The European AI Act and Its Relevance for NRENs

Magdalena Rzaca
SENIOR GDPR & IPR LEGAL ADVISOR, GÉANT ASSOCIATION
CIPM, CIPP/E, FIP, ISO 27001 LEAD AUDITOR

SIG AI Meeting - Prague
7/04/2025

Agenda

- EU AI Act
- Risk-based classification
- Focus on high risk
- EU AI Act roles
- Research & Open-Source Exemptions
- Sandboxes
- Fines
- Q&A

What is the European AI Act?

- First comprehensive AI legislation
- Introduces the first legally binding definition of AI systems
- Work started in 2020, final version adopted in 2024
- Risk-based approach to regulating AI

EU AI Act Risk-Based Classification

- **Four risk categories under the AI Act:**

1. ❌ **Unacceptable Risk** (Prohibited AI)

   AI systems that pose a clear threat to safety or rights (as for example: social scoring by governments, real-time biometric identification in public (with few exceptions), predictive policing based on profiling)

2. ⚠️ **High Risk**

   AI in critical sectors like education, law enforcement, healthcare, etc.

3. ⚙️ **Limited Risk**

   Systems like chatbots or deepfakes → must provide transparency to users

4. ✅ **Minimal Risk**

   Most uses of AI, including open-source tools and R&D experiments (e.g. AI spam filter)

Hidden game-changer: Annex III

Eight specific areas where AI systems are presumed to be **high-risk**, based on their **INTENDED** use including:

1. Biometric identification and categorization
2. Critical infrastructure (e.g. energy, transport)
3. Education and vocational training
4. Employment, workers management
5. Access to essential services
6. Law enforcement
7. Migration, asylum, and border control
8. Administration of justice

Annex III - details

1. Biometrics, in so far as their use is permitted under relevant Union or national law:

(a) remote biometric identification systems.
This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;

(b) AI systems **intended** to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;

(c) AI systems **intended to be used for emotion recognition**.

2. Critical infrastructure: AI systems **intended** to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.

Annex III - details (education & employment)

3. Education and vocational training:

(a) AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels;

(b) AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels;

(c) AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels;

(d) AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.

4. Employment, workers' management and access to self-employment:

(a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;

(b) AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

High risk systems obligations 1/2

Obligation	Article	What's Required
Risk Management System	Art. 9	Implement continuous risk identification, analysis, and mitigation across the lifecycle
Data and Data Governance	Art. 10	Use high-quality, representative, and unbiased data; ensure data traceability
Technical Documentation	Art. 11	Maintain up-to-date documentation proving compliance
Record-Keeping (Logging)	Art. 12	Ensure automatic logs are generated and stored for traceability and auditability
Transparency & User Information	Art. 13	Provide clear instructions and system descriptions to users

High risks systems obligations 2/2

Obligation	Article	What's Required
Human Oversight	Art. 14	Ensure systems are overseen and can be overridden by humans
Accuracy, Robustness, Cybersecurity	Art. 15	Build in resilience to faults, attacks, and ensure accuracy
Conformity Assessment	Arts. 16–20	Evaluate compliance before placing on the market (internal or third-party)
Post-Market Monitoring & Reporting	Arts. 61–62	Track performance, report serious incidents and risks
Registration in EU Database	Art. 51	Log high-risk AI systems in a public EU database before deployment

High risks systems – summary

High-risk designation under Annex III isn’t based on the tech itself—it’s based on **how and where it is intended to be used**.

For example: an AI model used to assess student performance in a university is **high-risk** if it influences access to education.

But the same model used in a research sandbox with no real-world impact may **not** be high-risk.

NRENs must understand not just **what AI systems are hosted**, but also **how they're used** and by **whom**. And remember about obligations.

Roles Under the AI Act – Who's Responsible for What?

