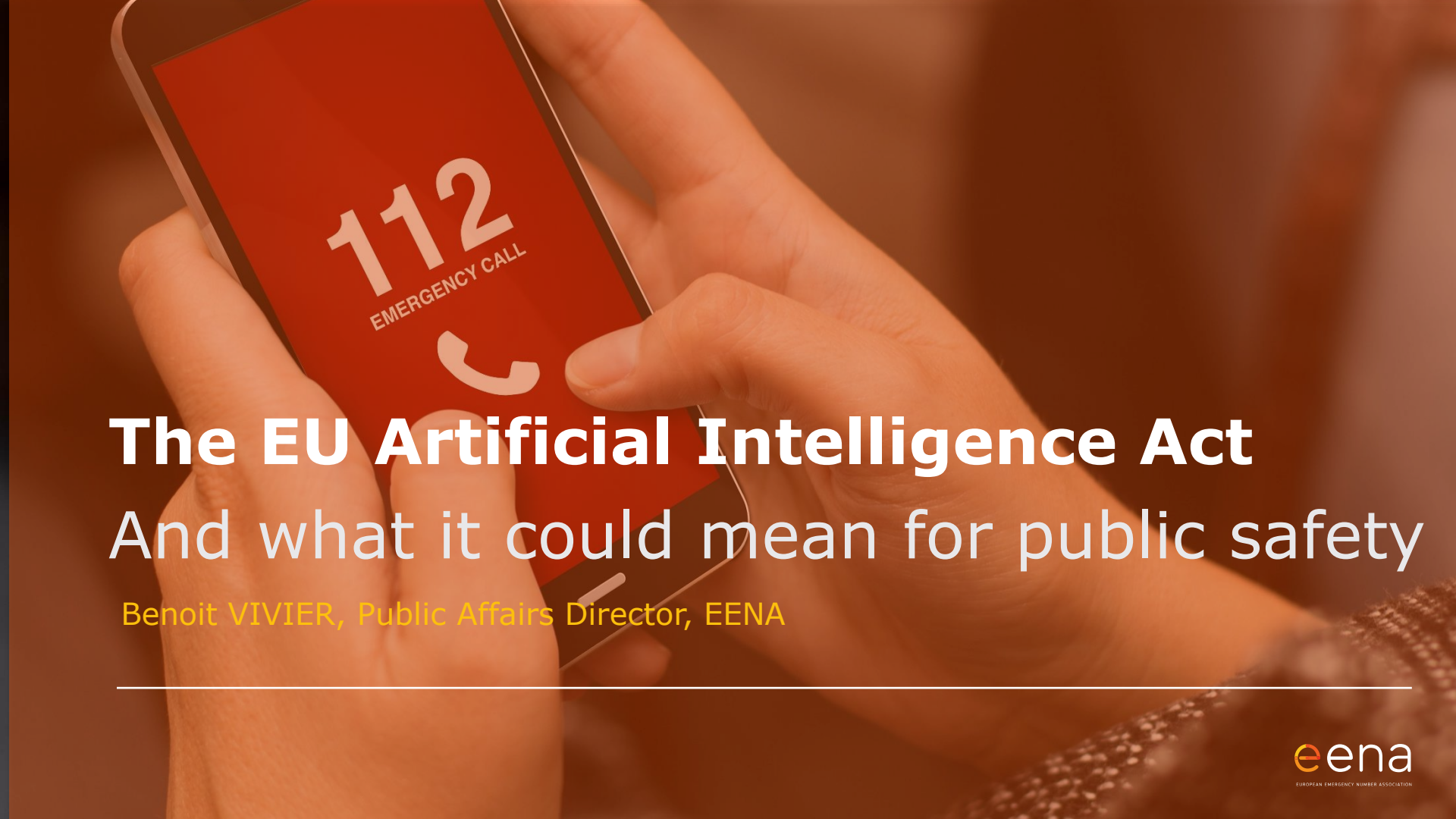


The EU Artificial Intelligence Act

And what it could mean for public safety

Benoit VIVIER, Public Affairs Director, EENA

eena
EUROPEAN EMERGENCY NUMBER ASSOCIATION

What are we discussing today

New EU regulation on Artificial Intelligence:

- Introduction to this upcoming legislation
- Will this affect public safety?
- Stage in the procedure and next steps

Spoiler of the presentation

- AI will not be banned
- Specific processes will apply to AI in emergency comms – handling.
- It is not that bad
- There will be drama

Who I am

- Public Affairs Director
- Follow EU policies related to emergency communications
- Joined EENA in 2015
- Background in EU politics

Agenda

1. Introductory remarks: EU decision-making
2. Introductory remarks: the EU AI Act
3. Practices to be banned
4. High-risk AI : what they are and what rules
5. Other provisions
6. Next steps
7. Q&A

1 The EU Decision-making

What is EU legislation?

