GILLE HRABAL

protecting ideas since 1950

Newsletter

EU AI Act: Where Regulations Meets Patent Strategy

The EU AI Act has entered into force in August 2024. In this Newsletter, an overview of the most important things to know for overseas companies and attorneys is provided. The EU AI Act is not directly linked to the patent system, but synergies can be used due to the overlap of the EU AI Act requirements for documentation and transparency and the sufficiency requirements for AI patent

1. Background

- The European Union has established the world's first comprehensive, risk-based regulatory framework for artificial intelligence with the AI Act, which entered into force in August 2024. Its provisions will be phased in between 2025 and 2027. The Act also incorporates practical instruments such as support measures for small & midsized companies as well as regulatory sandboxes to facilitate implementation.
- In comparison, Korea, USA and China have adopted or are preparing policies on AI promotion, ethical principles, guidelines. However, to date, there is no regulatory framework with legally binding force comparable to that of the EU.

2. Purpose of EU AI Act:

The EU AI Act has been introduced to manage the risks of artificial intelligence, safeguard fundamental rights and safety, and enhance trust within the Single Market.

3. Direct applicability:

As a *Regulation*, it does not require transposition into national law. Member States are only required to designate supervisory and notifying authorities.

4. Who is affected:

It depends on the **Risk Category** of the concerned AI application, if certain regulative requirements for that AI application have to be fulfilled (see point 6.). The regulatory obligations under the EU AI Act primarily apply to *Providers*. The Act also applies to companies established outside the EU if they place AI systems on the Union market or if the output of such systems is used within the EU. *Users* likewise carry certain supervisory and transparency obligations when operating high-risk AI systems in practice.

5. Implementation timeline:

- Aug.2024: The AI Act entered into force.
- Feb. 2025: Prohibited practices and AI literacy obligations apply.
- Aug. 2025: Obligations for GPAI and governance measures apply
- Aug. 2026: Most general provisions apply.
- Aug. 2027: Transitional rules for high-risk systems and GPAI fully apply.

6. Risk Categories (EU AI Act):

The EU AI Act classifies AI systems into four risk categories as outlined below. Accordingly, companies must determine which category their systems fall under and understand the requirements applicable to each level.

- **Category: *Prohibited***

  Includes practices such as social scoring, exploitation of vulnerable groups, indiscriminate facial image scraping, emotion recognition in workplaces or schools, and remote real-time biometric identification in public spaces (with narrow exceptions).

- **Category: *High-risk***

  Classified as such when AI systems are safety components of products under Annex I of EU AI Act (e.g., machinery, medical devices) or fall within the use cases listed in Annex III of EU AI Act, including biometric identification, critical infrastructure, education, employment, law enforcement, migration and border control, and administration of justice or democratic processes.

  These systems must comply strict requirements: risk management, data governance, technical documentation (Annex IV of EU AI Act), record-keeping, transparency, human oversight, and accuracy, robustness, and cybersecurity.

  Exceptions may apply if the AI performs narrow procedural tasks, merely assists human decision-making, or does not materially influence the outcome.

- **Category: *Limited-risk***

  Subject to transparency obligations, such as requiring chatbots, deepfakes, and emotion recognition systems to inform users that they are interacting with AI or to clearly label synthetic content.

- **Category: *Minimal-risk***

  No additional obligations apply. Systems such as spam filters or gaming AI are encouraged to follow codes of good practice.

7. Conformity assessment

The EU AI Act is enforced through conformity assessment and market surveillance according to the risk level, with responsibilities shared between Member States and EU institutions.

Notified Bodies designated by Member States verify whether high-risk AI systems meet the legal requirements, while Market Surveillance Authorities handle corrective actions or withdrawals of non-compliant products.

The EU AI Office oversees and coordinates GPAI-related implementation and supports risk evaluation.

8. General Purpose AI (GPAI)

General Purpose AI (GPAI) is governed by the Code of Practice and the GPAI Guidelines, focusing on transparency, copyright, and safety/security. The Code of Practice aims to reduce administrative burdens for companies and enhance regulatory clarity.

Obligations for GPAI model providers will apply from August 2025, the European Commission's enforcement powers from August 2026, and existing models must comply by August 2027.

9. Synergies with Patent applications

The description of a European AI patent application requires according to the examination guidelines information on how the AI algorithm was trained and what data or input parameters were used for said training. Although the present examination practice of the EPO seems to be not so strict in this regard, increased requirements are expected for the future. Therefore, the documentation that is eventually required for the EU AI Act can also be used in part for the related patent application to avoid eventual complications during European examination. Moreover, disclosing details of the algorithm and how it works will become more important to obtain potentially distinguishing technical features for AI patent claims. Also in this regard, the documentation for the EU AI Act can be used synergistically as a source for drafting the description of the patent application.

Ingo Bauer, Ph.D. (WHUT)
Partner

bauer@dpat.de

www.dpat.de

Appendix: Key Requirements of the EU AI Act with Sector-Specific Examples

Requirement	Legal Basis (AI Act)	Practical Examples in Chemistry & Biotechnology	Practical Examples in Electrical, Electronic & Mechanical Fields
Risk Management System	Art. 9, Annex IV	• Drug discovery AI: identify and mitigate bias and safety errors in advance • Laboratory automation robots: simulate malfunction and risk scenarios	• Autonomous driving systems: simulate driving errors and control failures • Power grid AI: prepare for cyberattacks and system overloads
Data Governance	Art.10, Annex IV	• Clinical trial data: ensure diversity and reproducibility • Experimental results: labeling and error rate management	• Image recognition AI: document dataset sources and labeling • Manufacturing AI: manage missing data and establish validation procedures
Record-keeping / Logging	Art.12, Annex IV	• Laboratory AI: log inputs and results • Track differences between model versions	• Medical device AI: log decision times and human interventions • Manufacturing AI: maintain change logs during updates
Transparency Obligations	Art.13	• Diagnostic AI: disclose AI involvement to patients • Synthetic data use: mandatory disclosure	• Chatbots/Deepfake tools: clearly label AI-generated content • Recruitment/assessment AI: provide documentation on criteria and weighting
Human Oversight	Art.14	• Diagnostic AI: final decision by medical professionals • Risk signals: manual review procedures	• Law enforcement facial recognition: co-review by experts • Industrial AI: override or stop function available
Accuracy, Robustness & Cybersecurity	Art.15	• Robustness tests for experimental data variability and noise • Encryption to secure clinical datasets	• Adversarial attack simulations • Cybersecurity controls in manufacturing and IoT
Quality Management System (QMS)	Annex IV, Art.17	• Document QA processes in experiments • External expert validation and audit • Researcher training on AI ethics	• Document QA in development processes • Internal/external technical audits • Operator training on security and risk awareness
Pre- & Post-market Evaluation and Incident Reporting	Art. 61–63	• Diagnostic AI: post-market clinical monitoring and adverse event reporting • Verify safety after system updates	• Autonomous driving/manufacturing AI: accident reporting and performance monitoring • Re-verify safety after software patches