

GUIDE · TOMORIS TOOLBOX

AI Act: Obligations and Deadlines at a Glance, Updated After the Digital Omnibus

Roles, risk levels, prohibitions, high-risk, transparency, AI literacy, penalties, and timeline of Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744

UPDATED

Oct 25, 2026

LENGTH

PDF, 9 pages

ONLINE

tomoris.com/en/downloads/ki-verordnung-pflichten-ueberblick

AT A GLANCE

Art. 4

AI literacy, revised since
Jul 27, 2026

Art. 5

Prohibitions, two more
from Dec 2, 2026

2027

High-risk under Annex III
from Dec 2, 2027

7%

Of annual turnover:
maximum for prohibitions

WHO IT IS FOR

- Executive management of companies that use or offer AI systems
- Compliance, legal, and data protection
- IT management that selects and operates AI tools
- HR departments that evaluate AI for recruitment or performance assessment

WHAT THIS COVERS

Since July 27, 2026, the AI Act has applied as amended by the Digital Omnibus (Regulation (EU) 2026/1744): Art. 4 has been revised, two prohibitions are added on December 2, 2026, and the high-risk obligations only begin in 2027 and 2028. This guide clarifies your role, explains risk levels, prohibitions, high-risk, transparency, and penalties with citations, and concludes with a checklist for the first steps.

This guide provides an overview and does not replace legal advice. The statutory text in its current version is authoritative, in particular the AI Act together with Regulation (EU) 2026/1744; classification depends on the individual case.

CONTENTS

01	What it is about and what changed in 2026	2
02	AI system and roles	3
03	The risk levels	4
04	Prohibited practices under Art. 5	4
05	High-risk AI systems and deployer obligations	5
06	Transparency obligations under Art. 50	6
07	AI literacy under the revised Art. 4	7
08	Timeline after the Digital Omnibus	7
09	Penalties	8
10	First steps for your company	8
11	Sources	9

01

What it is about and what changed in 2026

The AI Act, the Digital Omnibus, and the situation in Austria

The AI Act regulates AI systems according to their risk and applies directly in all Member States. It entered into force on August 1, 2024; its parts apply in stages (Art. 113). The Digital Omnibus Regulation on AI, Regulation (EU) 2026/1744 of July 8, 2026, was published in the Official Journal on July 24, 2026, and entered into force on the third day thereafter, July 27, 2026. Among other things, it revises Art. 4, adds to the prohibitions in Art. 5, postpones the obligations for high-risk AI systems, and extends relief on fines to small mid-cap companies.

Austria: According to the RTR AI Service Center, there is currently no national implementation of the competences yet, neither for the market surveillance authorities nor for the notifying authority. The AI Service Center sees itself as a point of contact and information hub for companies. The Commission's overview (page dated September 7, 2026, accessed October 25, 2026) did not yet name a single point of contact for market surveillance for Austria.

02 —

AI system and roles

What an AI system is and whether you are a provider or a deployer

Definitions under Art. 3 AI Act

AI system (point 1)	A machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment, and that infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions. The Commission published guidelines on this on February 6, 2025.
Provider (point 3)	Develops an AI system or has it developed and places it on the market or puts it into service under its own name or trademark, whether for payment or free of charge.
Deployer (point 4)	Uses an AI system under its own authority, except in the course of a personal, non-professional activity. This is the typical role of a company that uses AI tools.
Importer (point 6), distributor (point 7)	Place AI systems bearing the name or trademark of a provider from a third country on the market in the Union, or make them available in the supply chain.

From deployer to provider: Anyone who puts their own name or trademark on a high-risk AI system, substantially modifies it, or changes the intended purpose of an AI system, including a general-purpose AI system, in such a way that it becomes a high-risk AI system, is itself considered a provider with all provider obligations (Art. 25(1)). Review these cases particularly carefully when you adapt AI tools or use them for new purposes.

03 —

The risk levels

Which obligations depend on the classification

Risk levels of the AI Act

LEVEL	WHAT FALLS UNDER IT	CONSEQUENCE
Prohibited	Practices under Art. 5, such as manipulation, social scoring, emotion recognition in the workplace	May neither be placed on the market nor used
High-risk	Safety components of products under Annex I and applications in the areas of Annex III, such as recruitment, education, creditworthiness	Extensive obligations for providers (Art. 16) and deployers (Art. 26)
Transparency	Chatbots, generated content, deepfakes, emotion recognition, and biometric categorization	Label and inform (Art. 50)
General-purpose AI models	Large foundation models on which many applications are built	Obligations for the providers of the models (Chapter V)
All AI systems	Every AI system in the company	Measures for AI literacy (Art. 4)

04 —

Prohibited practices under Art. 5

What has been prohibited since February 2, 2025, and what is added from December 2, 2026

- a) Subliminal, purposefully manipulative, or deceptive techniques that materially distort behavior and can cause significant harm.
- b) Exploiting vulnerabilities due to age, disability, or a social or economic situation, causing significant harm.
- c) Social scoring of persons that leads to unjustified or unrelated detrimental treatment.
- d) Predicting the risk of a criminal offense based solely on profiling or personality traits.
- e) Facial recognition databases created through untargeted scraping of facial images from the internet or from surveillance footage.
- f) Inferring emotions in the workplace and in educational institutions, except for medical or safety reasons.
- g) Biometric categorization to infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation.
- h) Real-time remote biometric identification in publicly accessible spaces for law enforcement, with narrow exceptions.
- ba) New from December 2, 2026: AI systems that generate or manipulate realistic intimate or sexual depictions of identifiable persons without their explicit consent.
- bb) New from December 2, 2026: AI systems that generate or manipulate child sexual abuse material within the meaning of Directive 2011/93/EU.