Different kinds of legal acts:

- Directive
- Regulation
- Delegated and implementing acts

What is EU legislation?

Different kinds of legal acts:

- Directive
  - Binding
  - Require “transposition” in MS law
- Regulation
- Delegated and implementing acts

What is EU legislation?

Different kinds of legal acts:

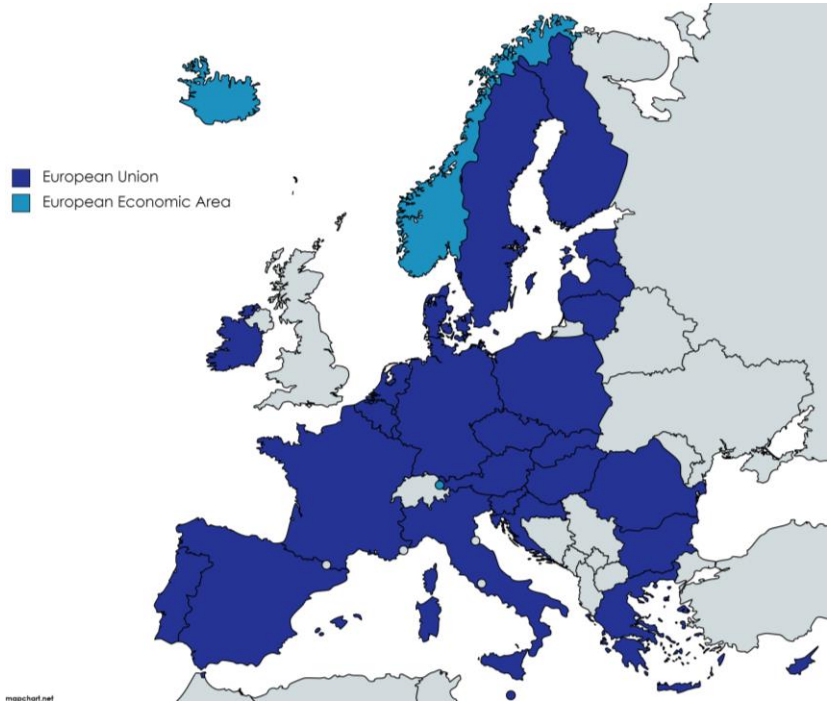
- Directive
- Regulation
  - Binding
  - Self-executive
- Delegated and implementing acts

What is EU legislation?

Different kinds of legal acts:

- Directive
- Regulation
- Delegated and implementing acts
  - Binding
  - Completes a previous legislation

Where does EU law apply?



