November 2026

&Compliance Risk Management

New regulation and practices for data governance and business risk management

AI Governance
Providing and Using AI Systems: Instructions for Use and Responsibilities Across the Supply Chain 2

D.Lgs. 231/2001
Digital Service Providers and Risks under Leg. Decree 231/2001: Why Supply Chain Audits Are Becoming Essential 3

Privacy | AI | Cyber
The importance of the appointment of a data processor pursuant to Article 28 GDPR 4

Risk Management
NIS2 and supply chain security: the obligations also apply to those not subject to this regulation 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** e **Edoardo Lazzaro**

November 2026

AI Governance

Providing and Using AI Systems: Instructions for Use and Responsibilities Across the Supply Chain

When a company purchases an **AI system** for use in its business operations, who is responsible for ensuring compliance and managing the risks associated with its use? The **AI Act** distinguishes between those who develop, or have developed, an AI system and place it on the market under their own name or trademark (providers), and those who use the system under their authority (deployers). These are distinct roles, each carrying separate but closely interconnected obligations.

For **high-risk AI systems**, **providers** must supply instructions for use setting out the system's intended purpose, capabilities, limitations, risks and human oversight requirements. **Deployers**, in turn, must use the system in accordance with those instructions, ensure appropriate human oversight and monitor its operation. The **instructions for use** therefore serve as a key link between the obligations of those who provide AI systems and those who use them.

Supply agreements also play a central role. They should address access to documentation, updates, technical support and cooperation in handling malfunctions and incidents. It is also important to bear in mind that, under certain conditions, substantial modifications to a system or changes to its intended purpose may result in a deployer assuming the obligations of a provider.

Effective **risk management** therefore requires both parties to have a clear understanding of the system's characteristics, the conditions governing its use and their respective **responsibilities**.

November 2026

D.Lgs. 231/2001

Digital Service Providers and Risks under Leg. Decree 231/2001: Why Supply Chain Audits Are Becoming Essential

The outsourcing of ICT services, cloud infrastructure and digital platforms to external providers has become an increasingly widespread practice among businesses. **Such reliance, however, entails risks** that may also affect the effectiveness of the Organisation, Management and Control Models adopted pursuant to Italian Legislative Decree No. 231/2001.

Deficiencies in suppliers' organisational and security systems may undermine a company's internal safeguards, exposing it to vulnerabilities potentially relevant to the **cybercrime offences** referred to in Article 24-bis of the Decree. Indeed, the mere outsourcing of an activity **does not relieve a company** of the need to assess its implications for the prevention of predicate offences.

Against this backdrop, the assessment of risks under Legislative Decree No. 231/2001 cannot be confined to internally managed processes but must also encompass sensitive activities entrusted to third parties.
Periodic audits, due diligence and ongoing monitoring therefore play a crucial role in assessing suppliers' reliability, identifying potential shortcomings and verifying the effective implementation of control measures.

The adoption of such safeguards, proportionate to the risks associated with outsourced activities, also enables companies to document the checks performed and the corrective actions taken, **thereby strengthening the effective implementation of the compliance framework established under Legislative Decree No. 231/2001**.

Digital supply chain security thus becomes an integral part of a compliance strategy capable of addressing risks extending beyond the company's organisational boundaries.

Privacy | AI | Cyber

The importance of the appointment of a data processor pursuant to Article 28 GDPR

Every organisation entrusts external parties with activities involving the processing of personal data: payroll processing, cloud services, IT support, CRM and call centers. In such cases, the supplier generally acts as a **data processor**, and Article 28 GDPR requires the data controller to regulate the relationship through a contract or other binding legal instrument.

This is not a mere formality. The data controller may only engage processors who provide sufficient guarantees regarding the implementation of appropriate **technical and organisational measures**. The appointment must therefore be preceded by an **assessment of the third party** (questionnaires, certifications, security measures), which must be documented and updated over time, in accordance with the principle of **accountability**. The appointment agreement must also include certain minimum provisions: processing only on the data controller's documented instructions; staff confidentiality; security measures pursuant to Article 32 of the GDPR; rules on sub-processors; assistance to the data controller (data subjects' rights, data breaches); erasure or return of data upon termination of the relationship; and the **right to audit**.

Failure to designate a data processor, or an unsuitable designation, exposes the company to **penalties** of up to 10 million euros or 2 per cent of its annual global turnover (Article 83(4) of the GDPR). The Data Protection Authority has on several occasions imposed penalties on data controllers for failing to designate suppliers who processed data on their behalf. Furthermore, without a clear contract, it is difficult to monitor the supplier and allocate **responsibilities in the event of an incident**. A supplier who determines the purposes and means of processing is in turn considered a data controller (Article 28(10)).

In view of this, and in light of developments in the regulatory framework, it is essential to map suppliers, assess them and update existing agreements.

Risk Management

NIS2 and supply chain security: the obligations also apply to those not subject to this regulation

Not falling within the scope of **NIS2** does not mean remaining unaffected by its implications. Legislative Decree 138/2024 requires essential and important entities to safeguard the security of the **supply chain**, whilst also taking into account their relationships with direct **suppliers** of goods and services. A supplier may unwittingly become the vehicle for a cyber-attack.

For this reason, even organizations not within the NIS2 scope may receive requests from their clients to adopt ICT and cyber security measures designed to protect their IT and cyber infrastructure and ensure their **resilience**, as well as to detect **security incidents** promptly.

This does not constitute an extension of NIS2 obligations to all suppliers. Indeed, as clarified by Italian Cybersecurity Agency, the requirements must be tailored to the **risk** and the nature of the supply, without indiscriminately transferring every measure envisaged for the client.

The **contract** therefore becomes a key tool: verifiable obligations, notification deadlines, controls and **responsibilities** must be defined, avoiding generic commitments to 'NIS2 compliance'.

For organizations outside the scope of the NIS2 regulatory framework, therefore, **cyber security** is no longer merely a technical issue: it can become a condition for securing a contract or retaining a client.