

Digital Omnibus on AI

An update on
EU AI legislation

Michael Löffler

23.06.2026



Funded by



EuroHPC
Joint Undertaking



**Co-funded by
the European Union**

 **Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria**

under discussion with



AI Factory Austria AI:AT has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101253078. The JU receives support from the Horizon Europe Programm of the European Union and Austria (BMIMI / FFG).

AI Factory Austria AI:AT – PUBLIC



AI Factory Austria AI:AT - Consortium

Disclaimer:

The speakers are solely sharing their personal experiences. Therefore, this talk is no substitute for professional/legal advice.

Beneficiaries



Affiliated Entities



Agenda

01 Introduction & Timeline

Legislative process, NLF alignment, and key deferred application dates.

02 General Changes

SMC definitions, capped fines, bias correction, and regulatory sandboxes.

03 Prohibited AI Practices

Banned systems under Article 5, synthetic nudification, and CSAM prohibitions.

04 High Risk AI

Safety components, Article 6(1) and Annex III, and revised deadlines.

05 AI Literacy

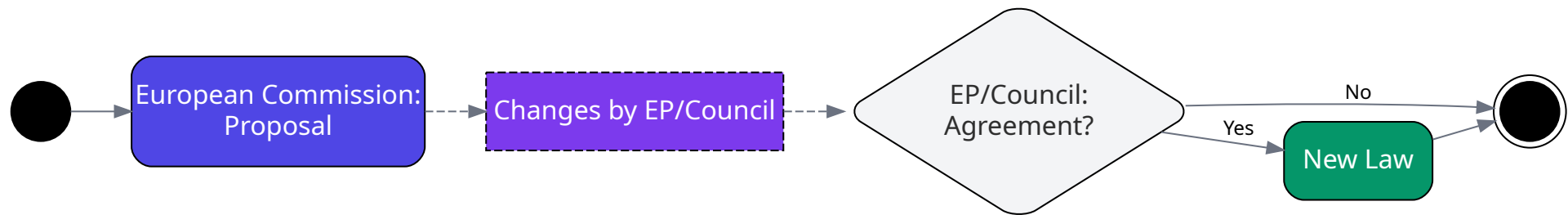
Mandatory organizational obligations under Article 4 for staff competence.



Timeline Update: The political agreement of 16.06.2026 postpones key application dates, aligning the AI Act's enforcement timeline with NLF harmonization.

AI Factory Austria AI:AT - PUBLIC – Michael Löffler

How EU Legislation Becomes Law



The AI Act Uses Europe's Proven Product Safety Framework

01



Essential Requirements

Safety goals, not technical instructions.

02



Harmonised Standards

CEN/CENELEC standards grant a **presumption of conformity**.

03



Conformity Assessment

Self-assessment or **Notified Body** testing, depending on risk.

04



CE Marking

Free movement **across the entire EEA**.



Significance of Harmonised Standards

Harmonised standards provide providers with concrete technical solutions for legally secure implementation.

LEGAL



Presumption of Conformity

Compliance with standards published in the EU Official Journal creates a **legal presumption** that regulatory requirements are met.

PRACTICAL



Ease of Proof

Acts as the primary mechanism for providers to demonstrate compliance with the Act's complex requirements in a structured way.

PROCEDURE

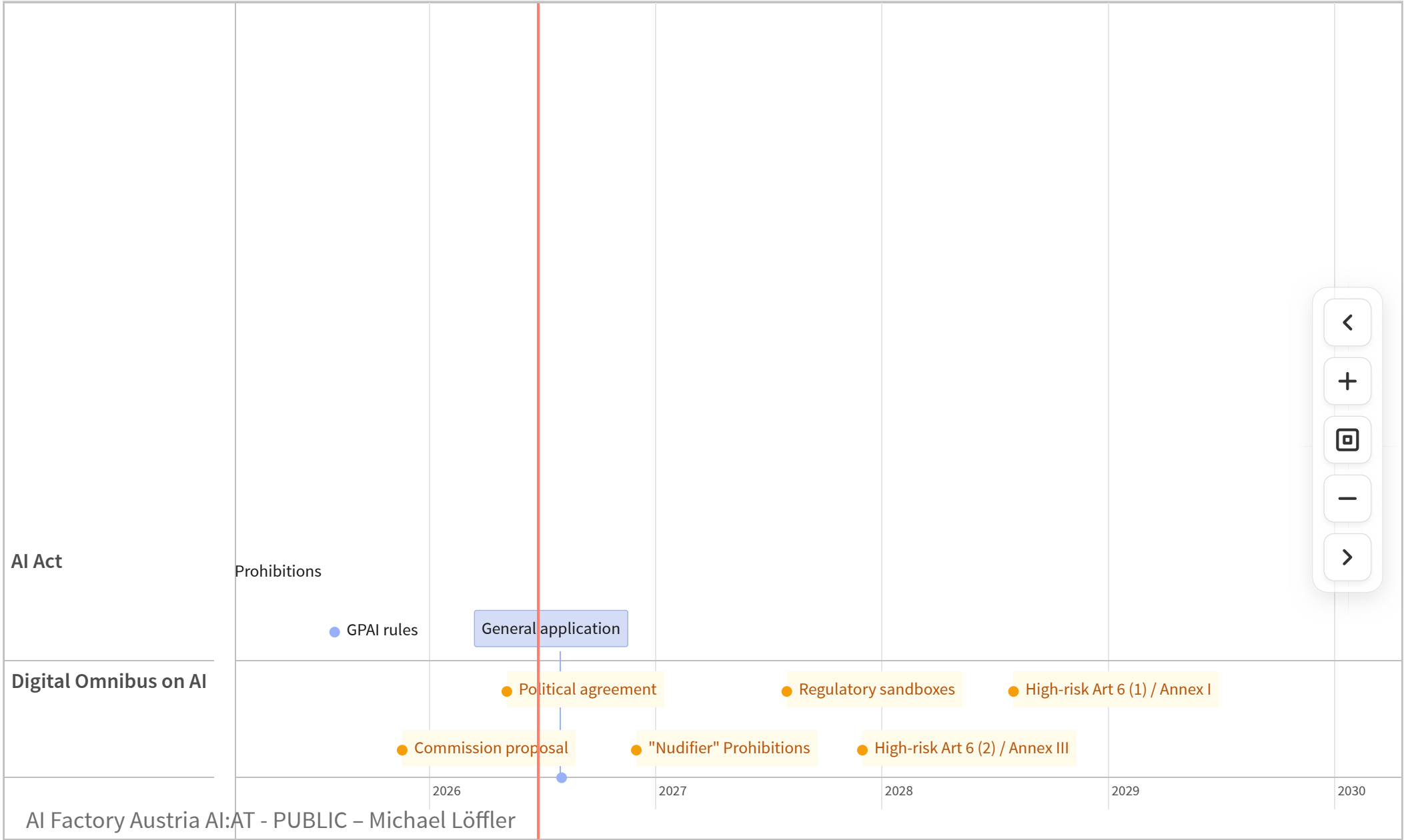


Impact on Assessment

Full application often enables simpler internal control procedures instead of mandatory external audits by Notified Bodies.



AI Act & Digital Omnibus: Key Dates



Timeline Adjustments

ART. 5 PROHIBITIONS

Prohibitions (Ch. I & II)

CURRENT LEGAL TEXT

Apply from 2 February 2025



POLITICALLY AGREED TEXT

Apply from 2 February 2025, **except new deepfake & CSAM prohibitions** (Art 5(1)(ba), (bb)) which apply from 2 December 2026.

