



SA Italy

Ours 09.06.2026 nr 2.1-1/25/264-627-21

FINAL DECISION pursuant to GDPR Article 60(8) - [REDACTED]

The Complaint

The complaint (national ref nr [2.1-1/25/264-627-1](#)) was lodged by [REDACTED] (hereinafter: the Complainant) before the Estonian Data Protection Inspectorate (hereinafter: DPI) on 25 February 2025. The Complainant, being the account holder of the email address [REDACTED] alleged a possible infringement of personal data protection legislation by the company [REDACTED] (hereinafter, the 'data controller'), which is based in Italy. The complaint was forwarded to the Italian Data Protection Authority (hereinafter: Garante or LSA) on 24 March 2025. In this specific case, considering that the company [REDACTED] – the data controller in question – has its registered office in Italy, the Garante has declared itself the lead authority in the relevant cooperation procedure initiated under Chapter VII of the GDPR.

More specifically, the complainant stated that:

- the company was sending unsolicited emails containing the complainant's personal data to the complainant's email address, without authorisation and although the complainant had never created an account on the data controller's website;
- the emails were sent with the aim of persuading the complainant to register on the data controller's website;
- the right to erasure under the GDPR was exercised by the complainant on 1, 6, 8 and 9 January 2025, and clarification was also requested as to how their personal data had been collected;
- on 10 January, the data controller replied, informing the complainant that an internal investigation had been launched into the matter;
- on 13 January, the data controller provided a follow-up reply, informing the complainant that the request had been forwarded to the ombudsman and the relevant internal departments;
- following these requests, the complainant received no further communication from the data controller.

The Complainant requested for the Data Controller to answer the question where his personal data (name, surname, e-mail address) was obtained from and then to delete the personal data/account in question.

The Garante conducted a fact-finding procedure and requested the data controller to provide clarification on the matter. Eventually the Grante adopted a draft decision proposing the adoption of a final decision to dismiss the complaint and order its transmission, pursuant to Article 60(3) of the Regulation, to the Estonian Supervisory Authority for the adoption of the final decision, pursuant to Article 60 (8) of the Regulation.

In accordance with GDPR Article 60(8), Estonian DPI, as the supervisory authority with which the complaint was lodged, hereby adopts the final decision as proposed by the Garante.

Decision of the Italian Data Protection Authority

The Garante did not find any infringements of the GDPR, especially considering that the data controller had stated that the data subject's personal data was collected through the registration on the official website as part of his participation in a meeting and has confirmed the deletion of the data subject's personal data. Therefore the Garante dismisses the complaint and procedure is closed.

The supervisory case

Fact-finding by LSA

On 29 May 2025 (Case File No. 77907/25), pursuant to the combined provisions of Articles 58(1)(a) of the GDPR and Article 157 of the Code, the Garante requested the data controller to provide clarification, setting out the provisions regarding false statements, certifications, submissions or documentation to the Garante (Article 168 of the Code) and informing the data controller of its role as the lead authority under the 'one-stop shop' mechanism, pursuant to Article 56 (6) of the GDPR, since the controller's single establishment is located in Italy.

On 5 June 2025 (Case File No. 80242/25), the data controller replied to the letter from the Garante, stating that: the data subject's request had been fulfilled prior to the Authority's intervention; that all data relating to the email address [REDACTED] had been deleted, thereby eliminating the risk of any emails being sent to the data subject; as demonstrated by the email dated 1 January at 3:13 am and by screenshots Nos. 5 and 6, some of the communications sent from the data subject's email address presented the typical characteristics of a phishing attempt and that, as a result, in accordance with internal security procedures, the Company had immediately ceased all communication with the data subject.

The controller's reply was forwarded to the Estonian Authority via procedure IMI VMN 773188, which then forwarded it to the complainant, who requested specific clarification regarding: where the controller had collected their personal data (first name, surname, email address); the erasure of their personal data; and the phrase 'characteristics typical of a phishing attempt' used by the data controller in reference to the emails received from the data subject.

On 22 July 2025 (Case File No.103032/25), the Garante sent a request for further information containing the complainant's requests, to which the data controller replied by letter dated 31 July 2025 (Case File No. 107366/25), stating that: the data subject's personal data had been collected through registration on its website in the context of a meeting; it had received several emails from the data subject containing clear evidence of spoofing and phishing activities; these emails had been classified as dangerous because they were sent from a non-institutional and generic email address, using a misleading subject line, presenting the email as originating from the 'European Union', and employing the flags and emblems of the European Union; consequently, in accordance with its internal security policy, the data controller ceased all communication with the data subject and classified the emails as an attempt at social engineering; the data subject's details had been deleted from the Company's databases, with the sole exception of the email regarded as fraudulent, which the Company retained for internal audit purposes and any subsequent investigations.

