QUOTIDIANOPIÙ

Lunedì 13/07/2026 • 05:00

LAVORO ENGLISH VERSION

Ex-Employee Access to Company Devices: A Case of Overprotection?

The **Italian Data Protection Authority** has sanctioned a company over the way it handled **a former employee's access to personal emails and files**: a ruling that may seem excessive, but one that offers valuable insight into **internal policies**, **data retention periods**, and the **proactive management** of access requests.

di Luca Failla - Avvocato Managing Partner Failla&Partners Studio Legale

di Paola Salazar - Avvocato in Milano

The ongoing technological evolution, coupled with changing approaches to the **monitoring and the protection of privacy**, is beginning to create new complexities in the management of **employment relationships**. European and national legislation on Artificial Intelligence – more specifically EU Regulation 2024/1689 (and the Omnibus Package of simplifications) on one hand, and on the other hand Italian Law No. 132/2025 and its internal implementing decrees – introduces **technical and organisational adaptation requirements** and compliance rules that are necessarily intertwined with the provisions of **GDPR** (EU Regulation 2016/679) and also with the guidelines and measures issued by the national **Italian Data Protection Authority** (Garante Privacy).

In this context, whilst this complex regulatory framework has ultimately led the Italian Supreme Court to **allow data collection** through specific technical tools (such as through **workplace access badges** - as per the recent Italian Supreme Court ruling No. 7985/2026) - the Italian Data Protection Authority on the flip side appears to **increasingly restrict the scope for the legitimate exercise of organisational powers** within the companies.

Whilst it appears legitimate to restrict the use of tools designed to create forms of covert surveillance – particularly today when supplemented by applications involving AI technologies (see Provision No. 342 of 14 May 2026) – it is, at the same time, difficult to understand the reasons behind the **particular rigour** with which the Italian Data Protection Authority penalises the **legitimate exercise of managerial and organisational power** in the Italian workplace.

Accessing

Former Employee's Access to Email and Personal Files

The most recent example is Provision No. 165 of 12 March 2026, where the Italian Data Protection Authority has once again ruled on the matter of access to data and, in particular, on access – at an employee's request – to **documents and personal files** stored on the workplace computer and in the **company email account**.

In this specific case, the issue centred primarily on the methods used by the company to store employees' documents and personal data. In this area, the Italian Data Protection Authority's primary concern now appears to be the **intermingling of personal data and business data** - particularly where there is a need to allow access to personal data. Hence, situations where the objectives of data protection also affect the way in which business data are managed.

This topic arose from a request made by a former employee who, following the termination of the employment relationship, had submitted several requests for access to their desktop and email account in order to retrieve personal documents. In response to these requests, the company organised a series of face-to-face meetings to **assist the employee in retrieving the requested data** - first providing access to their personal emails and subsequently also to the documents relating to their employment relationship. The documents had been duly **anonymised** by the company with regard to personal data relating to third parties, but the employee contested this procedure because it caused the "*cancellation of many elements*". Upon the termination of the employment relationship, the Company had, amongst other things, **disactivated the email account** – providing the forwarding for 14 days – and subsequently deleted the account after taking a backup for the purposes of preserving company data (required to be retained for 5 years).

Following an analysis of the facts, and taking into account the employee's request for access, the manner in which the request was handled and, above all, the prescribed data retention periods (5 years for the mailbox backup and 12 months for browsing metadata), the Italian Data Protection Authority declared the employer's conduct unlawful – and issued a fine.

The Italian Data Protection Authority considers that the employer's practice of carrying out **prior screening of emails** contained in the inbox, as well as the subsequent blocking of access, constituted an **infringement of the employee's rights and freedoms** regarding their data access rights. The employer's defence which was primarily aimed at protecting **company data** - including the prevention of the disclosure of trade secrets - was considered irrelevant by the Italian Data Protection Authority.

The Italian Data Protection Authority considered that, in situations of this kind, the **data controller** should be able to **demonstrate** that restrictions on the right of access are justified by **legitimate organisational grounds** - including the need not to prejudice the rights and freedoms of individuals other than the data subject - emphasising that in such cases the right of access may only be restricted in the event of relevant unfounded or excessive requests.