Art. 5(1a) narrows the new prohibitions ba and bb: providers are subject to the prohibition if generating such content is the purpose of the system or is foreseeably and reproducibly achievable without significant technical changes and reasonable safeguards are lacking; deployers only if they use the system for this purpose. The Commission's guidelines on the prohibitions of February 4, 2025, are not binding; only the Court of Justice of the EU can provide a binding interpretation.

05

High-risk AI systems and deployer obligations

When a system is high-risk and what deployers then have to do

Annex III names eight areas: biometrics, critical infrastructure, education, employment and workers management, access to essential services, law enforcement, migration, asylum and border control, and administration of justice and democratic processes. Particularly relevant for companies: AI for screening, filtering, and evaluating applications, for decisions on promotion or termination, and for performance evaluation (point 4), as well as for assessing the creditworthiness of natural persons and for pricing in life and health insurance (point 5(b) and (c)). Exception: a system under Annex III is not high-risk if it poses no significant risk and meets one of the four conditions of Art. 6(3), for example if it only performs a narrow procedural task or a preparatory task; with profiling of natural persons, it is always high-risk.

A provider that relies on this exception documents the assessment before the system is placed on the market or put into service, and registers it (Art. 6(4), Art. 49(2)).

- ☐ Use the system in accordance with the provider's instructions for use (Art. 26(1)).
- ☐ Assign human oversight to persons with the necessary competence, training, and authority (para. 2).
- ☐ Check input data, to the extent it is under your control, for relevance to the purpose and representativeness (para. 4).
- ☐ Monitor operation; in case of risk, inform the provider and market surveillance and suspend use, report serious incidents without undue delay (para. 5).
- ☐ Keep automatically generated logs for at least six months, to the extent they are under your control (para. 6).
- ☐ Before use in the workplace, inform workers' representatives and affected employees (para. 7).
- ☐ Inform affected persons when the system makes or assists in decisions about them (para. 11).
- ☐ Use the provider's information for the data protection impact assessment (para. 9).

- ☐ Fundamental rights impact assessment if you, as a deployer, are a body governed by public law or a private entity providing public services (except for critical infrastructure, Annex III point 2), or use AI for creditworthiness or for life and health insurance (Art. 27).

After the amendment by Regulation (EU) 2026/1744, these obligations apply to systems under Annex III from December 2, 2027, and to systems under Annex I from August 2, 2028. Systems placed on the market before then are only covered if their design is significantly changed; systems for public authorities must be brought into compliance by August 2, 2030 (Art. 111(2)).

06 —

Transparency obligations under Art. 50

Label and inform, since August 2, 2026

Chatbots (para. 1)	Providers design AI systems intended for direct interaction so that people are informed that they are interacting with an AI, unless this is obvious.
Generated content (para. 2)	Providers of systems that generate synthetic audio, image, video, or text content mark the outputs in a machine-readable format as artificially generated or manipulated. For systems placed on the market before August 2, 2026, this applies from December 2, 2026 (Art. 111(4)).
Emotion recognition (para. 3)	Deployers of emotion recognition or biometric categorization inform the persons concerned.
Deepfakes (para. 4)	Deployers disclose that image, audio, or video content constituting a deepfake has been artificially generated or manipulated; for evidently artistic, satirical, or fictional works, an appropriate notice is sufficient.
Texts on matters of public interest (para. 4)	Deployers disclose that texts published to inform the public are AI-generated, unless they have undergone editorial review and someone holds editorial responsibility.

The information must be provided clearly and distinguishably at the latest at the time of the first interaction or exposure and must be accessible (Art. 50(5)).

07 —

AI literacy under the revised Art. 4

What has applied since July 27, 2026

Providers and deployers of AI systems take measures to support the development of AI literacy of their staff and of other persons dealing with the operation and use of AI systems on their behalf. Technical knowledge, experience, education and training, the context of use, and the persons on whom the systems are used must be taken into account. Providers and deployers are not required to guarantee a specific level of literacy (Art. 4(1) as amended by Regulation (EU) 2026/1744). The Commission and the Member States provide support, especially for SMEs; the Commission publishes practical examples (para. 2).

Previously, Art. 4 required measures to ensure, to their best extent, a sufficient level of AI literacy of staff. This goal no longer applies; the measures now support the development of literacy. An internal AI policy with training is an obvious choice (TOMORIS recommendation); the "AI usage policy" download provides a template for this.

