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

AI Governance

AI Act: New Transparency Rules for Businesses and Professionals

Transparency has long been an essential safeguard in the EU legal framework, from data protection to consumer law.

Under the **AI Act**, however, it serves a specific purpose: reducing the information asymmetry created by the opacity of many artificial intelligence systems.

The obligations under **Article 50**, on which the European Commission has published specific Guidelines, have applied since 2 August 2026.

Unlike the requirements for high-risk systems, they depend on the system's features and use.

Providers of systems intended to interact directly with individuals must inform them that they are interacting with AI, unless this is obvious.

Providers of generative systems must also ensure that synthetic outputs are detectable in a machine-readable format.

Deployers also have specific duties: those using emotion recognition or biometric categorisation systems must inform the individuals exposed to them; those disseminating deepfakes or certain AI-generated texts on matters of public interest must disclose their artificial origin, subject to the applicable exceptions.

Not everyone, therefore, is subject to the same requirements. For businesses and professionals, the first step is to **identify their role, provider or deployer, and map their systems, outputs and recipients**.

Transparency thus becomes an operational obligation: knowing who does what, towards whom and by what means.

September 2026

D.Lgs. 231/2001

The Code of Ethics: A valuable tool for regulating the use of AI within Companies

Artificial intelligence is rapidly becoming part of business processes, offering new opportunities for efficiency and innovation while also introducing unprecedented risks: from the management of personal data and confidential information to the improper use of AI tools by employees.

In this context, the **Code of Ethics** can serve as one of the tools through which a company defines the fundamental principles and rules governing the responsible use of artificial intelligence.
The aim is not necessarily to turn the Code of Ethics into a technical document.

Rather, it can establish a set of **general principles of conduct**, which can then be implemented through specific policies, procedures and operational guidelines.
These may include, for example, transparency in the use of AI, a prohibition on entering confidential information into unauthorised tools, human oversight of AI-generated outputs, and a prohibition on using AI for unlawful or discriminatory purposes.

The Code of Ethics may also expressly require employees to use only **AI tools approved by the company**, in accordance with authorisation levels established internally.

This approach is also particularly relevant in the context of the **Organisational Model under Legislative Decree No. 231/2001**, as it makes it possible to link ethical principles to the corresponding control measures.
The use of AI may, in fact, have a cross-cutting impact on numerous business processes and, under certain circumstances, contribute to the commission of predicate offences.
The Code of Ethics becomes not merely a statement of values, but a genuine **"governance framework" for AI**, capable of guiding individual behaviour and strengthening the company's compliance culture, in coordination with its system of policies, procedures, controls and responsibilities.

Privacy | AI | Cyber

Emotion recognition and biometric categorisation: information obligations

As of **August 2, 2026, Article 50 of AI Act** takes effect, introducing **transparency obligations** also for those who use AI systems in their professional activities under their own authority (deployer).

In particular, anyone who uses **emotion recognition** or **biometric categorisation** systems must **inform** the individuals concerned **in advance** about how the system works and must process **personal data** in accordance with data protection regulations (GDPR).

On the operational side, it is therefore essential **to identify the AI systems in use** (e.g. access gates and attendance monitoring systems, contact centres with voice tone analysis, and retail analytics using customers' facial data).

Furthermore, it is advisable to check whether the system is subject to **the prohibition** set out in Article 5: from 2 February 2025, emotion recognition in the workplace and in educational establishments (except for medical or security purposes) and biometric categorisation aimed at inferring sensitive data will be prohibited.

If the systems used are not subject to the prohibition, **clear notice** must be provided, at the latest at the time of first exposure.
This notice may be incorporated into the **privacy notice**, but a simple clause or reference is not sufficient, as the two notices must in any case be separate and distinct.

Although the obligations for high-risk systems have been postponed until 2 December 2027 (Digital Omnibus), breaching transparency obligations already exposes organisations to **fines** of up to €15 million or 3 per cent of annual global turnover.
It is therefore advisable to review the notices in place and amend the contractual clauses in contracts with suppliers.

Risk Management

The Risk Manager's Added Value in AI Governance

Risk management often enters an organisation only after damage has occurred or a threat has become impossible to ignore.

With **AI**, however, waiting means falling behind: we are in an exploratory phase where opportunities and consequences evolve together.

The **Risk Manager** plays a pioneering role: researching, understanding and anticipating, because capabilities may produce equally significant impacts.

The method remains the **risk assessment** process: risk identification, risk analysis and risk evaluation, followed by **risk treatment**.
Identification cannot be reduced to a data-processing questionnaire.
The Risk Manager must step into the field and engage with marketing, production, finance and every function using AI, mapping use cases and risk sources.

Discriminatory content, unverified AI outputs in production or disclosure of confidential data are different but **interconnected risks**.

Limited historical data makes likelihood and impact difficult to estimate. Still, the Risk Manager must build a **risk map** and compare residual risk with corporate **risk appetite**.
A non-critical error may be tolerable if less frequent than human error; exposure to data breaches or cyberattacks is not.

The Risk Manager's added value emerges in the development of a risk treatment plan.
It is therefore essential to define **authorised GenAI tools**, guidelines and internal **procedures**, as well as technical measures to ensure data **security**, in addition to **training** staff on AI and keeping management informed.
The aim is not to impose blanket bans, but to provide practical rules and tools that turn risk into informed adoption and AI into **value for the business**.