On April 21, 2021 the EU Commission published its proposal for an Artificial Intelligence Act.

Here is what you need to know:

1. Limited prohibited uses
2. Regulation of high-risk AI systems
3. Ex-ante/ex-post requirements
4. GDPR-trained?
5. What comes next?
The Regulation identifies a series of AI practices that are prohibited because they go against the EU values or because they violate EU individuals’ fundamental rights.

**PROHIBITED USES**

- Use subliminal techniques to materially distort behaviors and (likely) cause harm.
- Exploit vulnerabilities and (likely) cause harm.
- Use real-time remote biometric identification systems in public spaces for law enforcement purposes.
- Are used for social scoring by public authorities (or on their behalf).

The use of “real-time” remote biometric identification systems (such as facial recognition) in public spaces for law enforcement purposes will however be authorized if strictly necessary for:

1. Targeted search for victims
2. Prevention of specific, substantial and imminent threats or terrorist attacks
3. Detection, localization, identification or prosecution of a perpetrator or suspect of certain criminal offences
The proposal primarily focuses on high-risk AI applications and impose **stringent requirements on ‘providers’ and ‘users’ of AI applications**, as well as across the supply chain. In-scope uses are listed in 2 annexes.

**ANNEX II**

- AI systems used as products or safety component of products covered by sectorial Union law including, inter alia:
  - Transport
  - Medical devices
  - Radio equipment
  - Safety equipment
  - Machinery

**ANNEX III**

- Other high risk AI applications including, inter alia:
  - Biometric identification and categorization of natural persons
  - Management of critical infrastructure
  - Education and vocational training
  - Employment
  - Access to essential private and public services
  - Administration of justice

The lists should be updated by the EU Commission through delegated acts.

**Specific information requirements for other AI systems** that interact with humans; use emotion recognition or biometric categorization systems; or manipulate content (videos, images, etc.) to generate ‘deep fake’.
EX-ANTE REQUIREMENTS VETTED BY A CONFORMITY ASSESSMENT

Before the placement of AI systems on the market or their putting into service, high-risk AI systems should undergo a conformity assessment to ensure they are in line with the requirements of the Regulation.

- **Transparency obligations** – including mandatory information to be provided in users’ instructions
- **Use of high-quality datasets** for training and testing the system
- **Robustness, accuracy, and cybersecurity requirements** that should apply throughout the lifecycle
- **Risk management systems**
- **Documentation requirements**
- **Logging of activities** to ensure traceability of results
- **Human oversight** – appropriate human-machine interface tools for natural persons to prevent or minimize risks

What’s the process?

- Conformity assessment
- EU declaration of conformity + CE marking
- Registration in an EU database
- AI System put on the market / in service

EX-POST REQUIREMENTS

Post-market requirements (monitoring system, reporting of serious incidents and malfunctioning) and surveillance.
A REGULATION TRAINED WITH GDPR DATA?

Various elements of the Regulation echo the GDPR.

**EXTRATERRITORIAL SCOPE**
the Regulation seeks to apply to providers and users (even if based outside the EU) that place AI systems on the market or put them into service in the EU and to providers and users of AI systems where the output produced by the system is used in the EU.

**PRINCIPLE OF ACCOUNTABILITY**
amongst others, providers need to put in place a quality management system that ensures compliance with the Regulation and is documented through written policies and procedures and technical documentation.

**EU REPRESENTATIVE**
obligation for providers based outside the EU to appoint an authorized representative when an importer cannot be identified.

**INCIDENT NOTIFICATIONS**
ex-post obligations include the requirement to put in place a monitoring system and to notify the competent authorities in case of serious incidents or malfunctions in the systems within 15 days after they become aware of the breach.

**HIGH-FINES**
that can go up to 30 million or 6% of the total worldwide annual turnover of the preceding financial year.

**ENFORCEMENT**
empowered national supervisory authorities and a European Artificial Intelligence Board to supervise the consistent application of the Regulation and issue interpretative guidance.
The proposal will have to undergo the EU legislative process, which might take quite some time and lead to significant changes. In its current format, most provisions should apply 2 years after the entry into force of the Regulation.

The EU is shaking the AI ecosystem and stepping in as a key regulator. This competes with other ‘principles-based’ regional approaches, such as the US one. We will closely follow the developments of the Regulation to help understand how the “AI EU way” will play out.
AUTHORS

Diletta De Cicco
Associate
ddecicco@steptoe.com

Charles-Albert Helleputte
Partner
(Head of EU cybersecurity, data & privacy)
chelleputte@steptoe.com

OTHER CONTACTS

Charlotte Brett
Policy Advisor
cbrett@steptoe.com

Charles Whiddington
Partner
cwhiddington@steptoe.com

David O’Sullivan
Senior Counselor
dosullivan@steptoe.com

Paul Hughes
Of Counsel
phughes@steptoe.com

or your regular Steptoe contact

www.steptoe.com