Making GDPR access rights workable in practice, reducing the burden on undertakings

Position paper on the proposed amendments to the GDPR in the European Commission's Digital Omnibus

March 2026

This document has been machine-translated from German; the German version is available here.

Summary

With its proposals concerning the General Data Protection Regulation (GDPR) in the Digital Omnibus, the European Commission rightly addresses a problem that has existed since its entry into force in 2018: strategic requests for access by employees tie up considerable human and financial resources of employers, as they often concern large volumes of data accumulated over many years. Small and medium-sized enterprises (SMEs) in particular are often overwhelmed, as they lack the personnel and resources to handle such requests. This constrains entrepreneurial freedom and puts productivity at risk. While the Commission's proposals to amend the GDPR contain important impulses, they fall short of the practical requirements of employee data protection. While the fair handling of employee data is an established and undisputed principle, the Regulation must be improved in a targeted manner to ensure its practical effectiveness:

- Employee data protection must be regulated uniformly across Europe; national derogations must be brought to an end.
- The conditions under which a request for access is considered excessive or otherwise abusive should be clearly defined in Article 12(5) GDPR. In addition, Recital 35 of the Digital Omnibus should be further clarified as guidance.
- Data that employees have themselves created or received must be excluded from the right of access under Article 15 GDPR.
- Information to be provided by the controller at the time of data collection pursuant to Articles 13 and 14 GDPR must be capable of being provided in electronic form.
- For data processing within a group of undertakings, Article 6 GDPR (lawfulness of processing) must provide for a group privilege, including a rebuttable presumption of a legitimate interest.

Abuse can be effectively prevented by adapting the Regulation, provided that the right of access is clearly defined and practicable procedures are available to controllers. This protects employees' rights, relieves

SMEs and strengthens trust in data protection. At the same time, targeted clarifications for data processing within a group of undertakings should facilitate the practical application of the GDPR.

In detail

Ensuring uniform employee data protection across Europe

Article 88 GDPR must be deleted in order to exclude national special rules on employee data protection. Uniform provisions must apply across Europe. Article 88 allows Member States to adopt their own rules on employee data protection. These special rules fragment the internal market, increase compliance costs and create legal uncertainty for undertakings—particularly in cross-border activities.

Defining criteria for excessive requests for access in Article 12 (5)

The text of Article 12 (5) GDPR must set out in a binding manner when a request for access is to be considered excessive. This would establish clearer legal conditions for refusing requests or charging a reasonable fee. The Commission proposal rightly provides that controllers may refuse manifestly unfounded or excessive requests under Article 15 GDPR and, where appropriate, charge a fee where this right is used for purposes other than the protection of personal data. However, it remains unclear when a request is to be regarded as excessive or when such abuse exists. It is not sufficient to address this solely in Recital 35 of the Digital Omnibus Regulation; the GDPR must regulate this clearly and in a binding manner in the legal text itself. A request should, in particular, be considered excessive or abusive where the provision of the information would require a disproportionate effort, where the data subject fails to provide a substantiated justification in the case of repeated requests despite being asked to do so, where the request clearly serves abusive purposes, or where it is objectively impossible to comply with the request. The justification could, for example, be facilitated by a standardised form to be completed. This would also be clear to controllers and, in the event of a dispute, to the courts. In addition, the burden of proof regarding the excessive or abusive character of a request should not lie with the controller, as such behaviour often lies outside its sphere of influence. Instead, the data subject should be required to demonstrate both that the request is justified and how it serves the protection of their personal data. This approach safeguards the legitimate interests of the data subject while at the same time protecting employees' personal data.

