November 2025

&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**, **Fabio Cecilia**, **Elisa D'Arrigo**

D.Lgs. 231/2001

Compliance under the spotlight: the 231 system tested in the luxury sector

The recent judicial administrations involving brands such as **Loro Piana, Valentino Bags Lab, Armani Operations**, and **Manufactures Dior** have highlighted a common weakness: the lack of control over **third parties** and subcontractors across the supply chain.

In a sector where production is often outsourced, due diligence on suppliers has become one of the main pillars of 231 liability.

Legislative Decree 231/2001 requires a preventive approach capable of identifying and managing risks of labor exploitation, irregular work, or unethical practices, even among business partners. A merely formal compliance model is not enough: companies must implement systems of **assessment, monitoring, and traceability** involving every player in the value chain.

In the world of luxury, compliance has become a true mark of authenticity. Ensuring effective oversight of suppliers and subcontractors means protecting not only legality but also the image and value of the brand.

In this context, reputation is the ultimate luxury to be safeguarded.

Privacy | AI | Cyber

How to make the privacy notice more understandable to third partiesi

Personal data protection legislation requires the Data Controller to **inform** data subjects (natural persons whose data are processed) about the purposes and methods of processing their personal data. The GDPR itself also states that the privacy notice must be **clear, easily accessible, and written in simple and understandable language.** However, in most cases, it presents itself as a long, technical and difficult to understand document.

To improve its communicative effectiveness, it is therefore essential to adopt measures and strategies that facilitate its reading and comprehension.

In particular, it is important to avoid technicalities and complex legal formulas, while, on the visual side, it is essential to organise the information into thematic sections, with clear titles and bullet points.

Moreover, the use of **infographics, icons** and diagrams typical of **legal design** can greatly facilitate the reading and understanding of a document that, statistically, is ignored by (web) users because it is boring, long to scroll through and difficult to understand, while at the same time making it more “catchy”.

On the practical side, adding FAQs at the bottom of the document and including interactive links could help users clarify any doubts.

Therefore, making privacy notice more understandable is not only a regulatory obligation, but also an opportunity to **strengthen user trust** and promote a more data protection-aware culture.

Risk Management

Risk in the supply chain: the importance of Third Party Risk Assessment

In an increasingly interconnected market, a company's strength also depends on the reliability of its partners. **Managing risk within the supply chain** has become one of the most critical areas of corporate compliance, as misconduct by suppliers, subcontractors, or consultants can result in serious legal, reputational, and financial consequences.

The **Third Party Risk Assessment** is the key tool to prevent such risks: it enables organizations to evaluate the integrity, soundness, and compliance of external entities both before and during the business relationship. Assessing parameters such as governance, environmental sustainability, respect for labor rights, and reputational history helps build a **transparent and resilient supply chain.**

International best practices draw inspiration from ISO standards, such as ISO 37001 (anti-bribery), ISO 20400 (sustainable procurement), and ISO 31000 (risk management), which promote a **systematic approach** to third-party assessment. On a practical level, many companies use standardized **due diligence questionnaires**, such as those under Sapin II – common among French-based groups – or Ecovadis assessments, which integrate ESG indicators and ethical criteria to monitor supplier performance over time. Other platforms, such as Sedex, IntegrityNext, or TRACE, further ensure compliance with ethical, social, and anti-corruption principles throughout the supply chain.

The Italian Legislative Decree 231/2001 reinforces this need by requiring organizational models that also cover activities outsourced to third parties. In a context where responsibility extends across the entire **value chain**, implementing structured processes for continuous third party assessment and **monitoring** is not only a protective measure but also a genuine competitive advantage.