

October 2026

& Compliance Risk Management

New regulations and practices
for data governance and
business risk management

AI Governance

Digital Omnibus and AI Act: new timelines for high-risk systems

2

D.Lgs. 231/2001

AI in D.Lgs. 231/2001

3

Privacy | AI | Cyber

AI ACT, Digital Omnibus and GDPR: redefining the legal bases and special categories of data

4

Risk Management

Risk Assessment in the Age of AI: New Sensitive Activities and Protocols for Human Oversight

5



Paola Finetto

Partner

paola.finetto@it.andersen.com



Luca Rigotti

Partner

luca.rigotti@it.andersen.com

Contributors: **Maria Lillà Montagnani, Elisa D'Arrigo, Nicolò Bottura and Giacomo Obetti**

October 2026

& Compliance Risk Management

New regulations and practices
for data governance and
business risk management

AI Governance

Digital Omnibus and AI Act: new timelines for high-risk systems

As part of the **Digital Omnibus** – the EU package aimed at simplifying the Union’s digital regulatory framework – the EU institutions have introduced amendments to the AI Act. These changes primarily affect the application of certain obligations, particularly those concerning **high-risk AI systems**.

In particular, the most significant adjustment concerns the postponement of the AI Act obligations applicable to the systems listed in Annex III, which are used in areas such as biometrics, critical infrastructure, education, employment, access to essential services, migration and the administration of justice. For these systems, the relevant obligations will apply from **2 December 2027**. For high-risk systems embedded in regulated products, the applicable deadline is **2 August 2028**.

Companies can use this additional time to build an **AI governance** model based on a concrete understanding of the AI tools they already use or are considering adopting. This means **mapping AI systems, classifying their risk**, identifying internal roles and responsibilities, defining **approval procedures**, setting rules for input and output data, and providing appropriate **training**. In practical terms, the postponement gives companies the opportunity to approach AI Act **compliance** in a more structured and gradual way, embedding it into their existing internal governance, control and risk management processes.

October 2026

& Compliance & Risk Management

New regulations and practices
for data governance and
business risk management

D.Lgs. 231/2001 **AI in D.Lgs. 231/2001**

Legislative Decree No. 160/2026, implementing the AI Act (EU Regulation 2024/1689), has entered into force. The decree introduced a new **Article 25-vicies** into Legislative Decree No. 231/2001, entitled “Offences committed through the use of artificial intelligence systems”.

The decree adds two predicate offences to the regulatory framework governing the administrative liability of entities. The first is **Article 437-bis** of the Italian Criminal Code, introduced by the same decree, which penalises the **failure to adopt technical safety measures or human oversight measures for high-risk AI systems**, as well as their unlawful alteration, provided that such conduct results in a concrete danger to life, individual or public safety, or State security. The second is Article 612-quater of the Italian Criminal Code, which criminalises so-called **deepfake**-related conduct.

For offences under Article 437-bis, the financial penalty imposed on the entity ranges from 600 to 1,000 quotas, while for deepfake-related offences it ranges from 200 to 700 quotas. Disqualification sanctions are also applicable, with the exception of disqualification from carrying on business activities.

From a Legislative Decree 231/2001 perspective, it will therefore be necessary, as part of the risk assessment, to assess whether and how AI, particularly high-risk AI systems, is used within the company's business processes. Where the analysis identifies a **concrete exposure to the risk** of committing the newly introduced predicate offences, the Organisational, Management and Control Model (231 Model) should identify specific **control measures**, including criteria and limitations governing the use of AI, the allocation of roles and responsibilities in relation to the generation and dissemination of content, mechanisms for reviewing and approving outputs, and appropriate training initiatives for employees.

October 2026

& Compliance & Risk Management

New regulations and practices
for data governance and
business risk management

Privacy | AI | Cyber

AI ACT, Digital Omnibus and GDPR: redefining the legal bases and special categories of data

On 27 July 2026, Regulation (EU) 2026/1744, the so-called “**AI Omnibus**”, came into force, amending the **AI Act**. The new text provides that providers may process special categories of data (**sensitive data**), such as health-related data, to detect and correct biases in AI systems. This power, previously reserved for providers of high-risk AI systems, now extends to **providers** and **deployers** of other AI systems and models, provided that the use of synthetic or anonymised data is prevented, additional enhanced security measures are adopted, access to data is restricted, and the data is deleted once the bias has been corrected. However, this is neither an obligation nor a derogation from the GDPR, which remains fully applicable.

The situation is different for the part of the Omnibus Act amending the **GDPR**, which is still under discussion. The European Commission’s proposal clarifies that the processing of personal data for the development and use of AI systems may be based on the **legitimate interest** of the data controller. However, this is not an automatic green light: a balance must still be struck with the rights of data subjects and individuals must be able to object to the processing unconditionally.

With regard to sensitive data, the proposal introduces two new exceptions to the prohibition in Article 9 of the GDPR. The first concerns **sensitive data present only in residual quantities within training datasets**: these are permitted provided the organisation takes appropriate measures to prevent their collection and to remove them if detected. The second allows the use of **biometric data to verify identity**, provided it remains under the exclusive control of the data subject.

In any case, it is advisable to take steps to map the data used in AI projects, check for the presence of sensitive data in datasets, and document the legal bases and security measures implemented.

October 2026

& Compliance Risk Management

New regulations and practices
for data governance and
business risk management

Risk Management

Risk Assessment in the Age of AI: New Sensitive Activities and Protocols for Human Oversight

AI does not need to make the final decision to influence it. It can choose which candidates a recruiter sees, which faults are flagged to production staff, or which customers are selected for review. It is a tool to support while the decision remains human.

That is where risk assessment begins. The Risk Manager maps how AI is used across business processes and identifies **sensitive activities**: those in which an error, distorted data or omitted information could affect people, financial results or **operational continuity**. For each activity, the Risk Manager considers what could happen, how likely it is and what harm it could cause. **Existing controls** are then assessed to determine whether the remaining risk is acceptable to the organisation.

Human oversight must also follow from this analysis. Someone approving a forecast must be able to check the data and assumptions behind it; someone reviewing anomalies selected by AI must also examine a sample of the cases it excluded. The protocol specifies who intervenes, when, what information they need and whether they have the authority to correct or stop the system. Reviews must be documented so that detected errors inform the next **risk assessment**.

The Risk Manager's role is not simply to add a human signature to the process. It is to identify where the organisation might lose control of its decisions and create the conditions for using AI with confidence.