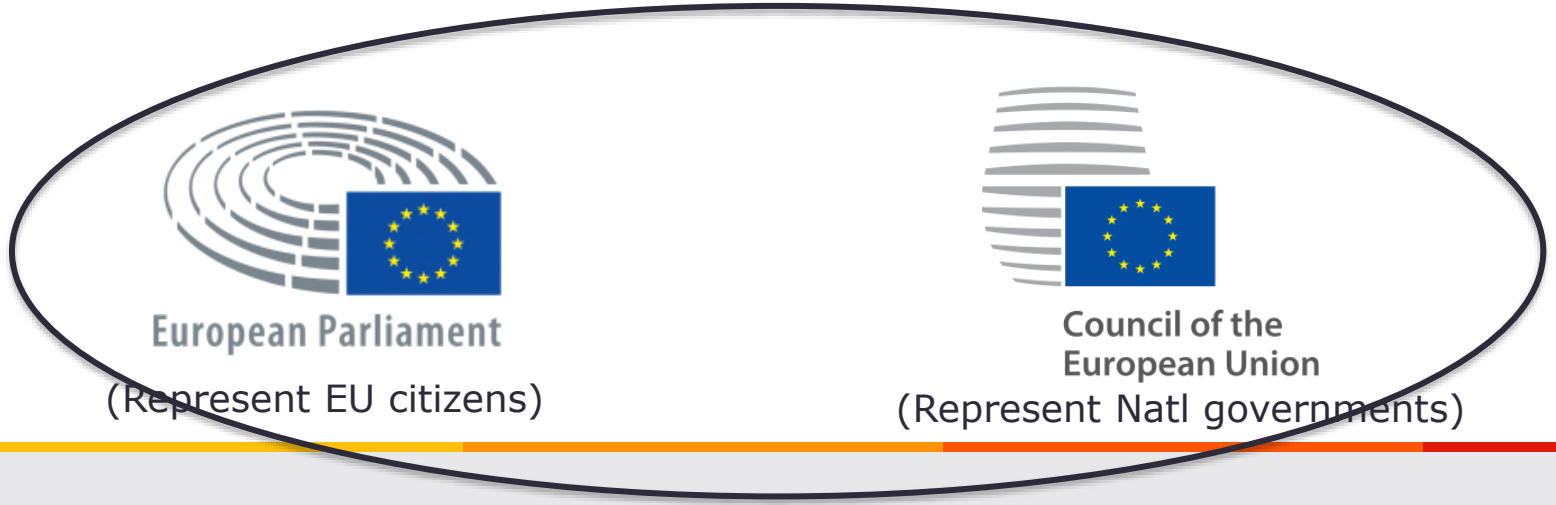
EU Decision-making

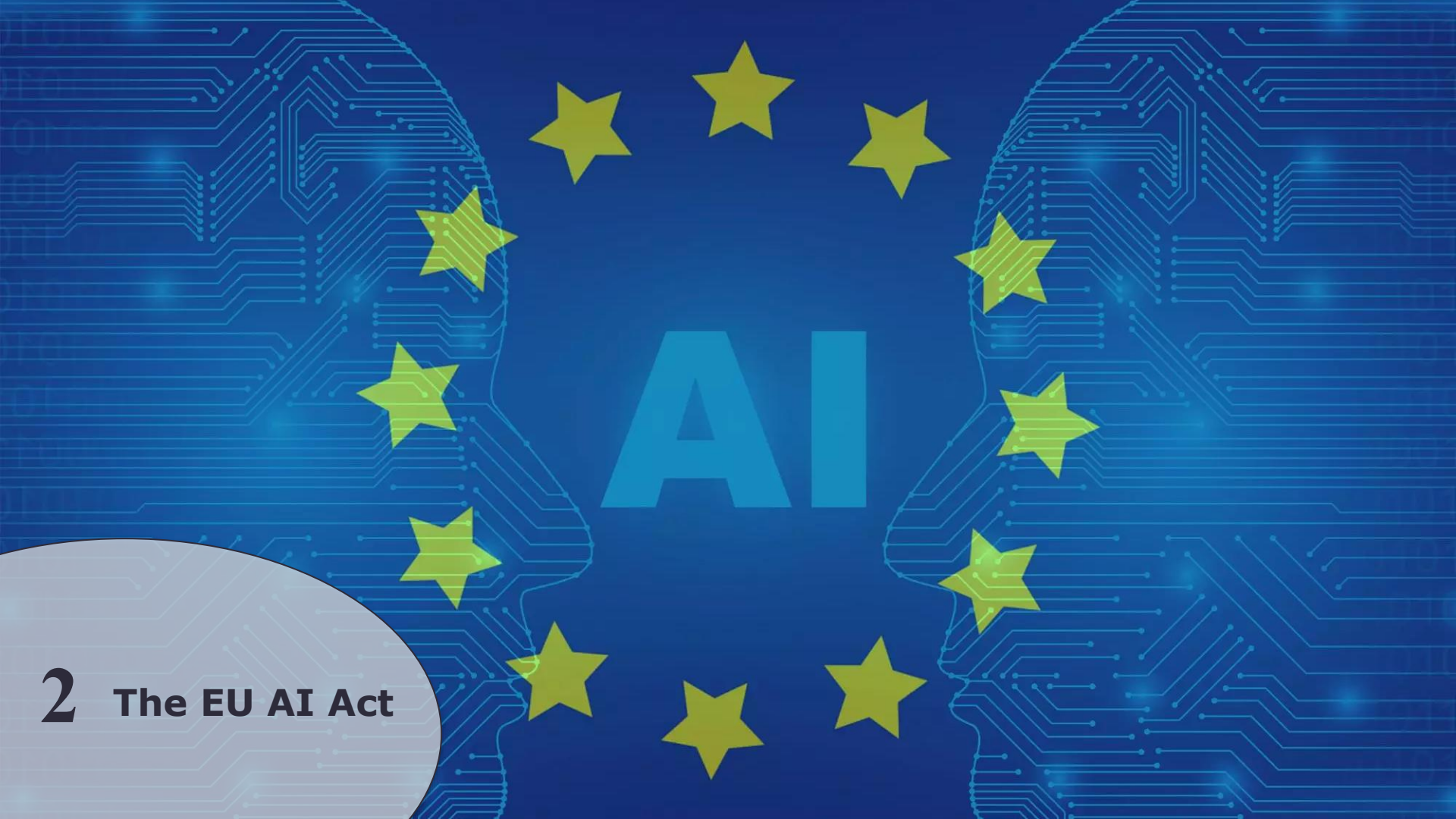
EU Decision-making

- Proposes draft legislations
- Enforce legislations

EU Decision-making

- Can amend proposals
- Adopt legislations





2 The EU AI Act

The EU AI Act: introduction

- Regulation
- Objectives:
  - Ensure that AI systems in the EU are safe and respect fundamental rights & Union values.
  - Ensure legal certainty to facilitate investment & innovation in AI
  - Facilitate the development of a single market for lawful, safe and trustworthy AI applications