ART. 57(1) SANDBOXES

Regulatory Sandboxes

CURRENT LEGAL TEXT

At least one national sandbox operational by 2 August 2026



POLITICALLY AGREED TEXT

At least one national sandbox operational by 2 August 2027

CH. III HIGH-RISK

High-Risk Obligations

CURRENT LEGAL TEXT

Apply from 2 August 2027 for all systems



POLITICALLY AGREED TEXT

Split application:

- **Annex III (Standalone): 2 December 2027**
- **Annex I (Embedded): 2 August 2028**

General Changes

01 Introduction & Timeline

Legislative process, NLF alignment, and key deferred application dates.

02 General Changes

SMC definitions, capped fines, bias correction, and regulatory sandboxes.

03 Prohibited AI Practices

Banned systems under Article 5, synthetic nudification, and CSAM prohibitions.

04 High Risk AI

Safety components, Article 6(1) and Annex III, and revised deadlines.

05 AI Literacy

Mandatory organizational obligations under Article 4 for staff competence.



Governance & Scope: Standardized definitions for Small Mid-Caps (SMCs) limit maximum fines, while new rules clarify bias correction data processing and national sandboxes.

Small Mid-Cap Enterprise (SMC)

Criterion 1



Staff Count Thresholds

SMC Range: ≥ 250 to < 750 staff

Criterion 2 (OR)



Financial Thresholds

Annual turnover: $> \text{EUR } 50\text{m}$ to $\leq \text{EUR } 150\text{m}$

— OR —

Annual balance sheet: $> \text{EUR } 43\text{m}$ to $\leq \text{EUR } 129\text{m}$

Fines & Needs of SMCs

Art 99 (6a)



Capped Penalties

For SMCs, each fine of the AI Act shall be up to the percentages or amount referred therein, **whichever is lower**.

General Principle



Equal Consideration

The specific interests and **needs of SMCs** shall be taken into account in the same way as those of SMEs.

Bias Detection & Correction

Art 4a (2) Scope



Exception Scope

Providers and deployers **of other AI systems/models** and deployers of high-risk AI systems may exceptionally process special categories of personal data.

Condition (a)



Strict Necessity

Processing must be **strictly necessary** to ensure bias detection and correction in view of biases likely to affect health/safety, fundamental rights, or lead to prohibited discrimination.

Condition (b) & Duty



Safeguards & No Duty

All legal safeguards must be applied. This paragraph **does not create any obligation** to conduct such bias detection and correction.

This legal basis was originally only available for providers of certain high-risk AI systems.

AI Regulatory Sandbox: Definition

Art. 3(55) Framework



Controlled Framework

Established by a **competent authority** to offer providers and prospective providers a safe, structured space for innovation.

Activities



Lifecycle Capabilities

Offers the possibility to **develop, train, validate, and test** innovative AI systems, including in real-world conditions where appropriate.

Parameters



Sandbox Governance

Operates pursuant to a specific **sandbox plan** for a limited time and strictly under regulatory supervision.

Union-Level Sandbox

GPAI



Union-Level Sandbox

The **AI Office** may establish a sandbox at the Union level for AI systems based on General-Purpose AI (GPAI) models developed by the same provider.

Cooperation



Joint Supervision & Access

Implemented in close cooperation with competent authorities, providing **priority access** to SMEs, start-ups, and Small Mid-Caps (SMCs).

Sovereignty



Member State Sandboxes

Established **without prejudice** to the competences of Member States to establish and supervise sandboxes under their national authority.

Prohibited AI Practices

01 Introduction & Timeline

Legislative process, NLF alignment, and key deferred application dates.

02 General Changes

SMC definitions, capped fines, bias correction, and regulatory sandboxes.

03 Prohibited AI Practices

Banned systems under Article 5, synthetic nudification, and CSAM prohibitions.

04 High Risk AI

Safety components, Article 6(1) and Annex III, and revised deadlines.

05 AI Literacy

Mandatory organizational obligations under Article 4 for staff competence.



Compliance Warning: AI systems falling under prohibited practices face the highest category of fines under the AI Act (up to €35 million or 7% of global turnover).

