September 2026

AI Omnibus: the AI Act "2.0"

The EU legislature has adopted a comprehensive revision of the AI Act even before key parts of the Regulation have become applicable (the "AI Omnibus").[1] The aim of the reform is to simplify the AI Act, to increase legal certainty and to reduce the compliance burden, without reducing the level of protection.

Specifically, the AI Omnibus clarifies the relationship between the AI Act and sector-specific product safety legislation, reduces the requirements relating to AI literacy, includes new prohibitions on intimate material and material depicting child abuse, and introduces administrative simplifications for small mid-cap enterprises. Furthermore, the AI Omnibus gives affected companies more time to comply with some of the key obligations of the AI Act.

This client briefing provides an overview of the key amendments, which entered into force on 27 July 2026, and considers their practical implications.

I. Background

The AI Omnibus is part of a broader European Commission initiative to reform the digital single market, which also includes the so-called Data Omnibus[2]. While the AI Omnibus has already entered into force, the Data Omnibus is undergoing the legislative procedure. Since the Commission presented its proposal in November 2025, neither the European Parliament nor the Council has adopted a negotiating position.

By EU standards, the AI Omnibus was adopted exceptionally quickly: only eight months elapsed between the publication of the Commission's proposal and the entry into force of the Regulation. This unusually swift process was driven in particular by the need to respond to existing and emerging implementation challenges before key provisions of the AI Act were originally scheduled to become applicable. For companies, the AI Omnibus therefore primarily provides additional preparation time and introduces

[1] https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0837

targeted relief, without calling into question the AI Act's overall regulatory approach.

II. The most significant change: more time for companies

The most important change introduced by the AI Omnibus concerns the postponement of the rules on high-risk AI systems (Art. 113 AI Act (new)). Companies that provide or deploy such AI systems will have more time to comply with the regulatory requirements of the AI Act. The obligations, which were originally scheduled to apply from August 2026 and August 2027 respectively, will now apply from **December 2027** (for high-risk AI systems pursuant to Annex III to the AI Act) and **August 2028** (with respect to high-risk AI systems pursuant to Annex I to the AI Act). This postponement reflects the fact that important technical standards needed for the practical implementation of the AI Act are not yet available. These standards are intended to provide companies with guidance on how to comply with the requirements of the AI Act.

Practical note: While the postponement gives affected companies more planning time, it does not eliminate the need for timely action. Companies should use the extended implementation period to establish appropriate compliance structures, allocate responsibilities and assess which of their products or applications could be classified as high-risk AI systems. Companies with longer development cycles, in particular, should start preparing for the forthcoming requirements as soon as possible.

III. Transitional rules and periods

The AI Omnibus also amends the **transitional provisions** (Art. 111 AI Act (new)). This ensures that the postponed dates of application are aligned with the rules for AI systems already placed on the market.

In addition, the reform introduces changes to the **transparency obligations under Art. 50 AI Act**. Providers of AI systems that generate synthetic text, images, video or audio must assess whether their existing systems require technical modifications. Since **2 August 2026**, artificially generated or manipulated content must be identifiable as such and marked in a machine-readable format (Art. 50(2) AI Act). Under the AI Omnibus, this obligation applies not only to new AI systems but also to AI systems already placed on the market. Providers must therefore take the necessary steps to comply with these requirements **by 2 December 2026**.

The precise scope of this grandfathering rule remains, however, uncertain. In particular, it is unclear whether the transparency requirements under Art. 50(1) AI Act AI, which concerns systems intended to interact directly with natural persons, also apply to AI systems already placed on the market.

Practical note: The transparency obligations of Art. 50 AI Act apply to certain providers and deployers of AI systems, irrespective of whether the systems qualify as high-risk. In particular, natural persons must be informed where content has been artificially generated or manipulated. This includes, for example, interactions with chatbots (para. 1) as well as AI-generated video, images and text (paras 2 and 4). In addition, the use of emotion recognition systems must be disclosed (para. 3).[3]

The obligations have been applicable since **2 August 2026.** In view of the legal uncertainty outlined above, companies should also review whether AI systems already placed on the market comply with the applicable transparency requirements.

IV. Closer alignment with sectoral product safety legislation

Another key element of the AI Omnibus is the **closer alignment of the AI Act with existing product safety legislation**. Many AI systems are also subject to sector-specific product safety requirements, which has resulted in overlapping conformity assessment procedures, documentation obligations and other regulatory requirements.