The EU AI Act: procedure

21/4/2021:
Publication of the proposal

14/6/2023:
Vote in 1st reading (+amendments)

9/12/2022:
General Approach

The EU AI Act: introduction

How "AI system" is defined:

"software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

"(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods."

The EU AI Act: introduction

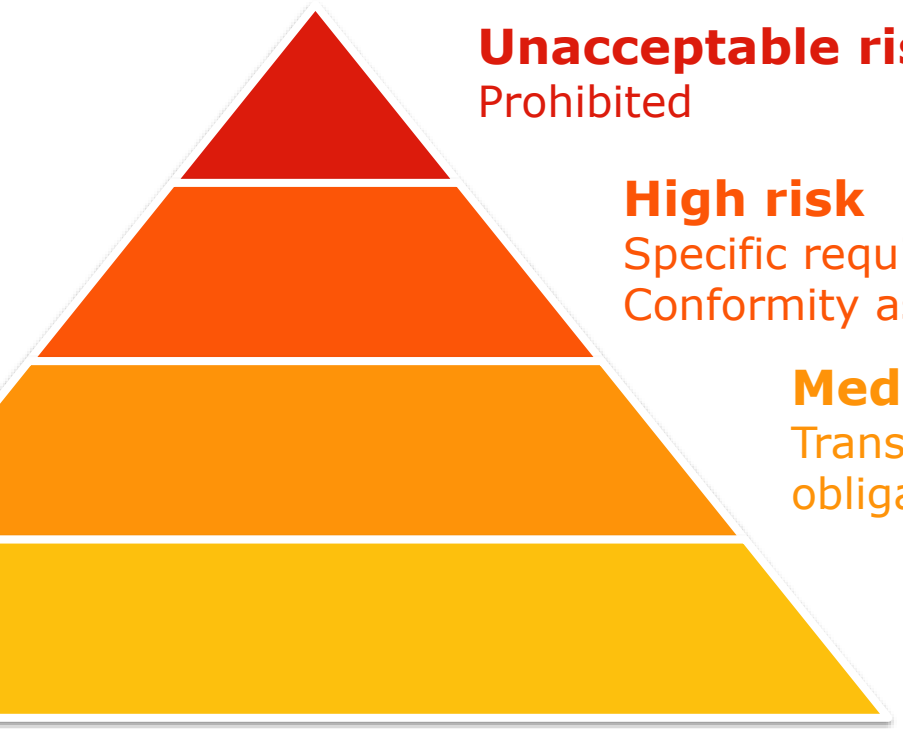
How “AI system” is defined:

“software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with”.