PROHIBITED AI PRACTICES



AI-generated

Prohibition of “nudifier” apps

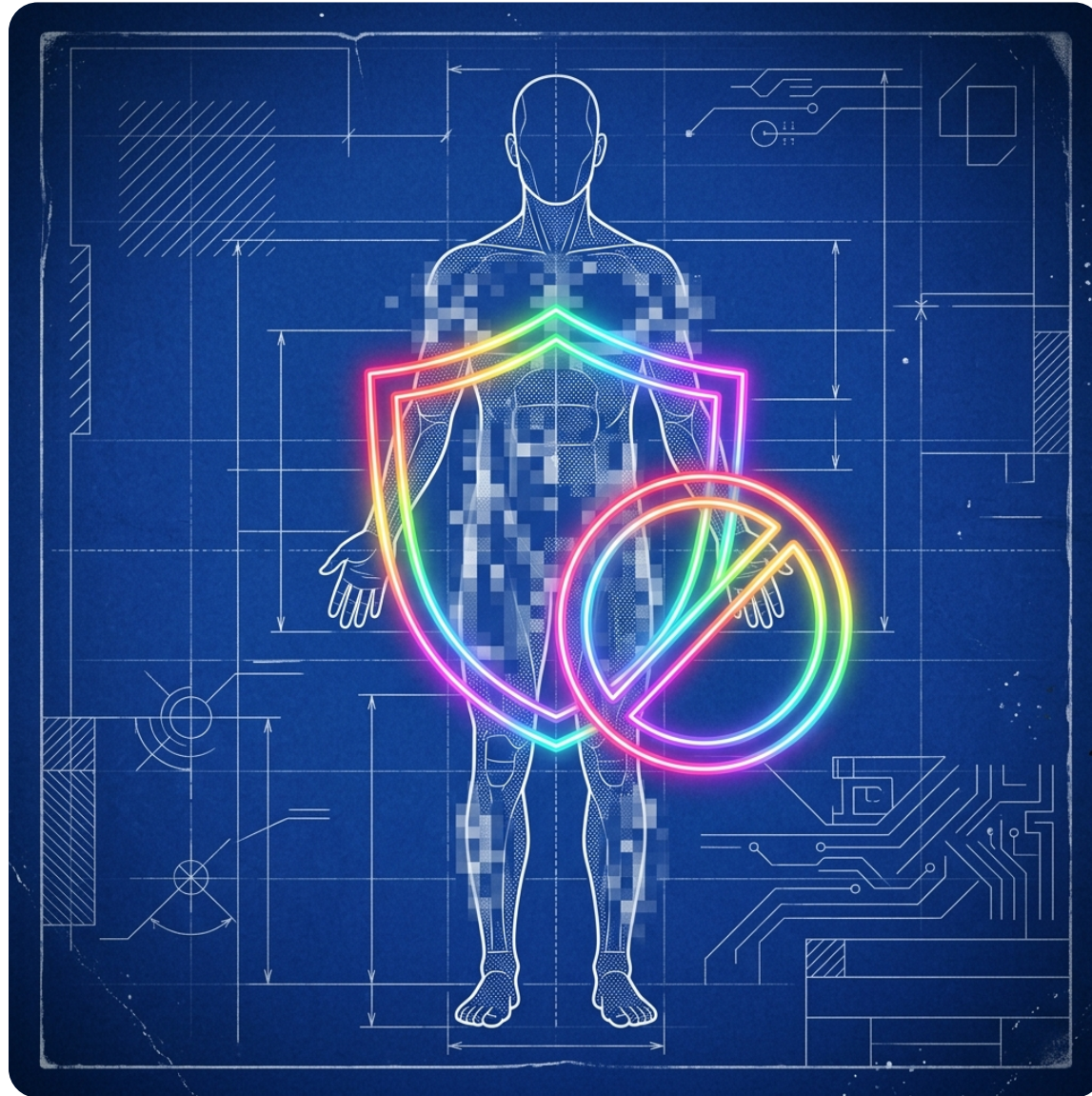


Image: AI-generated

NO CHILD PORNOGRAPHY

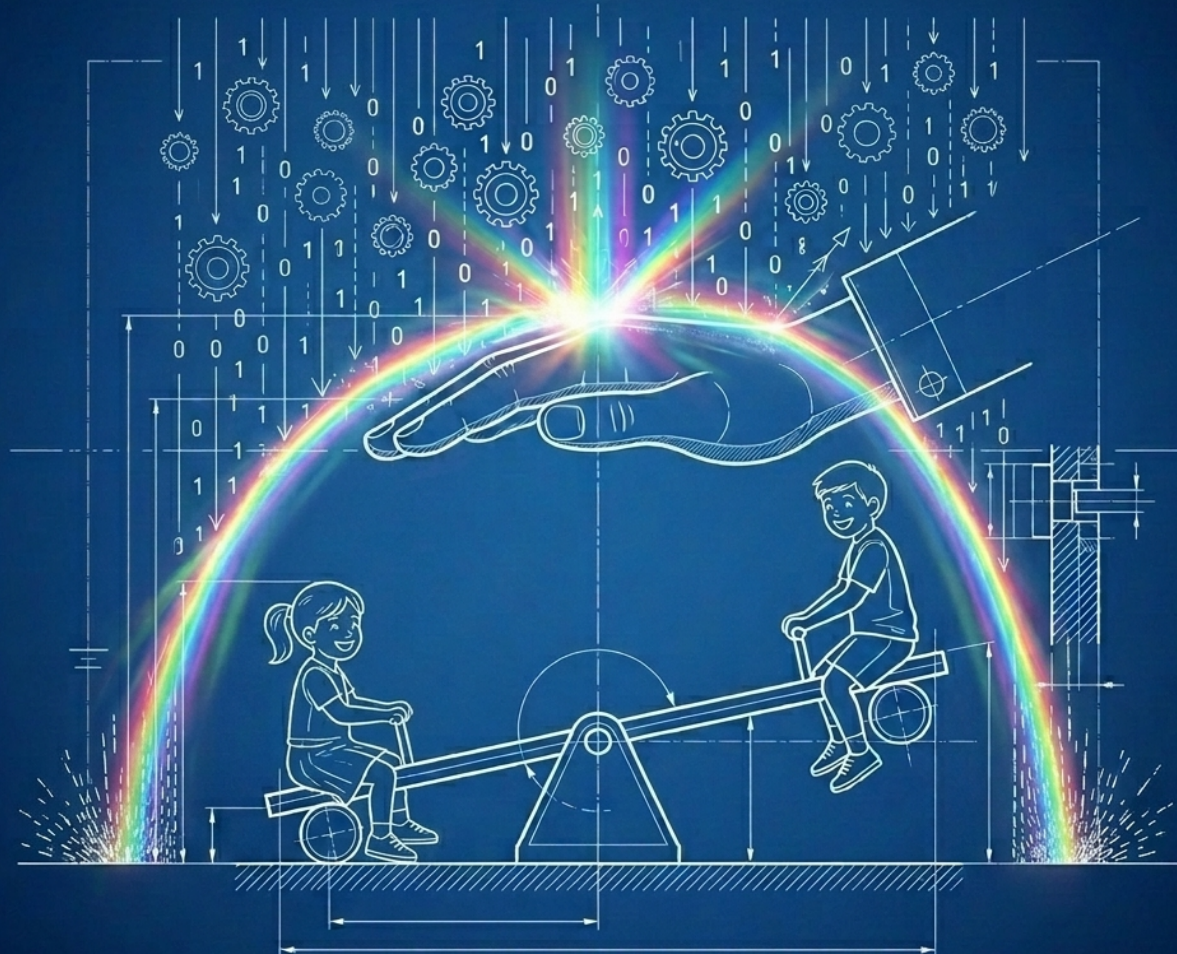


Image: AI-generated

High Risk AI

01 Introduction & Timeline

Legislative process, NLF alignment, and key deferred application dates.

02 General Changes

SMC definitions, capped fines, bias correction, and regulatory sandboxes.

03 Prohibited AI Practices

Banned systems under Article 5, synthetic nudification, and CSAM prohibitions.

04 High Risk AI

Safety components, Article 6(1) and Annex III, and revised deadlines.

05 AI Literacy

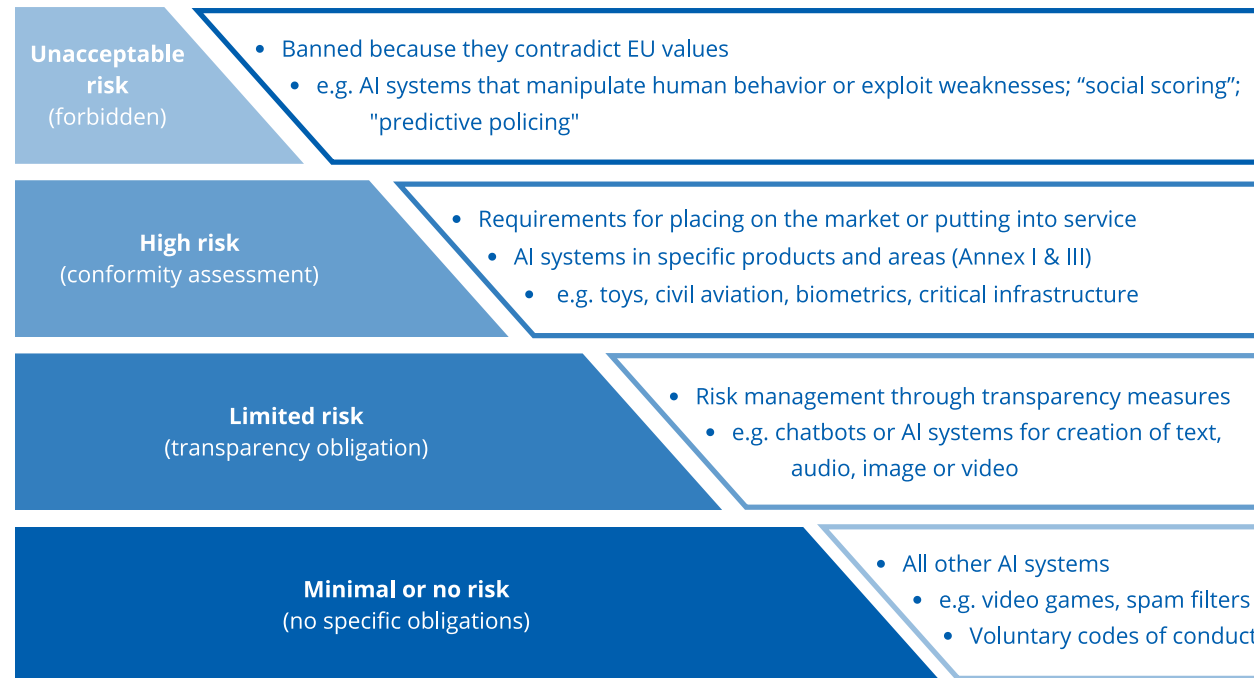
Mandatory organizational obligations under Article 4 for staff competence.



High-Risk Framework: Tightened safety component criteria under Article 6(1) and Annex III, with extended 36-month transition periods for product integration.