On 11 November 2025, the Estonian Authority, via IMI procedure VMN 845354, asked the Garante whether it had verified the controller's claims also in relation to the indication that the complaint be dismissed.

On 3 December 2025, the Garante replied to these remarks, stating the following via the same IMI procedure:

- the request for information addressed to the data controller had been sent together with a relevant reference to the criminal liability consequences arising from making false statements to the supervisory authority pursuant to Article 168 of the Code;
- the email sent by the data subject was to be regarded as potentially harmful or, at the very least, suspicious due to the use of the EU's official names and emblem;
- as the preliminary investigation phase was still ongoing, the Authority had not yet sent the notice of initiation of proceedings to the data controller and could, therefore, dismiss (not reject) the complaint. In this regard, the Garante referred to the decision of the CJEU (C-768/21, *TR v Land Hessen*) on the discretion of the supervisory authority (with particular reference to the interpretation of Article 57(1)(a) and (f), Article 58(2), and Article 77(1) of Regulation (EU) 2016/679 (the GDPR), in which the Court ruled that, where a personal data breach is established, the supervisory authority is not required to exercise a corrective power if such action is not appropriate, necessary or proportionate to remedy the shortcoming identified and ensure the full application of such Regulation.

Based on the documentation in the file, and in particular given that the Complainant registered voluntarily on the company's website and that the data had been erased prior to the Authority's intervention, the Garante, by means of IMI VMN 845354, informed the initiating country (the sole authority concerned) of its intention to draw up a draft decision pursuant to Article 60, (3) of the GDPR to enable the Estonian Authority to adopt the final decision, in accordance with Article 60(8) of the GDPR and EDPB Guidelines No 02/2022 on the application of Article 60 of the GDPR (paragraph 235, formerly 12).

Key provisions of the relevant legislation

GDPR applies to cross-border processing of personal data within the European Union, i.e. to processing carried out in the context of the activities of a single establishment of a data controller within the meaning of Article 4(23)(b) of the GDPR, and that, in such cases, the supervisory authority of the controller's single or main establishment acts as the lead supervisory authority (hereinafter also 'LSA') in accordance with the one-stop-shop mechanism.

In its capacity as LSA, the supervisory authority is required to involve and closely coordinate with the supervisory authorities concerned in the decision-making process, with a view to adopting a joint decision.

In this specific case, considering that the company [REDACTED] – the data controller in question – has its registered office in Italy, the Garante has declared itself the lead authority in the relevant cooperation procedure initiated under Chapter VII of the GDPR.

According to the aforementioned regulation, the controller is *'the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'* (Article 4(7) of the GDPR).

Chapter III of the General Data Protection Regulation (GDPR) grants data subjects a number of rights in relation to their personal data. In particular, the legislation grants data subjects the right to obtain from the data controller confirmation as to whether his or her personal data are being processed and, if so, the right to access his or her personal data and the information listed in Article 15(1) GDPR. Article 17 GDPR gives the data subject the right to request the erasure of his or her personal data if one of the circumstances set out in Article 17(1)(a) to (f) applies.

Furthermore, Article 12 of the GDPR establishes that the data controller *'shall provide information on action taken'* on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request; and that, if the controller does not comply with the request, it *'shall inform the data subject [...] within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy'* (Article 12(3) and (4) of the GDPR).

Reasons for the decision

In light of the documents that the Garante has analyzed, no infringements of the GDPR were found, especially considering that the data controller stated that the data subject's personal data was collected through the registration on the official website as part of his participation in a meeting and has confirmed the deletion of the data subject's personal data. The Garante has taken into account also the fact that the data controller received several emails from the data subject full of clues of spoofing and phishing activities. The data controller classified these emails as dangerous because: they were sent from a non-institutional and generic email address; a misleading title was used, introducing the email as coming from the "European Union"; EU flags and symbols were used inappropriately. In light of the above, the data controller, in accordance with its internal security policy, stopped all communication from the data subject, classifying it as an attempt at social engineering. Moreover there is no evidence that data controller keeps sending email spam.

According to GDPR Article 60(8), by derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

On the basis of the foregoing, and taking into account the Garante's assessment on this case, DPI adopts this final decision pursuant to Article 60(8) of the Regulation.

DPI has notified the complainant thereof (Decision nr 2.1-1/25/264-627-20 on 25.05.2026)¹ and informs the controller with this Final Decision via the Garante.

Respectfully,



lawyer
authorized by Director General

¹ The Complainant shall have 30 days to contest the notification of the closure of the supervisory procedures.