Applies to:

- Providers placing on the market or putting into service AI systems in the EU (irrespective of whether they are established in the EU or not)
- Users of AI systems in the Union
- Providers and users of AI systems that are located in a third country where the output produced by the system is used in the Union

The EU AI Act: a risk-based approach



Unacceptable risk
Prohibited

High risk
Specific requirements &
Conformity assessments

Medium risk
Transparency & Information
obligations

Minimal or low risk
Permitted with no restriction

3 AI practices to be banned

Prohibited AI practices:
Proposal by the European Commission

- Placing on the market of an AI system that causes physical or psychological harm of a person

- General purpose social scoring by public authorities

- Use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement

Prohibited AI practices:
Proposal by the European Commission

- Exemptions for the use of "'real-time' remote biometric identification systems in publicly accessible spaces ":
  - Search for specific potential victims of crime, including missing children
  - Prevention of an imminent threat to the life or the physical safety of natural persons or of a terrorist attack
  - Detection, localization, identification or prosecution of a perpetrator or suspect of a criminal offence.

- Such exemptions should take into account the nature of the situation and the consequences of the use of AI system for the rights and freedoms of the people concerned.

- The person to use such systems should receive a prior authorisation granted by a judicial authority or an independent administrative authority (except in duly justified situation of urgency).

Prohibited AI practices: *European Parliament amendments*

- Deletion of the exemptions for the use of biometric identification systems for the purpose of law enforcement.

- Addition to the prohibited practices of AI systems that:
  - Categorise people according to sensitive attributes.
  - Assesses the risk of a person (or group of persons) to commit criminal or administrative offenses based on profiling or assessing personality traits and characteristics.
  - Facial recognition from internet or CCTV footage
  - Infer emotions in the categories of law enforcement, border management, in workplace and education institutions

Prohibited AI practices:
Council General Approach

- Extension of the prohibition of AI on social scoring to private actors.

4 High-risk AI systems

High-risk AI systems:
List of High-risk AI systems (EC)

1. Biometric identification of people
2. Safety components in the management of critical infrastructure (road traffic, water, gas, heating & electricity)
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and public services and benefits
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes
9. AI used as safety component of certain products (incl. personal protective equipment & medical devices)

High-risk AI systems:
List of High-risk AI systems (EC)

1. Biometric identification of people
2. Safety components in the management of critical infrastructure (road traffic, water, gas, heating & electricity)
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and public services and benefits

    c. "AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid”

High-risk AI systems:
List of High-risk AI systems (EC)

1. Biometric identification of people
2. Safety components in the management of critical infrastructure (road traffic, water, gas, heating & electricity)
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and public services and benefits
6. Law enforcement
    a. Assessing the risk of people for committing criminal offences
    b. Detecting the emotional state of a person
    c. Detecting deep fakes
    d. Evaluating the reliability of an evidence
    e. Predicting the occurrence of a criminal offence based on profiling people
    f. Profiling people in the course of detectoin, investigation or prosecution.
    g. Crime analytics to search complex large data for investigation purposes

High-risk AI systems:
List of High-risk AI systems (EC)

1. Biometric identification of people
2. Safety components in the management of critical infrastructure (road traffic, water, gas, heating & electricity)
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and public services and benefits
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes
9. AI used as safety component of certain products (incl. personal protective equipment & medical devices)

High-risk AI systems:
List of High-risk AI systems (EP amendments)

Addition of several AI systems to the list, including:

- AI in the evaluation and classification of emergency calls
- AI to be used as safety components in the management and operational of critical digital infrastructure
- AI to be used for influencing the outcome of an election of referendum
- AI to be used by large social media platforms to recommend user-generated content available on the platform

Deletion of several entries in the list, including:

- AI systems used by LEAs to detect deep fakes

High-risk AI systems:
List of High-risk AI systems (EP amendments)

Addition of several AI systems to the list, including:

- AI in the evaluation and classification of emergency calls
- AI to
- AI
- AI

> ”AI systems intended ***to evaluate and classify emergency calls by natural persons or*** to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by ***police and law enforcement,*** firefighters and medical aid***, as well as of emergency healthcare patient triage systems;”***

Deletion of several entries in the list, including:

- AI systems used by LEAs to detect deep fakes

High-risk AI systems:
List of High-risk AI systems (EP amendments)

Addition of several AI systems to the list, including:

- AI in the evaluation and classification of emergency calls
- AI to be used as safety components in the management and operational of critical digital infrastructure
- AI to be used for influencing the outcome of an election of referendum
- AI to be used by large social media platforms to recommend user-generated content available on the platform

Deletion of several entries in the list, including:

- AI systems used by LEAs to detect deep fakes

High-risk AI systems:
List of High-risk AI systems (General Approach)

- AI system which do not lead to a significant risk to the health, safety or fundamental rights should not be considered as high-risk.