AI Act: Risk levels for AI systems

Not all AI systems fall into the regulated area - the higher the risk, the stricter the rules

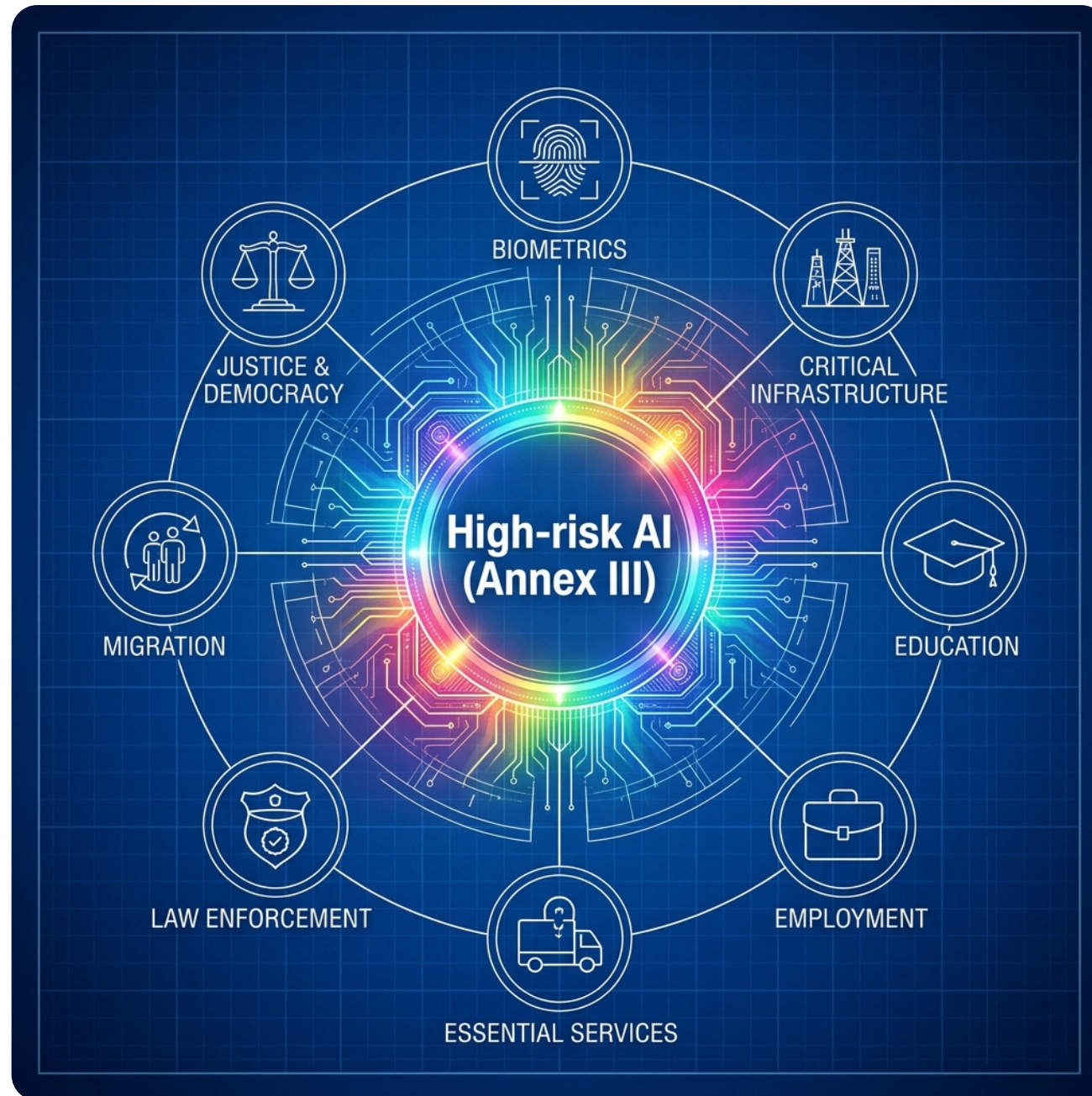


AI Service Desk

ai.rtr.at



Image: RTR: Risk Levels of the AI Act¹



AI-generated

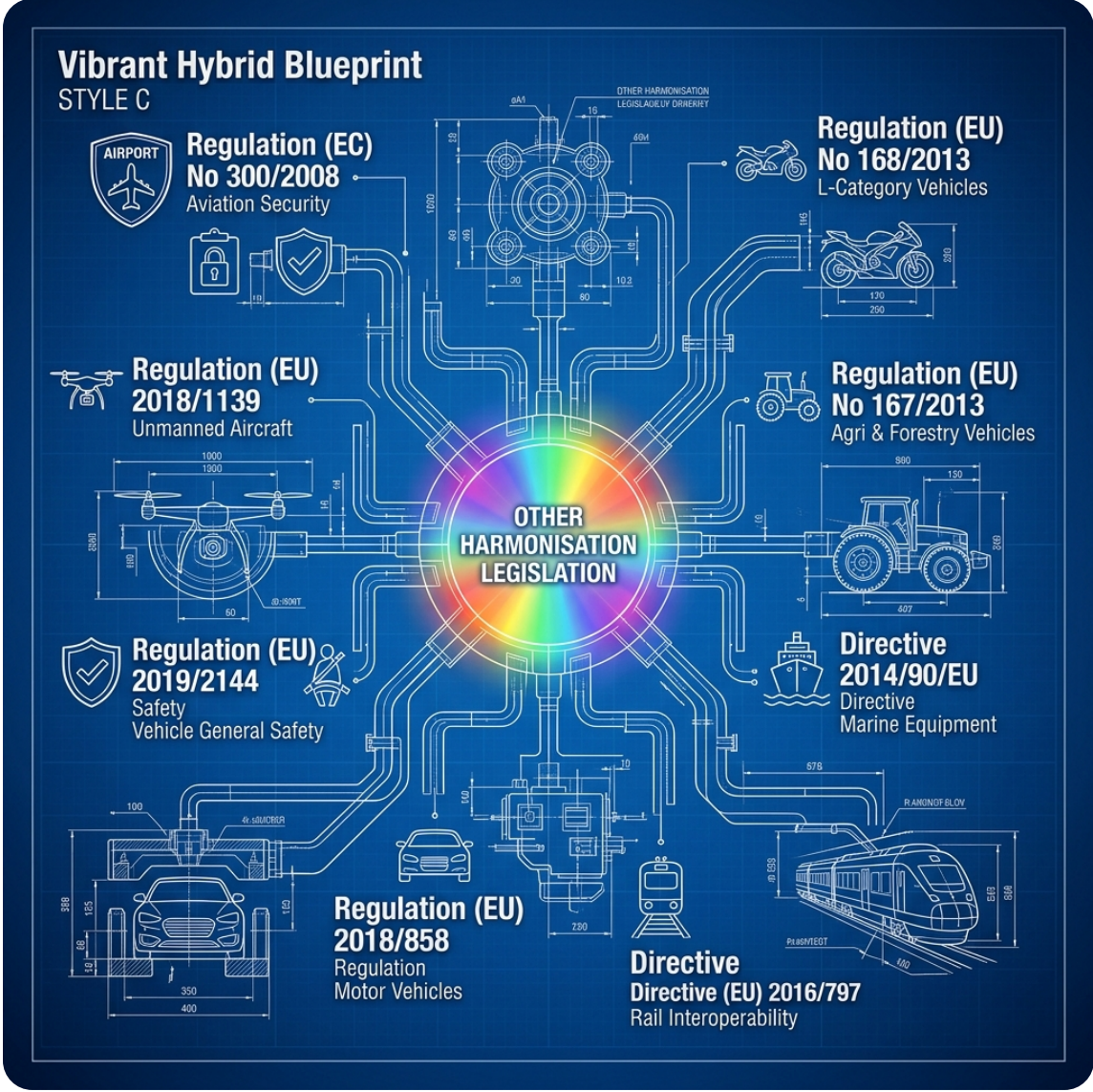
AI Act Annex I



AI-generated



AI Act Annex I



AI-generated

AI Act: Deployer obligations

The scope of obligations decreases according to the risk classification of the AI system