The AI Omnibus therefore seeks to improve the interaction between the two regulatory frameworks. Among other things, it facilitates the coordination of the respective conformity assessment procedures

[3] See also https://www.sza.de/en/thinktank/ai-labelling/

(Art. 43 AI Act (new)), which is intended to help companies avoid duplicative assessments and unnecessary administrative burdens.

In addition, the rules have the aim of preventing substantially identical requirements from applying in parallel under several legislative instruments. To this end, the Commission is empowered to adopt delegated acts in order provide for exemptions from the AI Act in certain areas, provided that existing product safety legislation ensures an equivalent level of protection (Art. 2(13) AI Act (new)). These delegated acts are to be supplemented by standards developed by the European standardisation organisations (Art. 40(2) AI Act (new)) and by Commission guidelines (Art. 96(1)(g) AI Act (new)). The aim of these measures is to support companies in simultaneously complying with the AI Act and the relevant product safety legislation.

Practical note: Many of these measures still have to be fleshed out. While the AI Omnibus provides the general legal framework for this, the specific interplay between the AI Act and sectoral product safety legislation will largely depend on future delegated acts, standards and guidelines. Companies should therefore follow these developments closely.

In addition, products falling within the scope of the **Machinery Regulation (Regulation (EU) 2023/1230)** are largely exempted from the obligations of the AI Act (Art. 2(2) AI Act in conjunction with Annex I, Section B to the AI Act (new)). The AI-specific requirements for such products are to be integrated directly into the Machinery Regulation.

V. Remaining legal uncertainty regarding AI literacy

The AI Omnibus retains the obligation to promote AI literacy, but frames it in less prescriptive terms (Art. 4 AI Act (new)). Companies are expected to take measures to support the development of AI literacy, but **are no longer required to ensure that their staff attain a specific level of literacy.**

This leaves considerable uncertainty as to what the obligation requires in practice. In particular, it remains unclear which specific measures are required in order to satisfy the regulatory requirements. In addition, it is questionable which legal consequences may result from non-compliance with the AI literacy obligation. The Commission is to publish guidance and best practices. At present, however, there are no binding requirements.

Practical note: Irrespective of the requirements of the AI Act, companies should ensure that their staff understand the legal risks associated with the use of AI systems. Relevant areas include data protection law, copyright law, cybersecurity law[4] and trade secret law[5], in particular with a view to the use of generative AI.

VI. More flexibility in AI training

Another practically significant change concerns the **processing of special categories of personal data in the development and training of AI systems** (Art. 4a AI Act (new)). Previously, the relevant exemption was limited to providers of high-risk AI systems. Under the AI Omnibus, this exemption is extended to all AI systems and models as well as to deployers of AI systems.

The reform therefore provides **providers and deployers** with more legal certainty when using sensitive data to identify and mitigate bias in AI systems and models. At the same time, the conditions for relying on the exemption remain strict. The processing must be strictly necessary for this purpose and comply with the additional requirements set out in Art. 4a AI Act, including documentation obligations, restrictions on further processing, limitations on data transfers, requirements relating to data deletion and appropriate safeguards for data security.

For companies, representative training data is often essential for developing high-performing and non-discriminatory AI systems and models. While the reform creates greater flexibility in this area, the

[4] https://www.sza.de/en/thinktank/cyber-resilience-act-obligations-products-with-digital-elements/

[5] https://www.sza.de/en/thinktank/ai-tools-trade-secrets/

applicable data protection requirements remain demanding.

VII. Prohibitions on nudifier and CSAM applications

The AI Omnibus introduces new prohibitions concerning AI systems that are capable of generating or manipulating **intimate material ("nudifiers") as well as material depicting child abuse and sexual exploitation of children (Art. 5(1)**, first subparagraph, points (ba) and (bb) AI Act (new)). The prohibitions apply to both providers and deployers of such systems.

Of particular importance for companies is the requirement for providers to implement appropriate technical safeguards to prevent their systems from generating or manipulating such content. The assessment is not limited to the provider's intended use of the system. A prohibition may also apply where the generation of prohibited content is a reasonably foreseeable outcome and adequate safeguards have not been put in place.

In practice, the AI Omnibus significantly **expands providers' responsibilities to prevent and monitor foreseeable misuse of AI systems**. Companies should therefore assess whether their AI systems could be misused to create such content and whether existing technical safeguards, such as filters, blocking mechanisms or abuse-detection tools, are sufficient. Measures for detecting, monitoring and preventing known forms of misuse are also likely to become increasingly important.