High-risk AI systems:
List of High-risk AI systems (EC)

1. Biometric identification of people
2. Safety components in the management of critical infrastructure (road traffic, water, gas, heating & electricity)
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and public services and benefits
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes
9. AI used as safety component of certain products (incl. personal protective equipment & medical devices)

High-risk AI systems:
List of High-risk AI systems (EC)

1. Biometric identification of people
2. Safety components in the management ritical infrastructure (road traffic, water, gas, he tricity)
3. Education and vocational training
4. Employment, workers manag d access to self-employment
5. Access to and enjo essential private services and public service ts
6. Law enfo
7. Mig lum and border control management
8. ration of justice and democratic processes
9. A used as safety component of certain products (incl. personal protective equipment & medical devices)

These systems will not be banned

High-risk AI systems:
Framework for High-risk AI systems

1. Risk management system
2. Data and data governance
3. Technical documentation
4. Record-keeping
5. Transparency and provision of information to users
6. Human oversight
7. Accuracy, robustness and cybersecurity

High-risk AI systems: *Specific obligations*

- Providers
  - Quality Management System
  - Draw up technical documentation
  - Conformity Assessment
  - Keep the logs automatically generated
  - Cooperation with competent authorities
  - Appointment of legal representative

- Importers
- Distributors
- Users

High-risk AI systems: *Specific obligations*

- Providers
- Importers
- Distributors
- Users

High-risk AI systems: *Specific obligations*

- Providers
- Importers
- Distributors
- Users
  - Monitor the operation of the AI system
  - Keep the logs automatically generated

High-risk AI systems: *Specific obligations*

- Providers
- Importers
- Distributors
- Users
- *EP Amendment:* Provider of a foundation model

High-risk AI systems:

EU Database

- European Commission to set up a database for stand-alone high-risk AI systems.
- Mandatory registration
- Should be accessible to the public.

High-risk AI systems:
Additional provisions

- Appointment of national notifying authorities
- Adoption of common specifications, where standards don't exist.
- Conformity assessment procedures
- EU Declaration of Conformity
- CE Marking
- Reporting of serious incidents and of malfunctioning
- Registration in EU Database

5 Other provisions

Other provisions

Transparency obligations

- AI systems intended to interact with natural persons
- Emotion recognition system or biometric categorisation system
- Deep fakes: AI systems that generate or manipulate images, audio or video content that appreciably resembles existing persons, objects, places and would falsely appear to a person to be authentic

Exemption for detecting, preventing, investigating and prosecuting criminal offences.

Other provisions

Measures to support innovation

- AI Regulatory sandboxes
- Guidance to small-scale providers and users about the implementation of the regulation.

Other provisions

Governance

- European AI Board vs. European AI Office

- Role:
  - Lead the cooperation between national authorities
  - Guidance on emerging issues related to AI
  - Assist national authorities and the Commission in ensuring the application of the legislation

Other provisions

Code of conduct

- To be drawn up
- Voluntary
- Would relate to for instance: environmental sustainability, accessibility for persons with disability, stakehodlers participation in the design and development, diversity of development teams…

Other provisions

Penalties

- Responsibility of the Member States to lay down the rules on penalties.
- Administrative fines up to €30 million or up to 6% of total worldwide annual turnover.

Other provisions

Additional rules proposed by the Parliament

- Right to lodge a complaint with a national authority
- Right to explanation of individual decision-making
- Guidelines by the European Commission

Other provisions

Additional rules proposed by the Parliament

- Rules regarding providers of "generative AI" :
  - Comply with transparency obligations
  - Should not breach with EU fundamental values
  - Should not breach EU legislation on copyright