08 —

Timeline after the Digital Omnibus

The key application dates and transition periods under Art. 113 and Art. 111

Application dates (Art. 113 and 111 AI Act as amended by Regulation (EU) 2026/1744)

DATE	WHAT APPLIES
Aug 1, 2024	Entry into force of the AI Act
Feb 2, 2025	Chapters I and II: general provisions, AI literacy, prohibitions under Art. 5(1)(a) to (h)
Aug 2, 2025	General-purpose AI models, governance, penalties (excluding Art. 101)
Jul 27, 2026	Regulation (EU) 2026/1744 in force: Art. 4 revised; amendments to other legal acts (Art. 102 to 110) apply
Aug 2, 2026	General date of application, including Art. 50 and fines under Art. 101
Dec 2, 2026	Prohibitions ba and bb including Art. 5(1a) and (1b); Art. 50(2) for older systems (Art. 111(4))
Aug 2, 2027	AI models already placed on the market before Aug 2, 2025 (Art. 111(3))
Dec 2, 2027	Obligations for high-risk AI systems under Annex III
Aug 2, 2028	Obligations for high-risk AI systems under Annex I
Aug 2, 2030	Deadline for high-risk AI systems intended to be used by public authorities
Dec 31, 2030	AI systems in large-scale IT systems under Annex X (Art. 111(1))

09 —

Penalties

Maximum amounts under Art. 99 and relief for smaller companies

Fines under Art. 99, whichever amount is higher

INFRINGEMENT	UP TO	CITATION
Prohibited practices	€35 million or 7% of worldwide annual turnover	Art. 99(3)
Obligations of providers, deployers, and other operators, transparency	€15 million or 3%	Art. 99(4)
Incorrect, incomplete, or misleading information to authorities	€7.5 million or 1%	Art. 99(5)

For SMEs, including start-ups, the lower of the two amounts applies in each case (para. 6); the same applies to small mid-cap companies for fines under paras. 4 and 5 (para. 6a, new). The Member States lay down the rules on penalties; they take into account the interests of SMEs and small mid-caps (para. 1).

10 —

First steps for your company

Checklist for taking stock, TOMORIS recommendation

- ☐ All AI systems in use and planned recorded, including AI features in existing software and cloud services.
- ☐ Your own role determined for each system: deployer, provider, or both; cases under Art. 25(1) reviewed.
- ☐ Prohibitions under Art. 5 ruled out, especially emotion recognition in the workplace and, from December 2, 2026, the new prohibitions ba and bb.
- ☐ Use in areas under Annex III reviewed, such as applications, performance evaluation, creditworthiness; result documented.
- ☐ Transparency under Art. 50 implemented, depending on the role: as a provider, notice for chatbots and machine-readable marking (paras. 1 and 2); as a deployer, information on emotion recognition, labeling of deepfakes and of AI texts on matters of public interest (paras. 3 and 4).
- ☐ Measures for AI literacy defined and documented, such as a policy, training, a contact person.
- ☐ Instructions for use and information requested from providers that you need for your obligations and the data protection impact assessment.

- ☐ Responsibility within the company defined and developments tracked: Commission guidelines, standards, national authorities.

NEXT STEP

Check It Yourself or Put It into Practice Together

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

11

Sources

All statements are supported by sources. Legislation applies in its current version.

- Regulation (EU) 2024/1689 (AI Act), consolidated version of July 27, 2026, EUR-Lex**
Art. 2 to 6, 25 to 27, 50, 99, 111, 113, Annex III, accessed October 25, 2026
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02024R1689-20...
- Regulation (EU) 2026/1744 (Digital Omnibus Regulation on AI), OJ L of July 24, 2026**
Art. 1(5), (7), (38) to (40), Art. 4 entry into force, accessed October 25, 2026
eur-lex.europa.eu/eli/reg/2026/1744/oj/deu
- RTR AI Service Center: Timeline and implementation of the AI Act**
Deadlines after the Digital Omnibus, accessed October 25, 2026
www.rtr.at/rtr/service/ki-servicestelle/ai-act/Zeitplan.de.html
- RTR AI Service Center: Frequently asked questions**
Tasks of the AI Service Center, national implementation of competences, accessed October 25, 2026
www.rtr.at/rtr/service/ki-servicestelle/faq/FAQ.de.html
- European Commission: Guidelines on prohibited AI practices (February 4, 2025)**
Description and status of the guidelines, accessed October 25, 2026
digital-strategy.ec.europa.eu/en/library/commission-publishes-g...
- European Commission: Guidelines on the definition of an AI system (February 6, 2025)**
Description of the guidelines, accessed October 25, 2026
digital-strategy.ec.europa.eu/en/library/commission-publishes-g...
- European Commission: Market Surveillance Authorities under the AI Act**
Single points of contact of the Member States, page dated September 7, 2026, accessed October 25, 2026
digital-strategy.ec.europa.eu/en/policies/market-surveillance-a...