POLICY BRIEF

POLLICINO & PARTNERS
AIDVISORY

The AI Act deadlines after the Digital Omnibus on AI - Applicable obligations and operational steps for providers and deployers

Oreste Pollicino[1], Giovanni De Gregorio[2] and Rebecca Pupella[3]

In view of the imminent 2 August 2026 deadline, organizations that develop, place on the market, put into service or use AI systems should complete a focused review of the obligations that will apply from that date.

Against this background, Regulation (EU) 2026/1744 (the "Digital Omnibus on AI") was published in the *Official Journal of the European Union* on 24 July 2026 and entered into force on 27 July 2026. The Digital Omnibus on AI amended the AI Act's application timetable, postponing a number of key obligations, most notably the requirements and operator obligations applicable to high-risk AI systems.

As an amending regulation, the Digital Omnibus on AI does not replace the AI Act or operate as a self-contained rulebook. It replaces individual provisions, inserts new provisions and changes specific dates or wording, while leaving the remainder of AI Act in force. The applicable legal framework must therefore be reconstructed by reading the AI Act together with the amendments introduced by the Digital Omnibus on AI.

The postponement, however, does not remove the practical significance of **2 August 2026**. A number of provisions will become applicable or fully enforceable from that date, while other obligations are already in force. This policy brief therefore clarifies which obligations organizations must address now and sets out the corresponding operational steps for providers and deployers.

The legal position after the Digital Omnibus on AI – the deferral of the high-risk regime

The Digital Omnibus on AI replaces the timetable set forth in Article 113(c) of the AI Act. Apart from Article 6(5), Sections 1, 2 and 3 of Chapter III will apply from **2 December 2027** to AI systems classified as high-risk under Article 6(2) and Annex III, and from **2 August 2028** to AI systems classified as high-risk under Article 6(1) and Annex I.

Accordingly, 2 August 2026 is no longer the deadline for completing obligations related to high-risk systems. Such obligations include, in particular, the

---

[1] Managing Partner, Pollicino AIdvisory.

[2] Vice Dean for Research, Católica Global School of Law.

3 AIdvisor, Pollicino AIdvisory.

info@orestepollicino.eu
https://pollicinoaidvisory.eu/

classification rules, the requirements on risk management, data governance, technical documentation, record-keeping, human oversight, accuracy, robustness and cybersecurity, and the corresponding duties of providers, deployers and other operators.

The postponement is targeted: indeed, it neither defers certain provisions nor removes the obligations already applicable.

Provisions applicable from 2 August 2026

1. Transparency obligations (Article 50 AI Act)

Article 50 allocates different duties according to the role performed in the relevant AI value chain.

Obligations for providers

Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. The information must be provided in a clear and distinguishable manner no later than the first interaction and must conform to the applicable accessibility requirements.

Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content must ensure that the outputs are marked in a machine-readable format and detectable as artificially generated or manipulated. Their technical solutions must be effective, interoperable, robust and reliable as far as technically feasible, subject to the exceptions in Article 50(2). Providers of such systems placed on the market before 2 August 2026 must take the necessary steps to comply with Article 50(2) by **2 December 2026**.

Operationally, providers should map the relevant interfaces and generative functions, implement and test the required notices or marking, retain evidence of the solution adopted and verify whether third-party or white-label arrangements affect their regulatory role.

Obligations for deployers

Deployers must provide clear, distinguishable and accessible information no later than the first exposure in the following cases:

i. Emotion recognition and biometric categorization: where the use is otherwise lawful, exposed natural persons must be informed about the operation of the system; applicable data-protection rules remain fully applicable;

ii. Deep fakes: the deployer must disclose that image, audio or video content constituting a deep fake has been artificially generated or manipulated, subject to the specific rule for evidently artistic, creative, satirical, fictional or analogous works or programs;

iii. Text on matters of public interest: the deployer must disclose the artificial generation or manipulation of text published to inform the public on matters of public interest, unless the content has undergone human review or editorial control and a natural or legal person holds editorial responsibility.

The provider's machine-readable marking duty and the deployer's human-facing disclosure duty are separate.

Non-compliance with Article 50 is subject to administrative fines of up to EUR 15 million or, for an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher, subject to the lower-cap rules applicable to SMEs, including start-ups, and SMCs. Any sanction must be determined on a case-by-case basis and remain effective, proportionate and dissuasive.

2. *Processing of special categories of personal data for bias detection and correction (Article 4a AI Act)*

From 2 August 2026, Article 4a, inserted by the Digital Omnibus on AI, provides a narrowly framed legal basis for the exceptional processing of special categories of personal data for bias detection and correction. It operates in addition to the applicable Union data-protection rules and does not create a general permission to process such data.