6 Next Steps

Next Steps

Procedure

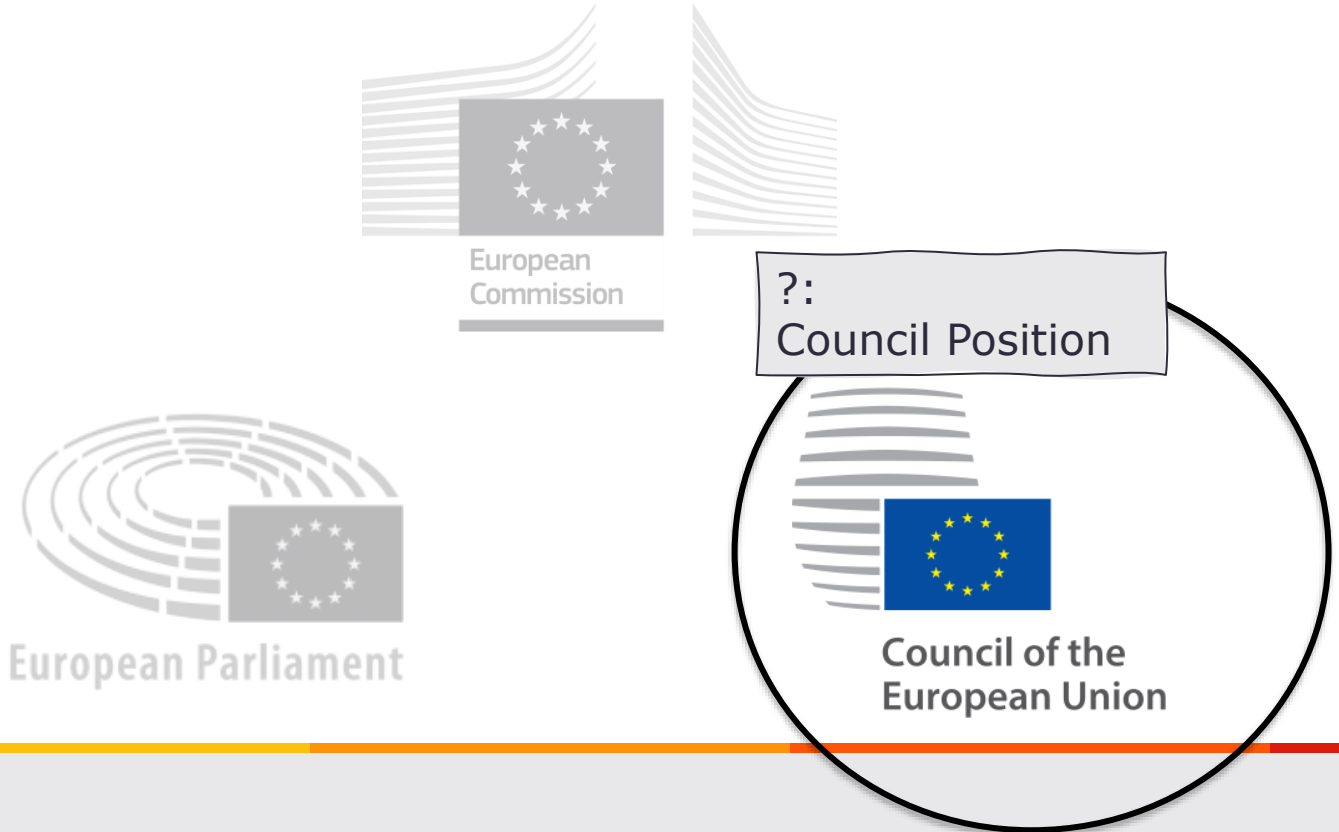
21/4/2021:
Publication of the proposal

14/6/2023:
Vote in 1st reading (+amendments)