Rationale Behind the Decision and Practical Takeaways

Ultimately, the Italian Data Protection Authority bases its approach on EU Regulation 2016/679 – which starts precisely with the **concept of 'processing'** as defined in Article 4, - and also encompasses the storage and organisation data rules.

Articles 13, 14 and 15 are then taken into account. These require the provision of an appropriate privacy notice which sets out the methods and purposes of data processing, taking into account the **principle of data minimisation**, and therefore a retention period for the information that is proportionate and appropriate to its purpose. It is within this framework that employers must find their own approach to defining the most appropriate technical measures for data management as well as identifying the best organisational solutions suited to and consistent with the GDPR.

Although in this specific case the employer lacked particularly detailed internal regulations regarding the limits on the use of email accounts (particularly with regard to the backup procedures and data retention periods) – requirements for organisational compliance that are today indispensable – it is nonetheless true that a 'systemic' examination of the measure leads one to **consider it, in this specific case, to be excessive**. It is precisely from an examination of its critical issues that some **useful points for reflection** emerge.

The Italian Data Protection Authority declares that the **line between what relates to the workplace and what constitutes 'personal data' is indeed very thin**. It would therefore be advisable for the employers to put in place systems for the classification and structured storage of all company documentation and activities (including email) - rather than relying solely on systems for identifying individual emails. This would lay the groundwork for making the use and retention of data (all data, including aggregated data derived from email) more traceable and thereby safeguarding the company's information assets and reducing risks in the event of a (legitimate) request for access by employees.

These are issues which – partly due to technological developments – are closely linked to the need to draw up **appropriate, detailed and effective internal policies**. It is always useful (if not now essential) to implement company regulations that comprehensively and exhaustively define and communicate the technical rules and procedures for the use of IT tools, including restrictions on the personal use of all work tools (including email accounts), accompanied by a **privacy notice** that specifies in detail :

- the purposes and methods of processing,
- the legal basis,
- the category of data processed,
- the retention period,
- the data subject's rights and (where applicable),
- the existence of any automated decision-making processes - as required by Italian law (Article 13 of the GDPR, Article 1bis of Legislative Decree No. 152/1997; Article 11 of Law No. 132/2025).

A Proactive Approach to Access Requests

Another critical aspect that emerges from this case is the **practical predictability of such requests**: access to data can no longer be treated as an **exceptional occurrence** but must, on the contrary, be embedded within a **defined procedural framework**, enabling the company to respond to requests in an appropriate, timely and verifiable manner.

It is necessary to **identify those responsible** for handling data access requests, the processing times, establish objective criteria for data extraction, and provide for **standardised techniques** for data masking or pseudonymisation, accompanied by a detailed justification of any restrictions. Every stage of the process should be **documented and tracked** – including with the assistance of the Data Protection Officer (DPO), who is responsible for the most complex technical assessment procedures – so as to be able to demonstrate, even *ex post*, the correctness of the choices made (also in light of the numerous and far-reaching guidelines periodically issued by the Italian Data Protection Authority).

Conclusions

In conclusion, this measure sets out a clear principle: the **management of email** requires a structured approach that is consistent with the principles of **transparency, data minimisation and accountability**. The individually assigned corporate email account remains a hybrid space, where organisational needs, employees' rights and the company's interests intertwine, requiring the employer to maintain high standards of analysis, management and compliance. **It is no longer a question of determining '*whether*' to grant access, but '*how*'**: the focus shifts from the individual decision to the robustness of the system underpinning it. **Compliance therefore hinges on *ex ante* measures** – the ability to design retention systems, policies and non-standardised procedures that make the volume of requests manageable and defensible.

However, there remains a **degree of uncertainty**, which suggests a prudent and well-documented approach to managing this complex matter within the organisation.

The message is clear: corporate email is no longer merely a technical tool, but instead a working tool that must be regulated in a precise manner. **Where organisation is lacking, risk increases**; where there is a systematic approach - compliance and efficiency are strengthened and thereby avoid negative consequences and repercussions for employers.