Role	Definition	Key Obligations
Provider	Develops or places an AI system on the market or into service under their name	Design compliance (e.g. data, documentation, risk management)
Deployer	Uses an AI system in the EU for their own purposes	Ensure proper use, human oversight, monitor outputs
Importer	Places an AI system from a non-EU provider into the EU market	Ensure system complies before entering EU
Distributor	Makes the AI system available without changing it	Check conformity, forward documentation
User (natural person)	Individual using the AI system, e.g. teacher using a chatbot	Mostly exempt unless misuse is intentional

Possible roles of NRENs

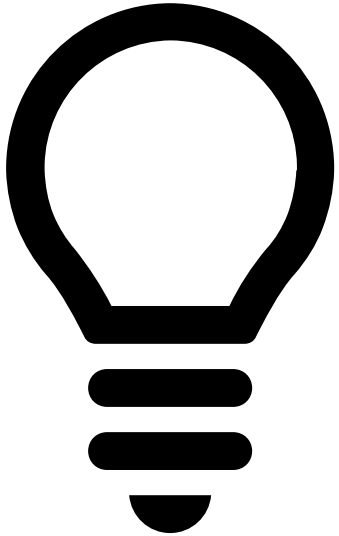
- **Providers** if they develop or co-develop AI tools or platforms.
- **Deployers** when they implement AI systems for managing their infrastructure or services.
- **Distributors** if they make AI tools developed elsewhere available to universities or research centers.

⚠ Each role carries **specific legal obligations** under the EU AI Act—especially for **high-risk systems**.

Understanding the roles

NREN-Specific Implications

- Running an AI-supported authentication system? → You're likely a **deployer**.
- Hosting or customizing an AI research tool used across universities? → You could be a **provider** or **distributor**.
- Collaborating on open-source AI? → Ensure **proper disclaimers** and documentation.



Research & Open-Source Exemptions

🔬 Scientific Research Exemptions (art. 2 (5) and recital 72)

- Exempts AI systems used **exclusively for research & development**
- Applies to **non-commercial R&D activities**
- As soon as AI is **put into service or affects real users**, **full obligations apply**

💻 Open-Source AI Exemptions (art. 2(6) and recital 73)

- Open-source AI models are partially exempt if **not placed on the market for a commercial purpose**
- Still must respect **transparency obligations** under **Article 52**, especially for **GPAI** models
- No exemption for **deployment in high-risk use cases**

🎓 Academic & Public Sector Flexibility (art. 53)

- EU Member States may **create AI regulatory sandboxes** that support institutions like **universities and public research bodies**
- These sandboxes allow **safe testing with guidance** from national regulators.

AI regulatory sandboxes

An **AI regulatory sandbox** is a **controlled environment** where organizations can **develop, test, and validate AI systems** under the **supervision of regulators — without immediately facing all legal obligations** of the EU AI Act.

🔍 Key Features:

- **Supervised by competent authorities** (e.g., national regulators, AI Office)
- Designed to **support innovation** while ensuring **compliance**
- Focuses especially on **high-risk or emerging AI applications**
- Helps providers understand **regulatory requirements early** in development

Sandboxes - benefits

🧪 How It Works:

- An organization (e.g., university, startup, NREN) applies to join a sandbox
- The AI system is tested in a **realistic but limited scope**
- Authorities give **feedback on risk, compliance, and documentation**
- Participants can **adjust their system** before full market deployment

🧠 Benefits for NRENs & Research Institutions:

- **Test AI solutions for research or infrastructure** without full liability
- Collaborate with regulators to shape **best practices**
- Explore ethical issues, data governance, and transparency early
- Ideal for **experimental tools** in education, health, cybersecurity, etc.

Fines: AI Act vs GDPR

Aspect	GDPR	EU AI Act
Max Fine (global)	€20 million or 4% of annual global turnover	€35 million or 7% of annual global turnover
Standard Fine Level	€10 million or 2% (for lesser violations)	€15 million or 3% (for lesser violations)
Basis of Fines	Data protection and privacy violations	Use of banned AI, non-compliance with rules
Examples of Violations	- Unlawful data processing - Consent issues - Data breaches	- Deploying prohibited AI (e.g., social scoring) - Failing to comply with high-risk obligations
Applicability	Data controllers and processors	AI system providers, deployers, importers, distributors

EU AI Office – since 21 February 2024

The **AI Office will guide interpretation and application of the Act**.

It will have a **central role in monitoring GPAI models** (like ChatGPT).

It may coordinate with **NRENs and research institutions**, especially those involved in AI testing, development, or deployment.

It promotes the development of trustworthy AI and supports innovation through AI regulatory sandboxes.

Q&A

Thank You!

Let’s connect: https://www.linkedin.com/in/magdalena-rzaca-fip/

Co-funded by
the European Union