9/12/2022:
General Approach

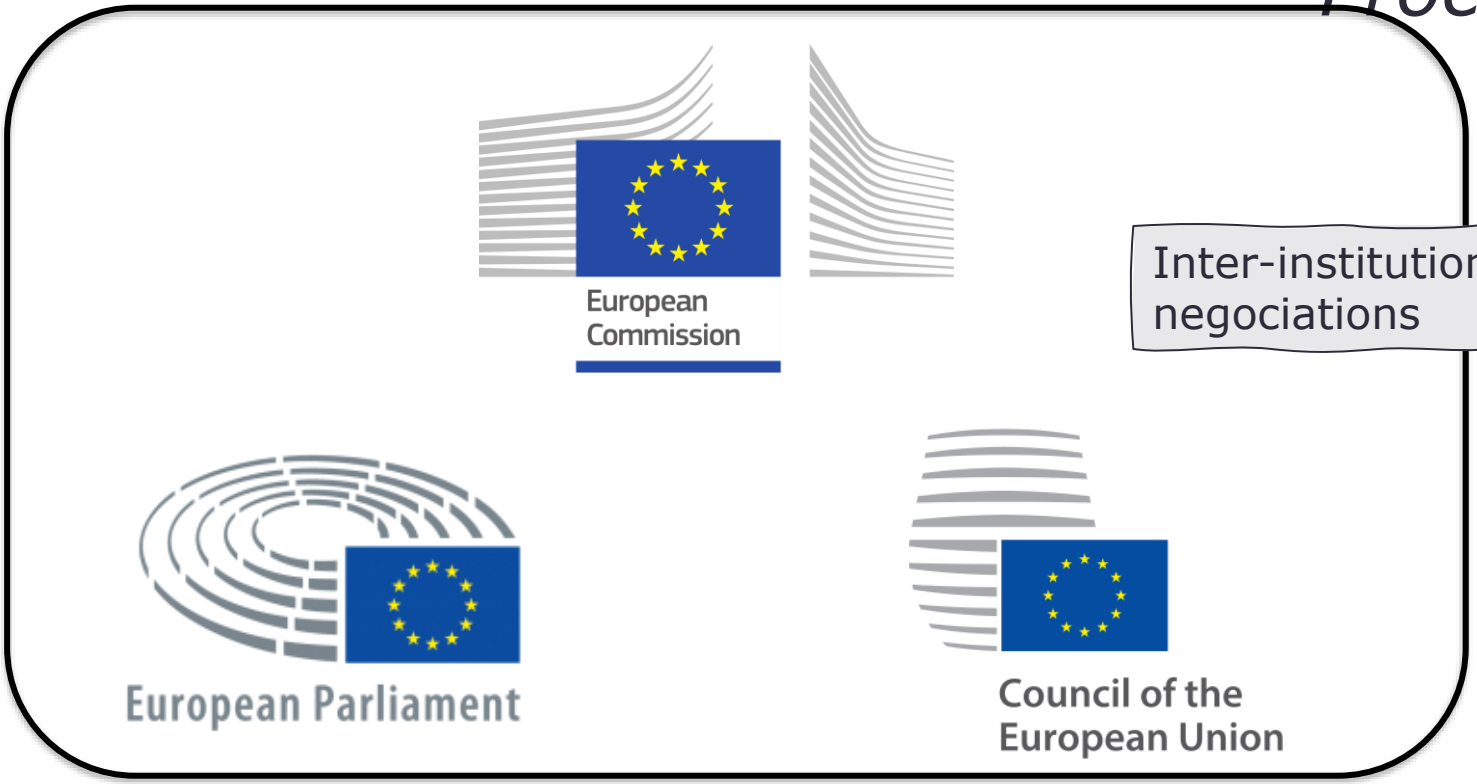
Next Steps

Procedure



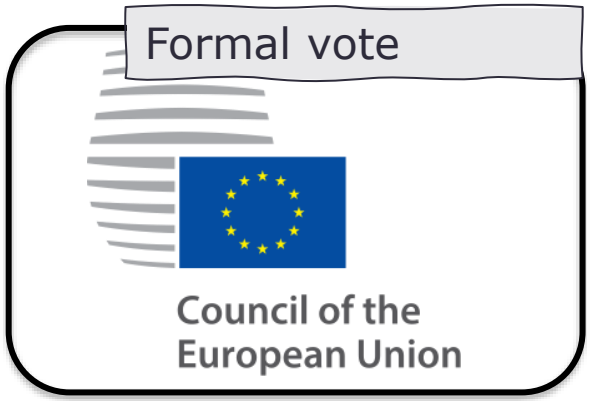
Next Steps

Procedure



Next Steps

Procedure



Next steps

Dates of entry into effect

- Entry into application:
  2 years after entry into force

To sum up

- AI will not be banned
- Some specific practices will be prohibited
- High-risk AI systems should come with specific protocols, documentation, strategies…
- Transparency obligations on some types of AI
- Legislative procedure is not finished yet

Useful links

- EU Commission Proposal – HERE
- EU Commission Proposal annexes – HERE

  Includes:
  - List of High-Risk AI systems (HRAIS)
  - Elements required in the technical documentation for HRAIS
  - EU Declaration of Conformity
  - Information to be submitted in the registration to the EU Database
- Council General Approach - HERE
- Amendments adopted by the European Parliament - HERE

CONTACT

Benoit VIVIER

Public Affairs Director, EENA

@ *bv@eena.org*

in *Benoit Vivier*