	High risk AI system	AI system limited risk	AI System minimal risk
AI literacy	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 26 (11)	Art. 50 (3), (4)	
Use of the AI system according to the instructions for use	Art. 26 (1), (3), (4)		
Human oversight	Art. 26 (2)		
Monitoring of the AI system	Art. 26 (5)		
Reporting of serious incidents	Art. 26 (5), 73		
Record-keeping	Art. 26 (6)		
Where relevant, data protection impact assessment	Art. 26 (9)		
Cooperation with competent national authorities	Art. 26 (12)		
Right to explanation of individual decision-making	Art. 86 (1)		
Information towards employee representatives <i>if employer uses high-risk AI systems in the workplace</i>	Art. 26 (7)		
Registration obligations <i>if EU institutions, EU bodies and other EU agencies</i>	Art. 26 (8), 49		
Authorisation by a judicial or administrative authority <i>if AI-system is used for post-remote biometric identification</i>	Art. 26 (10)		
Fundamental rights impact assessment <i>if i.a. public bodies and private entities provide public services</i>	Art. 27		

Image: RTR: Deployer Obligations¹

AI Act: Provider obligations

The scope of obligations decreases according to the risk classification of the AI system/AI model

	High risk AI system	GPAI model systemic risk	GPAI model	AI system limited risk	AI system minimal risk
AI literacy	Art. 4	Art. 4	Art. 4	Art. 4	Art. 4
Transparency towards downstream actors	Art. 13	Art. 55 (1)	Art. 53 (1) b	Art. 50 (1), (2)	
Data requirements	Art. 10	Art. 55 (1)	Art. 53 (1) c, d		
Technical documentation	Art. 11	Art. 55 (1)	Art. 53 (1) a		
Cooperation with authorities	Art. 21	Art. 55 (1)	Art. 53 (3)		
Appointment of authorized representative (if third country)	Art. 22	Art. 55 (1)	Art. 54		
Risk management	Art. 9	Art. 55 (1) a, b			
Accuracy, robustness and cybersecurity	Art. 15	Art. 55 (1) d			
Registration resp. notification obligations	Art. 49	Art. 52 (1)			
Reporting obligations to authorities	Art. 73	Art. 55 (1) c			
Record-keeping	Art. 12				
Implementation of human oversight tools	Art. 14				
Labelling requirements	Art. 16 b				
Ensuring accessibility requirements	Art. 16 l				
Quality management	Art. 17				
Documentation and log-keeping	Art. 18, 19				
Corrective actions	Art. 20				
Conformity assessment procedure, -declaration, -marking	Art. 43, 47, 48				

