Former employee email accounts and GDPR: lessons from an Italian DPA fine

26 November 2026 · 4 min read · blogs.iictp.org/former-employee-email-account-gdpr-access-request-fine

Short answer: under the GDPR, keeping a former employee's email account active and readable for months can be unlawful, according to an Italian Data Protection Authority decision summarised by the European Data Protection Board on 18 November 2026. The authority fined Techpartner S.r.l. EUR 25,500 for a late reply to an access request and for its handling of corporate email accounts. It matters because many companies have similar offboarding rules.

TL;DR The short version

- Italy's data protection authority fined Techpartner S.r.l. EUR 25,500 for a late reply to an access request and for how it handled corporate email accounts.
- Keeping a former employee's mailbox active and readable for months can be unlawful under the GDPR.
- Review offboarding: close or redirect accounts promptly, tell people what happens to their mail, and answer access requests on time.

Read online, listen to it, or change the text size: https://blogs.iictp.org/former-employee-email-account-gdpr-access-request-fine

What happened?

A former employee complained about an inadequate response to a request for access to personal data processed during employment. The authority also examined the company's internal rules on individual corporate email accounts, including what happened after employment ended. The final decision is dated 20 October 2026.

How the violations arose

- The company missed the GDPR deadline and replied only after the authority opened its investigation, about nine months after the request.
- Internal rules let former employees' accounts stay active for three to six months after departure.
- Incoming messages could be read during that period.
- The authority found this incompatible with lawfulness, data minimisation and storage limitation.

What the findings add for practice

The useful point is that the written policy itself was examined, not only one incident. The authority confirmed infringements of Articles 5(1)(a), (c) and (e), 12(3) and 15. Other allegations, on video surveillance and occupational medical information, did not result in established infringements.

Figures reported by the source

- EUR 9,500 for failing to answer the access request in time.
- EUR 16,000 for unlawful processing involving corporate email accounts.
- EUR 25,500 in total.
- 60 days from notification to bring internal IT policies into compliance.

Limitations and open questions

- This is one national authority’s decision on particular facts, summarised in English by the EDPB; the Italian text governs.
- The summary does not set a permitted retention period for departed staff mailboxes.
- Employment, telecommunications and secrecy law differ between countries and may add duties. This is not legal advice. Sources were read on 26 November 2026. Products, rules and standards change, so check the linked originals before you rely on any detail.

How to fix offboarding

1. Read your current mailbox rules and note how long accounts stay active and who can open them.
2. Disable the account promptly on departure and use an automatic reply that gives another business contact, subject to local law.
3. Move business records you must keep into a controlled system before closure, with a stated legal basis and period.
4. Stop forwarding or reading new personal messages.
5. Log access requests on receipt, assign an owner and diary the one-month response deadline and any lawful extension.
6. Test the process with a sample departure and a sample request.

What it means for employment and privacy lawyers

Check the IT policy, not only the privacy notice. A rule written for business continuity can create a standing breach each time it is followed. Access requests from former staff often arrive alongside employment disputes, which is when missed deadlines are most likely to be reported.

Frequently asked questions

- **Can an employer keep a former employee’s email account open?** In this case three to six months with reading of incoming mail was found incompatible with GDPR principles; check your national position.

- **How quickly must an access request be answered?** The GDPR generally requires a response within one month, with extension in limited cases.
- **How large was the fine?** EUR 25,500 in total.
- **Was every allegation upheld?** No. Allegations on video surveillance and medical information were not established.

Related reading

- EDPB on onward transfers and model clauses
- What is least privilege?
- AI in meetings and connected apps
- TPBOK standard

> Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. European Data Protection Board (national news). Italian DPA fines a company EUR 25 500 over employee access rights and corporate email accounts. 18 November 2026. edpb.europa.eu/news/italian-dpa-fines-a-company-eur-25-500-over-employee-access-rights-and-corporate-email_en

Published by IICTP, an independent technical credential body, on 26 November 2026. The current version of this post is at https://blogs.iictp.org/former-employee-email-account-gdpr-access-request-fine. More guides: blogs.iictp.org.