For high-risk AI systems, providers may process special categories of personal data only to the extent strictly necessary to ensure bias detection and correction in accordance with Article 10(2), points (f) and (g), and only where all the conditions and safeguards in Article 4a(1) are met. In particular, the objective must not be capable of being effectively fulfilled by processing other data, including synthetic or anonymised data; re-use must be technically limited; state-of-the-art security and privacy-preserving measures, including pseudonymisation, and strict access controls must be applied; the data must not be transmitted, transferred or otherwise accessed by other parties; the data must be deleted once the bias has been corrected or the retention period has expired, whichever comes first; and the records of processing activities must state why the processing was strictly necessary and why the objective could not be achieved using other data.

Providers and deployers of other AI systems and models, and deployers of high-risk AI systems, may also exceptionally process special categories of personal data where this is strictly necessary to ensure bias detection and correction in view of possible biases likely to affect the health and safety of persons, have a negative

impact on fundamental rights or lead to discrimination prohibited pursuant to Union law, provided that the same conditions and safeguards are applied. Article 4a(2) expressly states that this possibility does not create an obligation to conduct such bias detection and correction.

Operationally, an organization relying on Article 4a should document the necessity assessment, the alternatives considered, the applicable access and retention controls, and the reasons recorded in its records of processing activities. Article 4a should be treated as an exceptional route, not as a default basis for the use of special categories of personal data.

3. *Fines for providers of general-purpose AI models (Article 101 AI Act)*

The substantive obligations for providers of general-purpose AI models under Chapter V have applied since 2 August 2025, subject to the transitional rule for models placed on the market before that date. Those obligations include technical documentation, information and documentation for providers, a policy to comply with Union copyright law and a sufficiently detailed public summary of the content used for training. Additional obligations apply to providers of general-purpose AI models with systemic risk.

From 2 August 2026, Article 101 becomes applicable. Where the Commission finds that a provider of general-purpose AI models has intentionally or negligently committed one of the infringements specified in that provision, it may impose fines of up to 3% of the provider's annual total worldwide turnover for the preceding financial year or EUR 15 million, whichever is higher. Providers of models placed on the market before 2 August 2025 have until **2 August 2027** to take the necessary compliance measures.

An organization does not become a provider of a general-purpose AI model merely by using a third-party model. It should nevertheless determine whether it acts as a provider of a general-purpose AI model, a provider of an AI system integrating such a model, or a deployer, because the applicable obligations differ materially.

Obligations already applicable: the postponement is not a standstill

AI literacy remains an obligation (Article 4 AI Act)

Article 4 has applied since 2 February 2025. As amended by the Digital Omnibus on AI, it requires providers and deployers to 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, the context in which the AI systems are used, and the persons or groups on whom those systems are used.

The amended Article 4 expressly provides that this obligation does not require providers or deployers to guarantee any specific level of AI literacy of any individual.

It does not prescribe a particular training format, a minimum number of hours, a mandatory certification or a specific governance structure.

In our view, the contextual factors listed in Article 4 support a role- and use-case-specific approach rather than a one-off, generic exercise. A proportionate program should address, as appropriate, permitted and prohibited uses, the capabilities and limitations of the relevant systems, inaccurate or biased outputs, the handling of confidential and personal data, human verification and incident escalation. Although the AI Act does not prescribe a specific documentary framework, organizations would be well advised to retain evidence of the measures adopted and to update them when systems, roles or use cases materially change.

Prohibited practices remain immediately relevant (Article 5 AI Act)

The prohibited practices originally listed in Article 5 have applied since 2 February 2025. An organization must therefore screen a proposed use case before placing an AI system on the market, putting it into service or using it.

The Digital Omnibus on AI adds two prohibitions concerning AI systems that generate or manipulate realistic non-consensual intimate material depicting identifiable natural persons and AI systems that generate or manipulate child sexual abuse material. For providers, the prohibitions apply where the system is intended to generate or manipulate such material or where that result is reasonably foreseeable and reproducible and reasonable and adequate technical measures and other safeguards are not in place. For deployers, the prohibitions apply where the system is used for the purpose of generating or manipulating such material. These additional prohibitions, together with the related scope provisions, apply from **2 December 2026**. Providers and deployers of AI systems capable of generating or manipulating relevant material should therefore use the intervening period to review the intended purposes, reasonably foreseeable misuse, and the adequacy of the safeguards implemented.

How to use the high-risk extension

The extended implementation period should also be used to establish a structured high-risk AI compliance program. Without prejudice to Article 5, Article 111(2), as amended, provides that the AI Act applies to operators of high-risk AI systems placed on the market or put into service before the relevant date of application of Chapter III only where, from that date, those systems undergo significant changes in their design. In any event, providers and deployers of high-risk AI systems intended to be used by public authorities must take the necessary steps to comply with the applicable requirements and obligations by **2 August 2030**.

