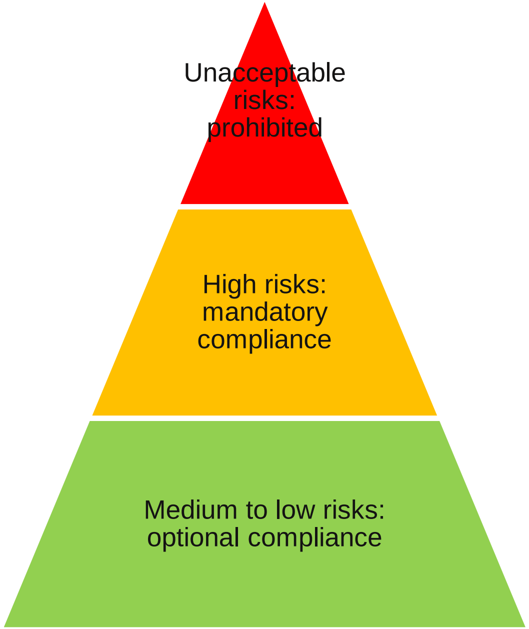
Classification of AI systems deployed in EU

Classification is (AI system) **purpose-based**

Unacceptable risks: prohibited

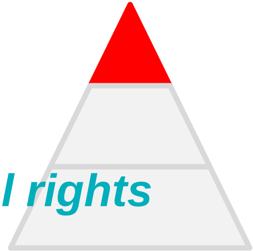
High risks: mandatory compliance with requirements & obligations

Medium to low risks: optional (but recommended) compliance to requirements & obligations


Unacceptable risks: prohibited
High risks: mandatory compliance
Medium to low risks: optional compliance

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

PROHIBITED AI SYSTEMS



Systems presenting *unacceptable risks for human beings or fundamental rights*

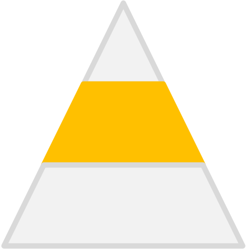
Subliminal techniques or persons' vulnerabilities exploitation

Social scoring leading to detrimental/unfavourable treatment

Real-time remote biometric identification in public space (for law enforcement)*

* with exceptions

HIGH RISK AI SYSTEMS



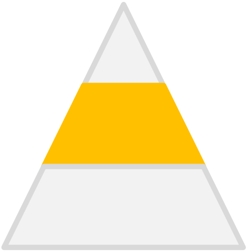
AI system embed in products that can physically harm a person (Annex II)

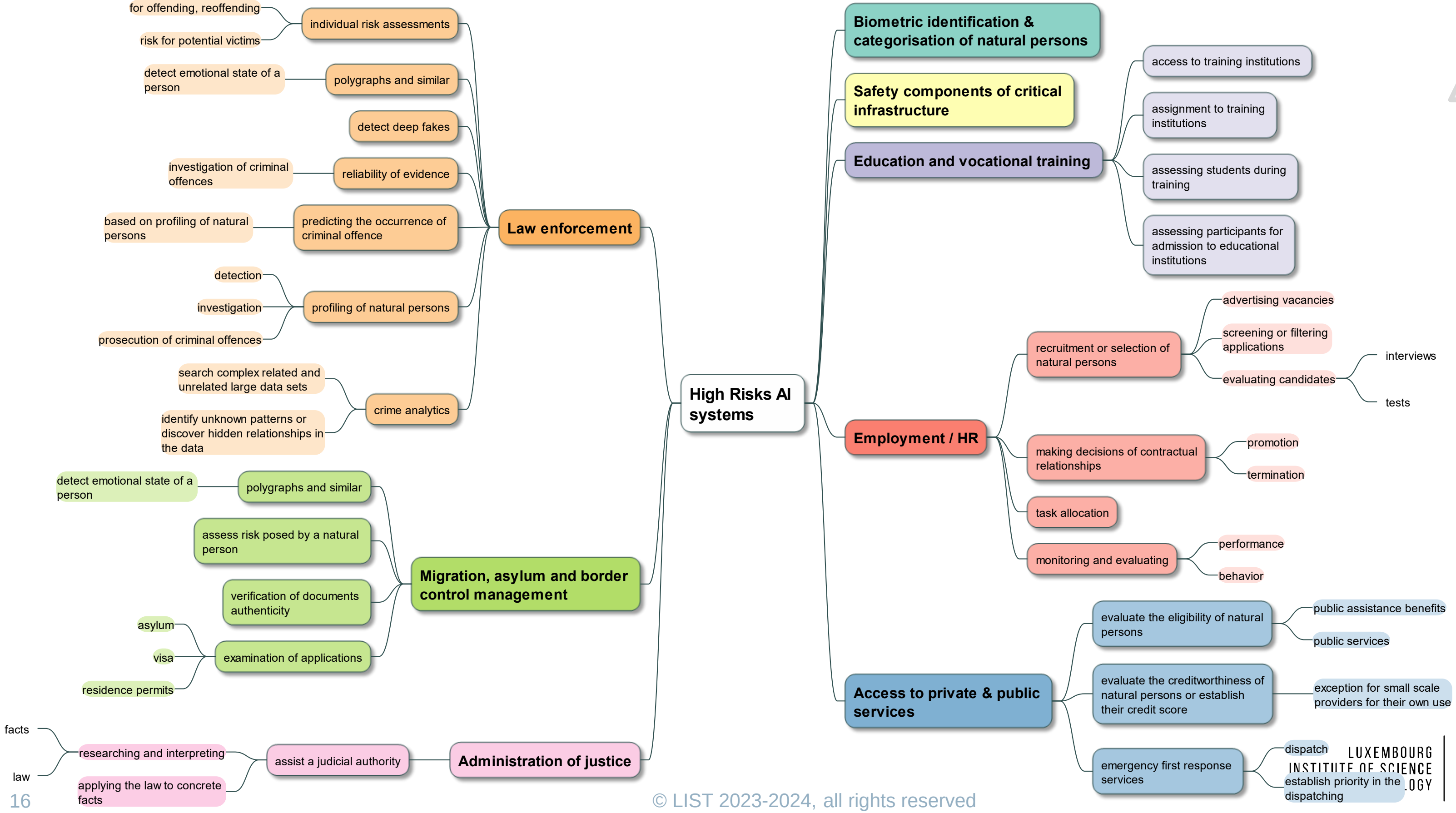
Products already covered by EU legislation
- Machines, toys, lifts, medical devices … (Annex II A)
- Vehicles : road, rails, water, air … (Annex II B)