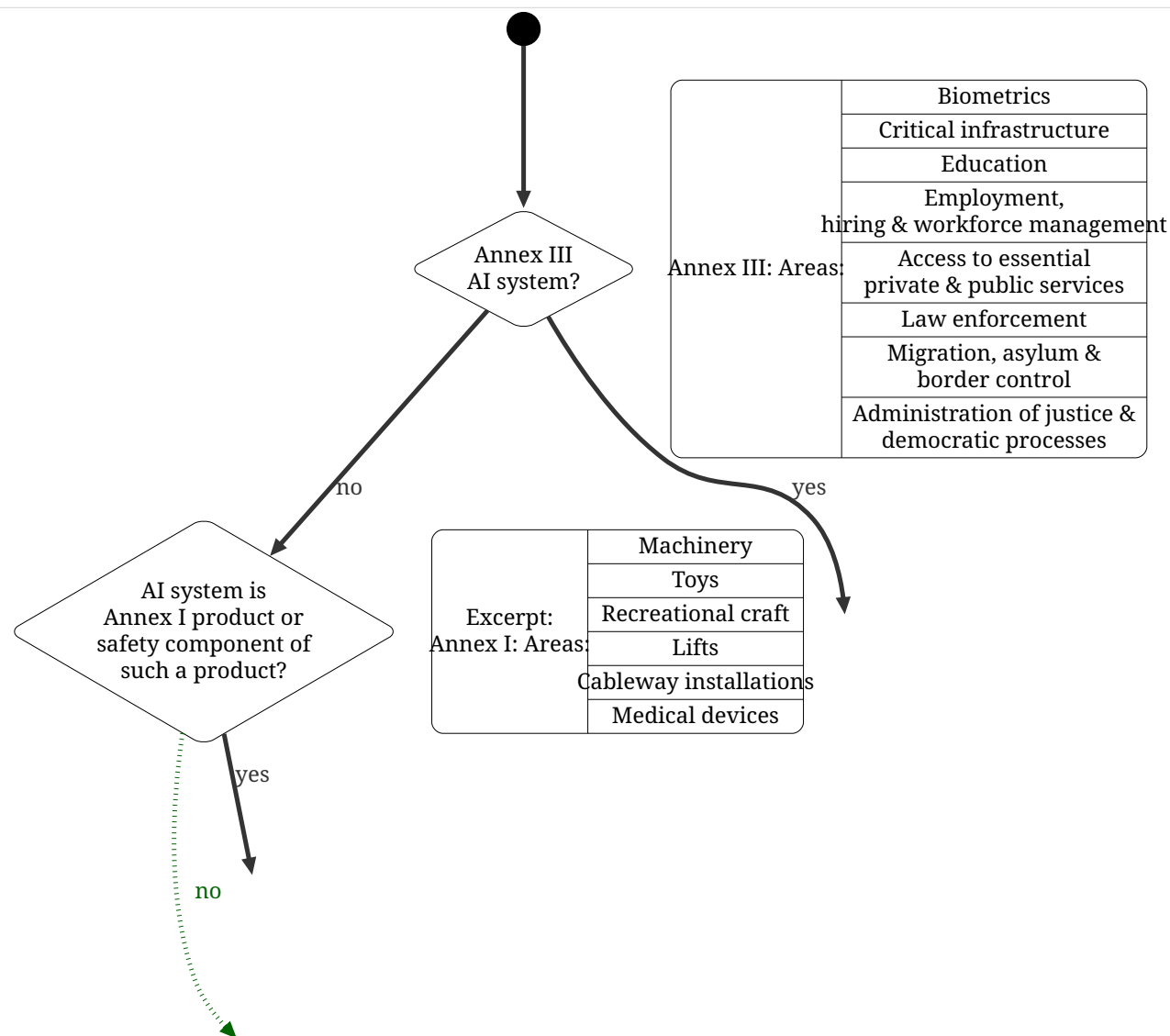
AI Service Desk

ai.rtr.at



Image: RTR: Provider Obligations¹

How to Classify High-Risk AI

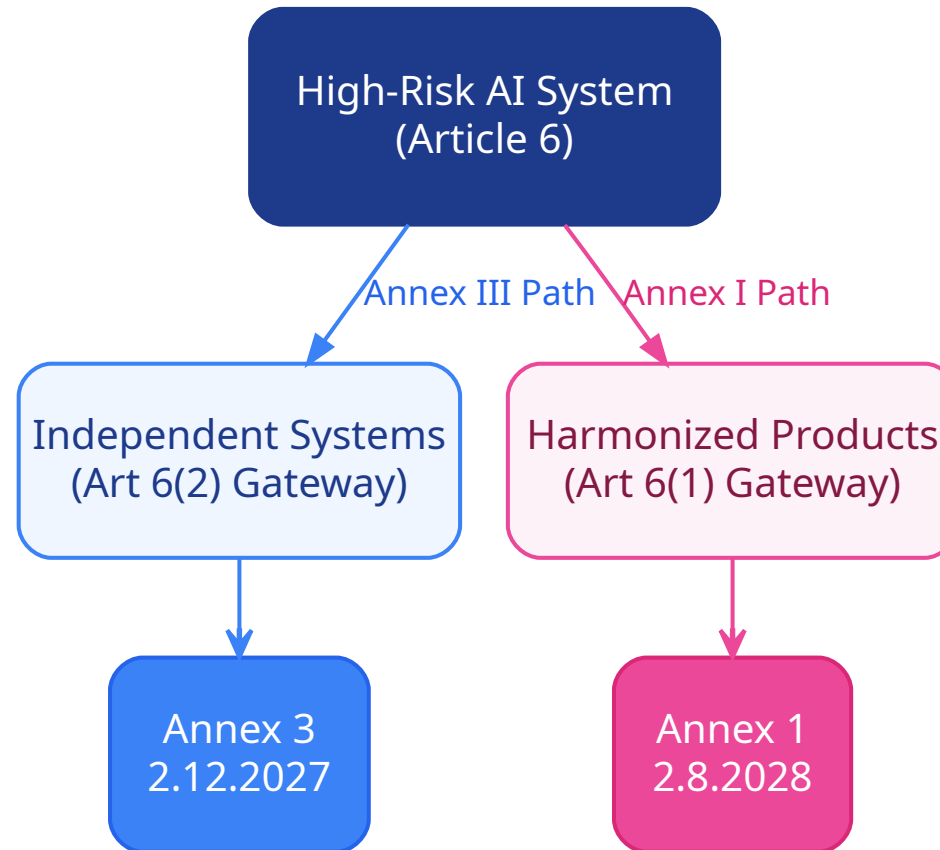


Classification scheme for High-risk AI systems (Art 6 AI Act)

[Reset Workflow](#)

[Reveal completely](#)

High-Risk AI Deadlines



High-Risk AI: Article 6(1) Gateway

An AI system is classified as high-risk under Article 6(1) if both of the following conditions are met:

Condition (a)



Product or Safety Component

The AI system is itself an Annex I product, or is intended to be used as a **safety component** of a product covered by the Union harmonisation legislation listed in Annex I.

Condition (b)



Conformity Assessment

The product or the AI system itself is required to undergo a **third-party conformity assessment** for placing on the market or putting into service pursuant to Annex I legislation.

Safety Component: Scope Clarification

ART 3(14) AI ACT

(14) 'safety component' means a component of a product or of **a** system which fulfils a safety function for that product or system, or the failure or malfunctioning of which endangers the health and safety of persons or property;

DIGITAL OMNIBUS

(14) 'safety component' means a component of a product or of **an AI** system which fulfils a safety function for that product or **AI** system, or the failure or malfunctioning of which endangers the health and safety of persons or property; **for the purposes of this definition, a component fulfils a safety function where its intended purpose is to prevent or mitigate risks to health and safety of persons or property;**

AI Literacy

01 Introduction & Timeline

Legislative process, NLF alignment, and key deferred application dates.

02 General Changes

SMC definitions, capped fines, bias correction, and regulatory sandboxes.

03 Prohibited AI Practices

Banned systems under Article 5, synthetic nudification, and CSAM prohibitions.

04 High Risk AI

Safety components, Article 6(1) and Annex III, and revised deadlines.

05 AI Literacy

Mandatory organizational obligations under Article 4 for staff competence.



Staff Training: Article 4 mandates that providers and deployers support AI literacy among staff, promoting understanding of operational risks and system limitations.

AI Factory Austria AI:AT - PUBLIC – Michael Löffler

AI Literacy: Legal Definition

Art. 3(56) Core



Core Capabilities

AI Literacy means the **skills, knowledge, and understanding** required to interact with AI responsibly.

Empowered Actors



Empowered Stakeholders

Enables **providers, deployers, and affected persons** to navigate their respective rights and obligations.

Dual Purpose



Double Objective

Allows **informed deployment** of AI systems, while building awareness of opportunities, risks, and potential harm.

AI Literacy: “Ensure” → “Support”

ART 4 AI ACT

Providers and deployers of AI systems shall take measures to ~~ensure, to their best extent, a sufficient level~~ of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

POLITICAL AGREEMENT

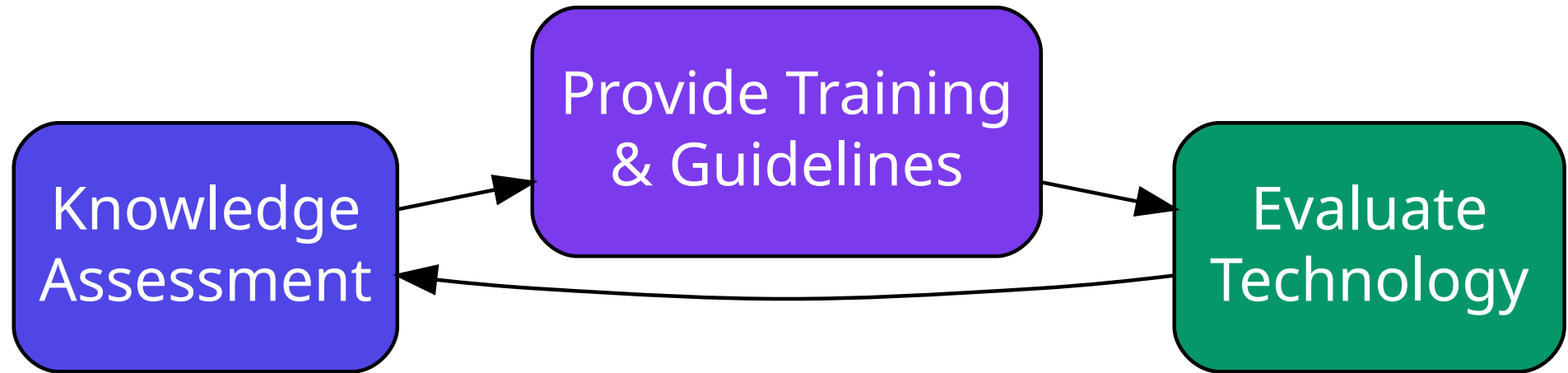
1. Providers and deployers of AI systems shall take measures to support the development of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used. This obligation does not require providers or deployers to guarantee any specific level of AI literacy of any individual.

2. The Commission and the Member States shall support and facilitate the efforts of providers and deployers of AI systems, in particular SMEs, in fulfilling their obligation under paragraph 1 of this Article. For that purpose, the Commission shall publish practical examples of how to comply with that obligation on the single information platform referred to in Article 62(3), point (b).

3. The Board shall adopt recommendations, taking into account European competence frameworks, to support the Commission and Member States in the promotion of AI literacy required under paragraph 1, including by setting out common objectives.

AI Literacy Drives Compliance and Competitive Advantage

The real driver is utility: People must understand AI to use it safely and effectively.