Recital 39 of the Digital Omnibus on AI clarifies that the transitional regime is assessed by reference to the type and model of the AI system. Where at least one individual unit of a given type and model has been lawfully placed on the market or

put into service before the relevant date, further units of the same type and model may continue to be placed on the market, made available or put into service without any additional obligations, requirements or need of additional certification, provided that the design remains unchanged. Any significant change to the design after the relevant date triggers the provider's obligation to comply fully with the applicable high-risk requirements, including the conformity assessment requirements.

As a matter of prudent implementation, organizations intending to rely on this transitional regime should preserve evidence of the first lawful placement on the market or putting into service, together with records identifying the relevant type, model and version, the intended purpose, the applicable design baseline and any subsequent changes. These records will be important in demonstrating both eligibility for the transitional regime and whether a later change is significant.

In parallel, organizations should maintain differentiated implementation roadmaps for systems classified as high-risk under Article 6(2) and Annex III, for which the relevant provisions apply from **2 December 2027**, and systems classified as high-risk under Article 6(1) in conjunction with Annex I, for which the relevant date is **2 August 2028**. In relation to Annex I systems, the roadmap should also take account of the specific scope limitations and sectoral rules applicable under Article 2 of the AI Act

From an operational perspective, it is essential for organizations to use the extended implementation period to establish an appropriate AI governance framework. That framework should provide an up-to-date mapping of AI systems and general-purpose AI models, allocate regulatory and operational responsibilities clearly, and define the information flows required for classification, approval, procurement, monitoring, incident escalation and change management. It should support, rather than replace, the separate legal assessment required for each system and use case.

Operational calendar

The following table summarizes the relevant deadlines.

DATE	OBLIGATION	DESCRIPTION
2 February 2025	**AI literacy and Prohibited AI practices in place before the Digital Omnibus on AI** (Articles 4 and 5 AI Act)	AI literacy and the original Article 5 prohibited practices apply. The additional prohibitions introduced by the Digital Omnibus on AI apply from 2 December 2026.

POLICY BRIEF

POLLICINO & PARTNERS
AIDVISORY

DATE	OBLIGATION	DESCRIPTION
2 August 2025	**General-purpose AI model obligations** and **institutional governance** (Chapter III, Section 4, Chapter V, except Article 101, Chapter VII, Chapter XII, Article 78 AI Act)	Chapter III, Section 4, Chapter V (except Article 101), Chapter VII, Chapter XII and Article 78 become applicable. Providers of general-purpose AI models remain subject to the transitional regime for models placed on the market before 2 August 2025. Article 101 applies from 2 August 2026.
2 August 2026	**Transparency obligations**, **article 4a framework** and **Penalties for GPAI enforcement** (Articles 50, 4a and 101 AI Act)	Article 50 applies. Article 4a establishes the exceptional framework for processing special categories of personal data for bias detection and correction. Article 101 becomes applicable to providers of general-purpose AI models.
2 December 2026	**New prohibited practices** and **marking for pre-2 August 2026 generative AI systems** (Articles 5 AI Act as amended by the Digital Omnibus on AI, and 50(2) AI Act)	The additional Article 5 prohibitions apply. Providers of AI systems, including general-purpose AI systems, that generate synthetic content and were placed on the market before 2 August 2026 must comply with Article 50(2).
2 August 2027	**General-purpose AI models placed on the market before 2 August 2025** (Article 111(3) AI Act)	Providers of general-purpose AI models placed on the market before 2 August 2025 must take the necessary steps to comply with the applicable obligations by this date.
2 December 2027	**High-risk AI systems under**	Chapter III, Sections 1 to 3 apply, with the exclusion of Article 6(5).

info@orestepollicino.eu
https://pollicinoaidvisory.eu/

POLICY BRIEF

POLLICINO & PARTNERS
AI DVISORY

DATE	OBLIGATION	DESCRIPTION
	Article 6(2) and Annex III (Article 6(2) and Annex III AI Act)	
2 August 2028	**High-risk AI systems under Article 6(1) and Annex I** (Article 6(1) and Annex I AI Act)	Chapter III, Sections 1 to 3 apply, except Article 6(5), subject to the scope rules in Article 2.
2 August 2030	**High-risk AI systems intended to be used by public authorities** (Article 111(2) AI Act)	Providers and deployers of high-risk AI systems intended to be used by public authorities must take the necessary steps to comply with the applicable requirements and obligations by this date.

info@orestepollicino.eu
https://pollicinoaidvisory.eu/