BCLP. Client Intelligent

Insights

BUSINESS EMAILS AND DSARS

HOW FRENCH COURTS ARE REDEFINING THE SCOPE OF 'PERSONAL DATA' UNDER THE GDPR

Apr 16, 2026

Article 15 of the EU General Data Protection Regulation (GDPR) grants users the right to access their data: this broadly requires that the data subject has the right to know whether their personal data is being processed and if its processing is lawful. This right is often weaponized, creating compliance challenges for large companies who can face abusive Data Subject Access Requests (DSARs). In a recent decision[1], the Court of Justice of the European Union Court held that a DSAR may, under certain circumstances, be considered excessive (and therefore not one to which a data controller needs to respond) if a data controller can demonstrate that the request is made not to verify the lawfulness of the data processing but with the intention of artificially creating the conditions required to obtain redress under the GDPR. The recent EU Digital Omnibus regulation proposal specifically tackles the issue of abusive DSARs, with a DSAR being abusive when this right is exercised *"with the only intent of causing damage or harm to the controller"*[2], rather than to check if personal data is being s processed in compliance with the GDPR.

Another difficulty arises from the interpretation of article 4 of the GDPR, which provides a broad definition of *"personal data"* which could encompass the data subject's business emails (i.e. those sent or received from an employee's work email account). The current debate in France highlights the importance of having a clear and unambiguous interpretation of this provision, as it may have considerable influence on the type and volume of documents that will need to be provided in response to a DSAR.

AN ONGOING DEBATE IN FRENCH CASE LAW

There is a long-running debate in France regarding the interpretation of article 4 of the GDPR, especially regarding business or employee emails.

In a 2025 decision[3] issued by the French *Cour de Cassation* (the highest French court), the Court ruled that "*emails sent or received by the employee through their work email account constitute personal data within the meaning of Article 4 of the GDPR; (…) the employee has the right to access*

these emails, with the employer required to provide the employee with both the metadata (timestamps, recipients, etc.) as well as their content, unless the information requested is likely to infringe upon the rights and freedoms of third parties."

This interpretation of article 4 of the GDPR has significant consequences for employers as it implies the provision of a copy of the entire employee mailbox in response to an employee DSAR.

Nevertheless, this wide interpretation seems to contradict article 4 of the GDPR, which defines personal data as *"any information relating to an identified or identifiable natural person".* An identifiable natural person is a person *"who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

In light of this definition, an email may not contain any identifying information other than the sender's email address, first and last name.

What's more, both the French CNIL and the EDPB provide clear guidance as to how to handle DSARs: The right of access permits the data subject to obtain a copy of the personal data being processed, **but not necessarily a reproduction of the original documents containing such data**. Even though the data controller may provide a copy of the documents containing personal data relating to the data subjects out of convenience, this remains an option rather than an obligation.

The Court of Cassation's extensive interpretation thus creates a divergence of opinion with the position taken by the CNIL and the EDPB on this issue by considering personal data and emails as equivalent. However, it is important to note that this decision was given in a particular context, one in which the employer had refused to provide any kind of document to the data subject without explanation. This context could explain the straightforward, but misleading, wording used by the French Supreme Court.

However, in a recent decision issued by the Paris Court of Appeal[4], the Court seems to correct the misunderstanding.

It reiterates that the purpose of article 15 GDPR is to grant data subjects the capacity to assess whether the processing of their personal data is lawful. The Paris Court of appeal considers that, **unless the claimant proves otherwise**, the only personal data contained in an email is the email address and the name of the data subject. Consequently, there is no requirement to provide the applicant with a copy of their email account; only the personal data it may contain is required. On a different note, it also noted that the other documents or emails which are stored in folders labelled "*private and personal*" do not constitute personal data within the meaning of the GDPR and are therefore not required to be provided in response to a DSAR.

This decision appears to contradict the strict position of the Court of Cassation and to return to a more traditional understanding of what may constitute personal data. It should be noted that, under French law, the case law of the Court of Cassation is generally binding on the Courts of Appeal, and therefore legal practitioners are now awaiting a new ruling from the Court of Cassation.

The Court of Appeals' ruling would now provide grounds for denying a request for bulk disclosure of email data, but it would not allow a data controller to deny access to personal data contained in their mailboxes. This will therefore require a thorough analysis of the personal data a mailbox may contain, particularly to ensure the protection of third parties' privacy, trade secrets, or legal privilege.

BCLP's IP-IT-Data team utilizes proprietary legal tech tools to assist clients when responding to complex DSARs while respecting the rights of the data subject and third parties.

If you would like more information on this topic or assistance with responding to any DSAR you may receive, please contact Pierre-Emmanuel Frogé or your usual contact at BCLP.

---

[1] Court of Justice of the European Union, March 19th, 2026, C-526/24 - Brillen Rottler GmbH & Co.

[2] Recital 35 of the Digital Omnibus Regulation Proposal.

[3] Cour de cassation, Chambre sociale, June 18th, 2025, n° 23-19.022

[4] Cour d'appel de Paris, Pôle 6 chambre 2, December 18th, 2025, n° 25/04270

RELATED CAPABILITIES

- Corporate
- Finance
- Data Privacy & Security
- General Data Protection Regulation

MEET THE TEAM

Pierre-Emmanuel Frogé

Counsel, Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