AI system that can jeopardise human rights (Annex III)

Risks of discrimination or unfair treatment

HIGH RISK AI SYSTEMS



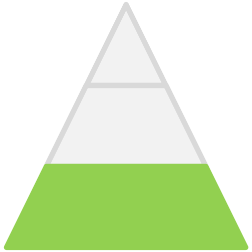


- High Risks AI systems
  - Law enforcement
    - individual risk assessments
      - for offending, reoffending
      - risk for potential victims
    - polygraphs and similar
      - detect emotional state of a person
    - detect deep fakes
    - reliability of evidence
      - investigation of criminal offences
    - predicting the occurrence of criminal offence
      - based on profiling of natural persons
    - profiling of natural persons
      - detection
      - investigation
      - prosecution of criminal offences
    - crime analytics
      - search complex related and unrelated large data sets
      - identify unknown patterns or discover hidden relationships in the data
  - Migration, asylum and border control management
    - polygraphs and similar
      - detect emotional state of a person
    - assess risk posed by a natural person
    - verification of documents authenticity
    - examination of applications
      - asylum
      - visa
      - residence permits
  - Administration of justice
    - assist a judicial authority
      - researching and interpreting
        - facts
        - law
      - applying the law to concrete facts
  - Biometric identification & categorisation of natural persons
  - Safety components of critical infrastructure
  - Education and vocational training
    - access to training institutions
    - assignment to training institutions
    - assessing students during training
    - assessing participants for admission to educational institutions
  - Employment / HR
    - recruitment or selection of natural persons
      - advertising vacancies
      - screening or filtering applications
      - evaluating candidates
        - interviews
        - tests
    - making decisions of contractual relationships
      - promotion
      - termination
    - task allocation
    - monitoring and evaluating
      - performance
      - behavior
  - Access to private & public services
    - evaluate the eligibility of natural persons
      - public assistance benefits
      - public services
    - evaluate the creditworthiness of natural persons or establish their credit score
      - exception for small scale providers for their own use
    - emergency first response services
      - dispatch
      - establish priority in the dispatching

LUXEMBOURG INSTITUTE OF SCIENCE & TECHNOLOGY LIST

Summary of high risks AI systems as defined by the Annex III of AI Act

MEDIUM TO LOW RISKS AI SYSTEM



All other systems not classified unacceptable or high

No obligation to compliance, but recommendation to do so, through codes of conducts

#4 OBLIGATIONS

For AI users and developers

EU AI ACT

Compliance scope and obligations for high-risks AI systems

Compliance scope

- Risk management system
- Data & data governance
- Technical documentation
- Record keeping
- Transparency & information to users
- Human oversight
- Accuracy, robustness, cybersecurity