Digital Omnibus on AI: Summary



Contact



michael-löffler

Michael Löffler

Lead Legal, Regulatory and Ethics
AI Factory Austria AI:AT

+43 664 883 906 92

michael.loeffler@ai-at.eu

Karl-Farkas-Gasse 22, 1030 Wien

References

Council of the European Union, [Proposal for a regulation of the European Parliament and of the Council as regards the simplification of the implementation of harmonised rules on artificial intelligence](#), Letter sent to the European Parliament, 05/13/2026

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), AI Act: Deployer Obligations, https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Deployer_obligations.en.html, aufgerufen am 10/20/2025

—, Provider obligations in the AI Act, https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/Provider_obligations.en.html, aufgerufen am 10/20/2025

AI Factory Austria AI:AT

Digital Omnibus on AI
2026

Krisztina Rozgonyi DDr

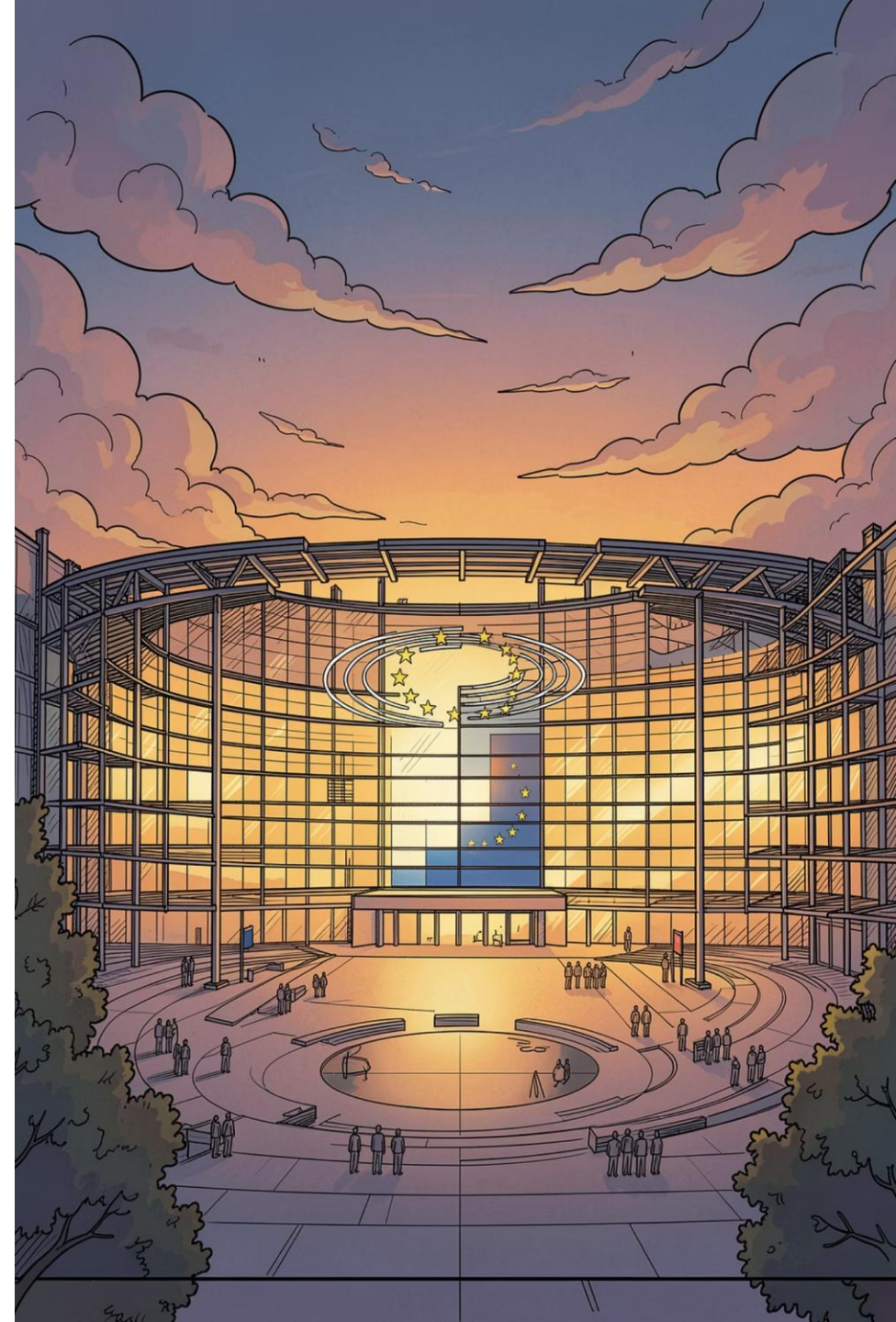
23.06.2026



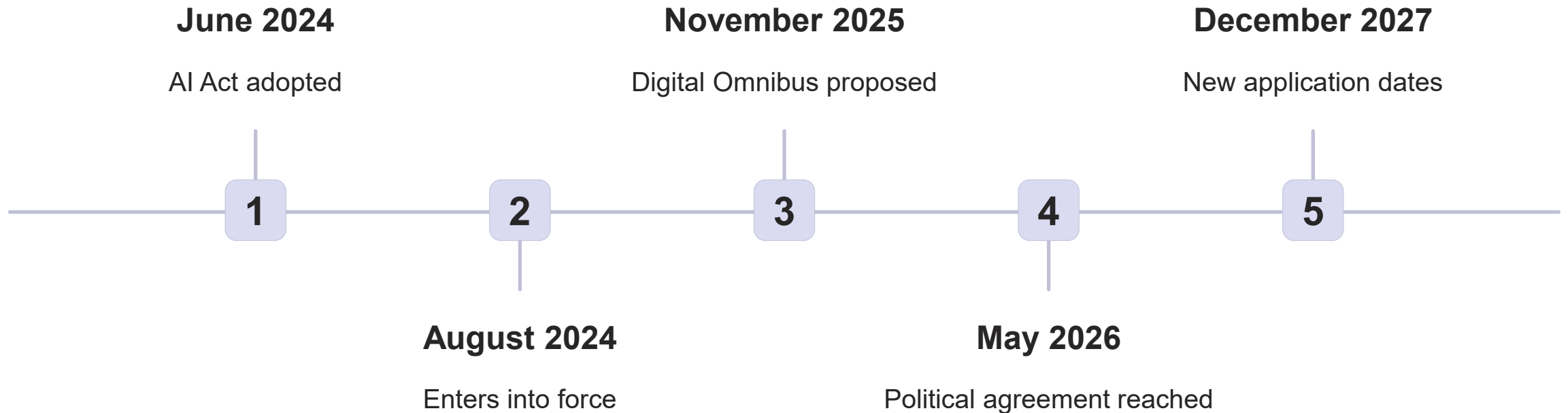
The Digital Omnibus on AI

Simplification, Competitiveness, or a Recalibration of European AI Governance?

The Omnibus is not merely a technical amendment package. It may signal a broader shift in the European approach to AI governance.



Why Is the AI Act Already Being Revised?



❓ Most high-risk obligations are not yet applicable. Why reopen Europe's flagship AI regulation before it has even entered into application?

Europe's Competitiveness Debate

Influential Developments

- **Letta Report (2024)** — Completing the Single Market
- **Draghi Report (2024)** — European competitiveness strategy
- **Competitiveness Agenda/Compass (2025)** — Growth and innovation priorities
- **Digital Sovereignty Agenda/ AI continent action plan (2025)** — Strategic autonomy in technology

Core Concern

Europe regulates successfully (i.e. GDPR regulatory spill-over). But can Europe **innovate and scale** successfully?

The Omnibus sits at the intersection of regulatory ambition and competitive reality.

The Return of Digital Sovereignty

Europe remains structurally dependent on external actors across the AI value chain — raising fundamental questions about the feasibility of technological autonomy.



