Employees' Right to Personal Data Protection After Termination of Employment: Analysis of the Practice of the Belgian and Italian Data Protection Authorities

A data subject has the right to access and protect their personal data processed by another party, as guaranteed by both the EU General Data Protection Regulation ("**GDPR**") and the national legislation of EU Member States.

This right is unquestionably exercised during the employment relationship, but recent practice confirms that issues concerning the right of access, erasure, and restriction of processing do not automatically end with the termination of employment.

This article analyzes two decisions of European data protection authorities:

- Belgian GBA/APD, No. 158/2025, dated 7 October 2025, and
- Italian DPA, No. 10162267, dated 10 July 2025.

Case Background

In the first case, the data subject had previously served as a director at a Belgian company (the employer and controller). After the termination of employment, the employer failed to deactivate the individual's professional email account and company mobile phone number. The data subject claimed that personal communications remained linked to these accounts and were still accessible and reported the matter to the Belgian Data Protection Authority ("**GBA/APD**"). The employer argued that the phone number was owned by the company and that the email account would soon be closed.

In the second case, a professor filed three complaints with the Italian Data Protection Authority ("**Garante**") against his former employer, an Italian university, claiming that as a controller it had:

- failed to deactivate his work email account and delete his communications after termination;
- unlawfully published his personal data on the university website;
- rejected his requests for access and erasure, as well as his objection to data processing.

In both cases, the data subjects alleged unlawful processing by the controllers and violations of GDPR provisions.

Decisions of the Authorities

Belgium – GBA/APD

The GBA/APD found that the controller:

- failed to comply with the principles of purpose limitation, data minimization, and storage limitation under Article 5(1)(b)(c) GDPR, as the data was no longer used for professional purposes but continued to be processed after the termination of employment (i.e., the company failed to deactivate the email and phone number);
- did not inform the data subject about the processing nor act on the request for erasure, violating the data subject's rights under Articles 12, 13, and 17 GDPR;
- lacked a lawful basis for continued processing after the end of employment, as the contractual purpose of processing had ceased and no other legal basis (such as consent or legitimate interest) existed, thereby violating Articles 5(1)(a) and 6(1) GDPR.

Given the controller's cooperation and the fact that the company was in liquidation, a warning was issued instead of an administrative fine.

Italy – Garante

The Garante confirmed that the employer, acting as controller:

- failed to deactivate the professor's email account and delete his communications after the termination of employment, violating Articles 5(1)(a)(e) and 6 GDPR;
- unlawfully published the professor's personal data and the personal data of other individuals on the university website, violating Articles 5(1)(a) and 6 GDPR, as well as relevant provisions of Italian data protection law;
- rejected the professor's requests for access and erasure without providing justification, thereby violating Articles 12(3), 17, and 21 GDPR.

The Garante emphasized that termination of employment does not relieve the controller of the obligation to respond to access requests, as the right of access covers all personal data, including data already known to the data subject.

The controller was fined **EUR 8,000.**

Conclusion

Both cases confirm that t**ermination of employment does not automatically extinguish the data subject's rights to access, erase, or control their personal data**. Even after employment ends, the controller must:

- deactivate professional accounts and tools that allow access to personal data;
- respond to requests for access, erasure, or restriction of processing;
- provide an explanation if a request is rejected, including information on the data subject's right to lodge a complaint with the competent data protection authority.

The decisions of the GBA/APD and Garante also make it clear that **merely invoking legal necessity or the need to defend legal claims is insufficient**, the controller must demonstrate that the processing is **specifically necessary** for the establishment, exercise, or defense of a legal claim.

This article is for informational purposes only and does not constitute legal advice. If you need further information, feel free to contact us.