ANDERSEN®

July 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** and **Edoardo Vittorio Lazzaro**

D.Lgs. 231/2001

## When monitoring an employee's emails may constitute a predicate offence under Legislative Decree 231/2001

Access to employees' work emails is not always lawful. In certain circumstances, the way in which a company monitors an employee's email may constitute actual offences relevant to the **liability of the organisation** under Legislative Decree 231/2001.

The risk arises when a manager, without authorisation, **accesses an employee's email, uses login details** that are known or have been obtained without consent, **retains access** to the account after the employment relationship has ended, **monitors** emails systematically or **acquires** the content of emails without meeting the conditions laid down by law.

Such conduct may constitute the offences of unauthorised access to a computer system or the unlawful interception of computer communications, both of which are included amongst the offences that may give rise to **the organisation's liability under Article 24-bis of Legislative Decree 231/2001**.

The risk to the organisation increases when checks are carried out to **obtain confidential information** about the employee, **prevent disputes**, gather evidence for use in disciplinary proceedings or **gain organisational advantages** for the company.

Unclear monitoring procedures, a lack of formalised authorisations and shortcomings in IT protocols can turn an internal audit into a significant 231 risk: prevention relies on **clear policies, documented authorisations and targeted training**.

Privacy | AI | Cyber

## Corporate email: the importance of a procedure to ensure GDPR-compliant use

Many companies still regard work emails as merely an operational tool, forgetting that these messages actually contain large amounts of personal data (including sensitive data) relating to employees, customers and suppliers.

Without specific internal regulations, the **risk of non-compliance with privacy regulations** is very high for any business, regardless of its size.

The Data Protection Authority has repeatedly emphasised that employers must never indiscriminately monitor employees' correspondence.

Even after the employment relationship has ended, the email account cannot remain active indefinitely, nor can emails be systematically and automatically forwarded to a line manager.
Such practices, in fact, do not comply with the **principles of data minimisation, transparency and storage limitation** set out in the European Regulation.

To prevent security incidents as well as to avoid litigation or penalties, every organisation must adopt a specific **procedure for the use of email**.

This policy must define the proper **methods for using email accounts, the requirements for email account login credentials, the maximum retention periods** for correspondence, the **methods of access** by the company, the circumstances under which **monitoring** may be conducted in accordance with privacy and labor laws, **the management of terminated accounts**, and the **consequences of non-compliant conduct**.

Conscious and compliant management of corporate email provides essential protection for a business's information assets and reputation. Implementing an internal procedure reduces legal risks and turns compliance into a tangible competitive advantage in the market.

Risk Management

## Identifying and mitigating the risks of cyber-attacks delivered via email

Email remains one of the primary vectors for cyber-attacks. Phishing campaigns and malware distribution increasingly exploit the **human factor**, persuading users to disclose confidential information, compromise their credentials, or authorise fraudulent transactions, often through nothing more than a single "click" on an email attachment or embedded link.

Managing this risk cannot rely solely on technological safeguards. It requires a **governance** framework that integrates technical, organisational and procedural measures, based on prior **risk assessment** and a clear allocation of roles and responsibilities.

Ongoing staff **awareness and training**, procedures for verifying unusual requests, well-defined incident **response protocols**, and the periodic review of implemented safeguards are all essential components of an effective and resilient **security** framework.

Against a regulatory landscape that places increasing emphasis on **cyber resilience** and organisational **accountability** (including AI Act, DORA, NIS2, CER and GDPR), the security of electronic communications is no longer merely a technical safeguard.

It is a fundamental element of sound corporate governance and of the protection of an organisation's information assets.