Cloud Infrastructure

Dominated by US hyperscalers



Advanced Semiconductors

Dependent on Asian supply chains



Foundation Models

Led by US-based developers



Digital Platforms

Concentrated in few global actors



Technical Standards

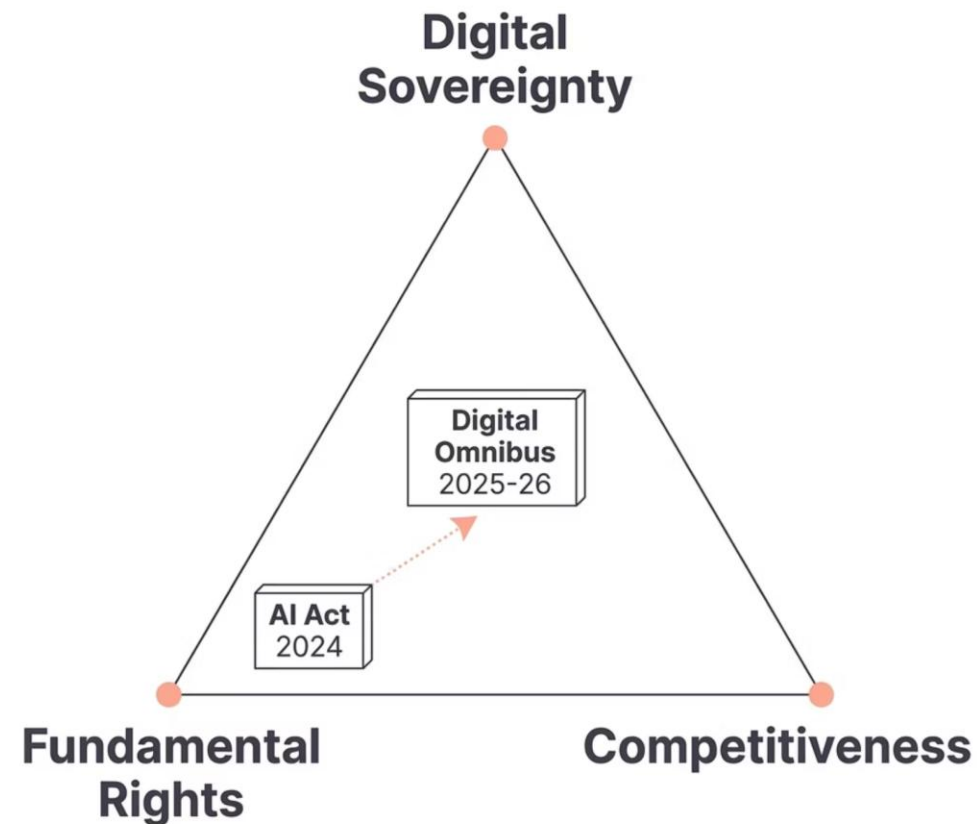
Influence shaped by global bodies

❓ Can Europe achieve technological sovereignty while remaining structurally dependent?

The Triangle of European AI Governance

European AI governance navigates three competing priorities. The AI Act (2024) positioned itself closer to the **fundamental rights** corner. The Digital Omnibus (2025–26) shifts the balance toward the **centre** — reflecting growing pressure from competitiveness and sovereignty agendas.

Both the competitiveness and rights narratives claim to defend Europe's future. The Omnibus reveals which priorities are winning.



The AI Governance Ecosystem in the EU

The AI Act does not govern alone. It depends on a network of supporting infrastructures — standards bodies, regulatory authorities, and administrative capacity — to translate legal text into practical compliance.

Weaknesses in any layer of this ecosystem directly undermine the Act's effectiveness in practice.

„Digitale Unsouveränität”
(Gerdemann, 2025)

The Omnibus is also a response to the **implementation challenges** — not opposition to the AI Act itself. Delayed standards, under-resourced authorities, and missing guidance created structural pressure for revision.

What Changes? Three Reform Clusters

1. Simplification

- Delayed obligations for high-risk AI
- Reduced registration requirements
- Simplified documentation burdens

2. Governance

- Stronger AI Office mandate
- More centralised oversight
- Coordinated national enforcement

3. Innovation

- Expanded regulatory sandboxes
- Real-world testing provisions
- EU-level sandbox from 2028

Key changes include a **delay of high-risk rules** from 2026 to 2027–2028, a shift in AI literacy from **obligation to encouragement**, and standards increasingly functioning as **governance instruments** rather than mere technical tools.

Omnibus Assessment: Technology and Governance

The Digital Omnibus illustrates that technology and governance are not separate domains — they **co-produce** (Jasanoff, 2004) each other.

Infrastructure dependence

Governance relies on technical infrastructures to function.

Standards as regulation

Technical standards increasingly encode regulatory intent.

Feedback loops

Implementation challenges reshape the law itself.

Two Visions for Europe's AI Future

Competitiveness Narrative

- Simplification reduces friction
- Innovation-friendly environment
- Growth and scale-up priorities
- Strategic autonomy

Rights Narrative

- Delays weaken protections
- Reduced accountability
- Weaker transparency obligations
- Risks for fundamental rights

Ultimately, a debate about political priorities and competing visions of Europe's digital future.



Question TBD

Can Europe simultaneously achieve

Trustworthy AI?

Technological
Competitiveness
?

Digital
Sovereignty?

Or will trade-offs become unavoidable in the pursuit of a human-centric digital future?

Contact

Michael Löffler

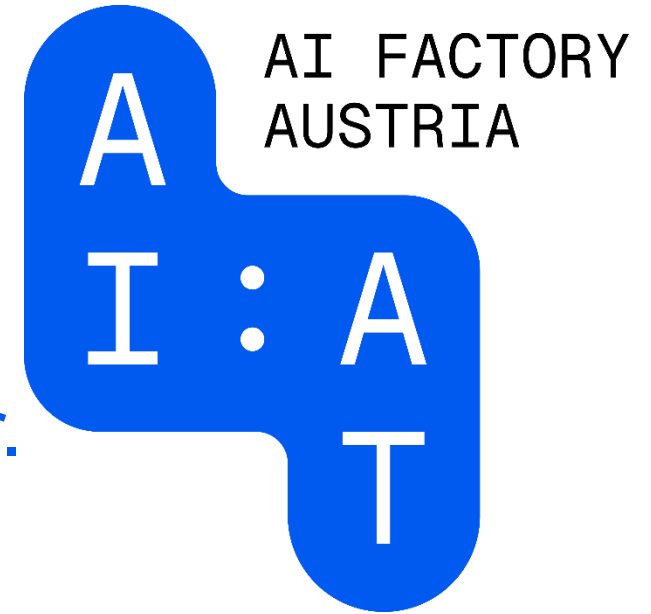
Lead Legal, Regulatory and Ethics
AI Factory Austria AI:AT

+43 664 88390692
michael.loeffler@ai-at.eu

Krisztina Rozgonyi DDr.

Senior Scientist, Legal and Policy
AI Factory Austria AI:AT

+43 664 78042372
krisztina.rozgonyi@ai-at.eu



AI Factory Austria AI:AT
Karl-Farkas-Gasse 22
1030 Wien
training@ai-at.eu
info@ai-at.eu

ai-at.eu

 [@ai-factory-austria](https://www.linkedin.com/company/ai-factory-austria)

Training & Skills Development

• AI Workshops • Courses • Webinars



Scan to explore
our events

Funded by



EuroHPC
Joint Undertaking



**Co-funded by
the European Union**



Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria

under discussion with



AI Factory Austria AI:AT has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101253078. The JU receives support from the Horizon Europe Programm of the European Union and Austria (BMIMI / FFG).