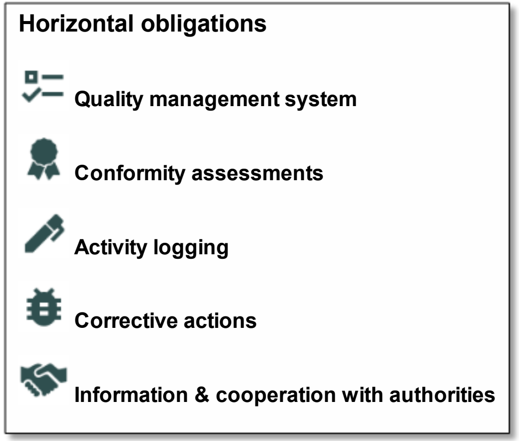
Horizontal obligations

- Quality management system
- Conformity assessments
- Activity logging
- Corrective actions
- Information & cooperation with authorities

EU AI ACT

Obligations for providers

- Ensure compliance
- Disclose contact details
- Have a **QMS**
- Keep documentation
- **Keep logs** when operating the AI system
- Perform **Conformity assessment** before placing on the market
- Register AI system in the EU database
- Take **corrective actions** in case of non conformity
- Mark CE in case of conformity
- **Inform authorities**, incl. in case of non-compliance & demonstrate conformity when requested



Horizontal obligations

Quality management system

Conformity assessments

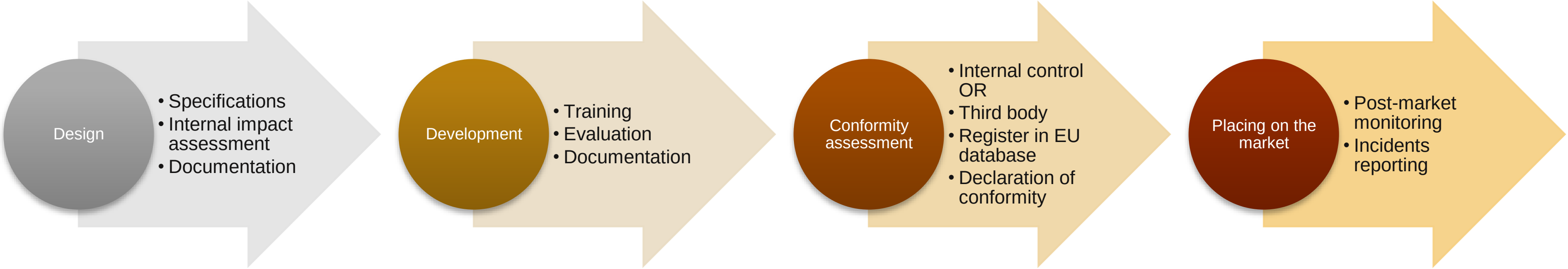
Activity logging

Corrective actions

Information & cooperation with authorities

TIMELINE OF A HIGH-RISK AI SYSTEM

Assumption that the AI system is ML-based



Design

- Specifications
- Internal impact assessment
- Documentation

Development

- Training
- Evaluation
- Documentation

Conformity assessment

- Internal control OR
- Third body
- Register in EU database
- Declaration of conformity

Placing on the market

- Post-market monitoring
- Incidents reporting

EU AI ACT

Obligations for other than providers

Providers obligations transferred in case of

- Branding transfer (name, trademark)
- Substantial modification after placing on the market
- Purpose modification of a system placed on the market making the system high-risk
- Placing on the market a general-purpose system making it high-risk or component of a high-risk system

CONCLUSION

AI ACT : HOW TO PREPARE

Stay tuned

Vote to come in 2024

Application in 2026

Prepare

Document
Log
Keep records

Identify the AI systems in use / planned & their purpose → risk classification

Get support

… there will be plenty

Ready4AI conference series (CC)

EU model of contractual clauses for procurements of AI systems

EXCELLENCE FOR IMPACT

LIST.lu

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

LIST

REFERENCE TEXTS

1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
2. https://artificialintelligenceact.eu/wp-content/uploads/2023/05/AIA-%E2%80%93-IMCO-LIBE-Draft-Compromise-Amendments-16-May-2023.pdf
3. https://artificialintelligenceact.eu/wp-content/uploads/2022/12/AIA-%E2%80%93-CZ-%E2%80%93-General-Approach-25-Nov-22.pdf
4. https://artificialintelligenceact.eu/wp-content/uploads/2022/06/AIA-IMCO-LIBE-Report-All-Amendments-14-June.pdf