March 2026

&Compliance Risk Management

New regulations and practices for data governance and business risk management

Paola Finetto
Partner
paola.finetto@it.andersen.com

Luca Rigotti
Partner
luca.rigotti@it.andersen.com

Contributors: **Nicolò Bottura**, **Elisa D'Arrigo**

March 2026

D.Lgs. 231/2001

Corporate criminal liability in case of offences related to the use of AI-based systems

The use of Artificial Intelligence systems in corporate processes – from recruitment to predictive analytics and supply chain management – opens up new frontiers of efficiency, but also unprecedented risk profiles under Legislative Decree n. 231/2001.

Corporate liability may arise where the use of AI-based systems becomes an instrument for committing predicate offences: for example, cybercrimes (unauthorized access, unlawful data processing), data protection offences, computer-related forgery, as well as fraud, market manipulation, or breaches of workplace health and safety regulations where improperly configured algorithms affect production processes.

The adoption of automated solutions does not mitigate **organizational fault**; on the contrary, it requires stronger safeguards. Companies must be able to demonstrate that they have assessed **AI-related risks**, defined clear responsibilities within AI **governance**, and implemented **controls** over datasets, output quality, and the traceability of algorithmic decisions.

In this context, the 231 Model should be updated by integrating: mapping of AI-driven processes, technical and legal validation protocols, segregation of duties between development, implementation and oversight, and dedicated reporting flows to the Supervisory Body (OdV).

Staff training on the responsible use of AI tools is equally crucial.

Technological innovation does not relieve companies of their duty of oversight: true compliance lies in governing the algorithm, not being governed by it.

Privacy | AI | Cyber

GDPR and AI ACT: an integrated approach to protect personal data

In the European digital landscape, the protection of personal data now requires an increasingly integrated approach.

The interaction between the **GDPR** and the **AI Act** is crucial for the **responsible and ethical** development of artificial intelligence, as it aims to ensure that technology, in particular systems based on artificial intelligence (AI), is developed in a way that respects people's fundamental rights.
Since its entry into force, EU Regulation 2016/679 (known as the GDPR) represents the essential regulatory framework for the protection of personal data.

In fact, it provides for compliance with fundamental principles such as **minimisation, transparency, accountability and proportionality** and establishes specific rules in cases where an AI system can make **decisions in an automated manner** (e.g. credit scoring systems).

However, this is not enough. The rapid evolution of AI has required further action by the European legislator.
EU Regulation 2024/1689 (known as the AI Act), which came into force on 1 August 2024, introduces criteria for classifying AI systems according to risk, governance obligations and data quality requirements to ensure that algorithms operate in a safe, fair and verifiable manner.
Integrated management of these two regulations therefore makes it possible to address the critical issues associated with automated systems: from the necessity of **explainability of decisions** to the prevention of bias, from proper impact assessment to the definition of roles and responsibilities among developers, suppliers and users.

In operational terms, for organisations, this means strengthening **governance** by carrying out specific **risk assessments**, defining clear and transparent internal **procedures** and **training** staff in data protection, cybersecurity and AI.
The integration of the GDPR and the AI Act thus becomes a strategic lever for increasing stakeholder confidence, ensuring digital sustainability and the use of technology in compliance with fundamental rights.

Risk Management

The classification of AI systems based on risk: high-risk AI systems

The European regulation on artificial intelligence (**AI Act**) identifies high-risk AI systems in view of their potential impact on the health, safety and fundamental rights of individuals.

These systems are not prohibited, but their placing on the market is subject to strict **compliance requirements**. High-risk AI systems include toys, lifts, radio equipment, pressure equipment, recreational craft equipment, cableway installations, medical devices, in vitro diagnostic medical devices, motor vehicles and aircraft, as well as systems intended to be used as safety components of critical digital infrastructure and installations for the supply of water, gas, heating and electricity.

In addition, AI systems used in education or vocational training, for example to assess learning outcomes, or systems used in the employment sector, in particular for staff selection or for monitoring or evaluating workers, fall within this category.

Consider, too, AI systems used to determine access to or suspension of essential public assistance services or benefits, such as health services, social security benefits and social services.

The AI Act sets out specific requirements for the development, marketing and use of such systems, with the aim of balancing **innovation** and **protection** of individuals.

These systems must be designed and developed in such a way that they can be used under the constant **supervision** of natural persons.

In addition, periodic controls are required to verify that they meet high standards of **safety**, in line with the objectives of the European digital strategy to make AI both innovative and reliable.