VIII. Relief for SMEs and small mid-caps

The AI Omnibus also **extends** various **support and relief measures** that were previously intended to benefit above all small and medium-sized enterprises (SMEs) to so-called **small mid-cap enterprises (SMCs)**. These are larger mid-sized companies with up to 750 employees which have either an annual turnover of no more than EUR 150 million or a balance sheet total of no more than EUR 129 million (Art. 2(14b) AI Act (new)).

For affected companies, this entails, among other things, certain regulatory reliefs, such as simplified documentation obligations for providers of high-risk AI systems (Art. 11(1) AI Act (new)), reduced penalties (Art. 99(6a) AI Act (new)) and easier access to administrative support (cf. Art. 70(8) AI Act (new)). In addition, SMEs, though not small mid-caps, may comply with certain quality management requirements in a simplified manner (Art. 63(1) AI Act (new)).

It is important to note, however, that the AI Omnibus does not create any general exemption from the substantive requirements of the AI Act. The **core compliance obligations**, in particular those related to high-risk AI systems, **remain largely unchanged**. The purpose of these amendments is primarily to reduce administrative burdens rather than to lower the level of regulatory protection. How meaningful these relief measures will be in practice will depend largely on future Commission guidance, support measures and administrative practice.

IX. Other changes

The AI Omnibus also introduces a number of **institutional and organisational changes**. A key role is played by the AI Office, whose responsibilities are being expanded and further clarified (Art. 75 AI Act (new)). Under certain conditions, the AI Office assumes responsibility for supervising AI systems based on general-purpose AI models that are developed within a corporate group. In addition, it oversees AI systems integrated into very large online platforms and very large online search engines within the meaning of the Digital Services Act. The AI Office is also granted broader monitoring, investigative and enforcement powers (Arts 75a-d AI Act (new)). Overall, this leads to more centralised AI oversight at EU level.

Further changes concern **AI regulatory sandboxes** which allow companies to test AI systems in controlled environments under regulatory supervision. Under the new rules, the AI Office may establish a Union-wide AI regulatory sandbox itself (Art. 57(3a) AI Act (new)). In addition, the possibilities to test certain high-risk AI systems in real-world conditions are being expanded (Arts 60, 60a AI Act (new)). This may create additional flexibility in developing innovative or complex AI applications and facilitate their market entry. However, it remains to be seen to what

extent AI regulatory sandboxes will deliver practical benefits.

X. Conclusion

The AI Omnibus introduces targeted simplifications and clarifications, but it does not fundamentally reshape the AI Act. While the compliance timeline for high-risk AI systems has been extended and certain obligations have been clarified, the core compliance requirements remain largely unchanged. Companies should therefore not expect the overall regulatory burden to decrease significantly.

Rather, the AI Omnibus highlights once again that the practical application of the AI Act will continue to depend heavily on future guidance, standards and other implementing measures, particularly those issued by the European Commission and the European standardisation organisations. Many important questions, including the interpretation of individual obligations and the interaction between the AI Act and other areas of digital regulation, remain uncertain.

For companies, AI compliance therefore remains a "moving target". The regulatory framework continues to evolve and requires continuous monitoring as well as regular adjustments to internal processes and governance structures.

We continue to monitor developments in European AI regulation and support companies in assessing new legal requirements, implementing compliance measures and developing practical AI governance and training frameworks.

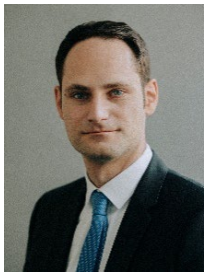
This client information provides only a non-binding overview of the subject area it addresses. It does not replace legal advice. The following contacts are available to answer questions on this client information and to advise you:

Dr. Thomas Nägele
Rechtsanwalt | Partner
Compliance, Internal Investigations | Privacy and Data Security| Intellectual Property | IT Law | Litigation and Arbitration

T +49 621 4257 222
E Thomas.Naegele@sza.de

Dr. Simon Apel
Rechtsanwalt | Partner
Intellectual Property | Privacy and Data Security

T +49 621 4257 386
E Simon.Apel@sza.de



Alexander Stolz, LL.M. (Dresden / Exeter)
Rechtsanwalt | Counsel
Commercial | Privacy and Data Security| Intellectual Property | IT Law

T +49 621 4257 222
E Alexander.Stolz@sza.de

Serpil Dilbaz, LL.B.
Rechtsanwältin | Senior Associate
Privacy and Data Security| Intellectual Property | IT Law

T +49 621 4257 222
E Serpil.Dilbaz@sza.de

Hannah Bräunche
Rechtsanwältin | Associate
Intellectual Property | Privacy and Data Security | Commercial

T +49 621 4257 386
E Hannah.Braeunche@sza.de