CJEU: the purpose of the request for access is not decisive

In practice, requests for access by employees under Article 15 GDPR often do not serve the protection of their personal data, but other objectives—for example, where employees use the right of access to exert pressure in employment disputes. In such cases, the purpose is not to access personal data, but to strengthen the employee's negotiating position, for example regarding severance payments. Employers are often asked to waive the access request in exchange for compensation, turning data protection into a tactical instrument. However, in its judgment of 23 October 2023 (Case C-307/22), the Court of Justice of the European Union held that requests for access may not be refused solely on the basis of purposes unrelated to data protection. A justification of the request is not required. This case law has changed previous practice in Germany: previously, undertakings could reject claims where purposes unrelated to

data protection were evident. This uncertainty makes it more difficult to handle requests for access in a legally compliant manner and increases organisational requirements for undertakings.

Recital 35 as guidance for excessive requests for access

In addition, Recital 35 of the Digital Omnibus must more clearly specify when a request for access is excessive and therefore abusive. It must not replace the binding provisions of Article 12 (5) GDPR, but should clarify how they are applied in practice. The examples of abuse of access rights in the current Recital 35 remain too general. As a result, it is unclear which requests controllers may actually refuse. The Recital should—supplementing the legal definition in Article 12 (5)—set out typical categories of cases in which a request for access is excessive or otherwise abusive. These include, in particular, repeated requests without a substantiated reason and concerning the same data, requests for manifestly irrelevant data, requests aimed at circumventing rules on the burden of proof in civil proceedings, automated or mass requests, as well as broad requests covering multiple categories of data. The deliberate compilation of extensive datasets where only specific information is relevant also indicates abuse. Vague, overly broad or combined requests are likewise clear indicators and should, where appropriate, be treated as excessive. Only such clarifications will make clear which abusive uses of access rights are intended. This creates legal certainty, prevents unnecessary disputes and strengthens trust in fair data protection. It provides undertakings with clear guidance for legally compliant and practicable implementation. The rules protect undertakings from unnecessary burdens while ensuring that legitimate requests for access by employees are reliably fulfilled.

Excluding own data from the right of access

Data that employees have created themselves or can access themselves should not fall within the scope of the right of access. Anyone who writes an email or receives documents already knows their content. Consequently, such data generally requires less protection. Otherwise, undertakings would need to compile large volumes of data—such as entire email inboxes, file systems, or archives—without providing employees with any new insights. This significantly increases the burden while offering little informational value to the data subject. The EU legislator should clarify this by amending Article 15 GDPR and limiting the scope of the right accordingly. In future, undertakings would only need to provide data that the data subject does not already possess or cannot access. The protection of personal data remains unaffected.

Enabling electronic provision of information at the time of data collection

The controller's information obligations under Articles 13 and 14 GDPR should be explicitly capable of fulfilment through electronic means. The legal text should clarify that it is sufficient to provide the name and contact details of the controller at the time of data collection and to refer to further information via an electronic link, such as a URL or QR code. This solution is proportionate and enhances transparency. It avoids duplication and lengthy mandatory texts. Controllers can initially focus on the essential information, giving employees a clear overview while allowing them to access further details as needed. This effectively protects their rights while making it easier for controllers to comply with the requirements. It also facilitates compliance with information obligations—particularly in cases of indirectly collected or historical datasets.

Anchoring a group privilege in the GDPR

The GDPR should explicitly facilitate data processing within a group of undertakings in the employment context. Undertakings often organise human resources, IT or compliance centrally across several entities. However, the GDPR does not provide clear rules for this. The legislator should therefore introduce a group privilege in Article 6 GDPR (lawfulness of processing) for internal administrative purposes. For such data transfers within a group of undertakings, a rebuttable presumption of a legitimate interest should apply. This should also extend to certain health data in the employment context, for example in the administration of sick leave.

Contact:

BDA | DIE ARBEITGEBER
Bundesvereinigung der Deutschen Arbeitgeberverbände
Confederation of German Employers' Associations
Abteilung EU, Internationales, Wirtschaft
T +49 30 2033-1050
eu@arbeitgeber.de
EU-Transparenzregister: 7749519702-29

As umbrella organisation, BDA represents the social and economic policy interests of the entire German business community. It brings together the interests of one million undertakings with around 30.5 million employees. These undertakings are affiliated with BDA through voluntary membership in employers' associations.