

WHEN IS A REQUEST FOR INFORMATION ABUSIVE?

Information on data protection | February 2025

Introduction

The constitutional right to informational self-determination means that data subjects can generally decide for themselves which of their personal data may be processed by which bodies and for which purposes. In order to make use of this right, it is necessary for the data subjects to know what exactly happens to their data. Based on this approach, the General Data Protection Regulation (GDPR) provides for various information obligations for data processors such as companies as well as extensive rights for persons affected by the processing of personal data. One of the central rights of data subjects under the GDPR concept is the right of access, which is enshrined in Art. 15 GDPR.

The right of access under Art. 15 GDPR

The right of access under Art. 15 GDPR is intended to give data subjects the opportunity to become aware of the processing of their personal data and to verify the lawfulness and accuracy of the processed data. The request for information does not have to be justified, nor does a specific format have to be adhered to or a specific communication channel used.

Pursuant to Art. 15 (1) GDPR, a data subject may first request confirmation as to whether personal data concerning them is being processed by the controller at all. If this is the case, they have a right of access to all the information specified in Art. 15 (1) GDPR. This includes the processing purposes, the categories of personal data processed, the recipients of the data, any transfers to third countries, the storage period, the origin of the data and the existence of automated decision-making, including profiling. In addition, Art. 15 (1) (e) and (f) GDPR provide for information on the further rights to which the data subject is entitled. The specific request of the data subject is decisive for the scope of the respective obligation to provide information.

The response to a request for information must be provided immediately, and in any case within one month of receipt of the request (Art. 12 (3) (1) GDPR). The deadline may be extended by a further two months if this is necessary, taking into account the complexity and number of requests. The information must be provided to the data subject in a concise, transparent, intelligible and easily accessible form (Art. 12 (1) (1) GDPR) and, in principle, free of charge (Art. 12 (5) (1) GDPR). Before any information is provided, the controller must verify the identity of the person making the request in order to prevent the data subject's personal data from being disclosed to an unauthorized third party by mistake or through manipulation.

Exceptions to the obligation to provide information in cases of non-identification and misuse

The controller may only refuse to act on a request for information from a data subject if it can credibly demonstrate that it is not in a position to identify the data subject (Art. 12 (2) (2) GDPR).

In addition, in the case of manifestly unfounded or – especially in the case of frequent repetition – excessive requests by a data subject pursuant to Art. 12 (5) GDPR, the controller may either demand a reasonable fee or refuse to act on the request, whereby the controller must provide evidence of the manifestly unfounded or excessive nature of the request. The exemption provision must be interpreted narrowly in principle. Recital 63 (1) of the GDPR states that a data subject should be able to exercise their right of access at reasonable intervals, so that not every repeated request for information is to be regarded as “excessive” and therefore abusive. In this respect, a frequent repetition of requests based on legitimate reasons, such as a change in factual circumstances, is not to be considered excessive within the meaning of the standard. According to the EDPB, the more frequently changes are made to the controller's database, the more frequently a data subject can request information, without this being considered excessive. The Higher Regional Court of Vienna has also ruled that a very extensive request for information that is repeated at regular intervals is not in principle an abuse of rights ([OLG Wien, decision dated 10.06.2024 – Ref. 14 R 48/24t](#); we reported on this in [December 2024](#)). Specifically, it found that a repeated request for information at intervals of three years cannot be considered excessive even if the data situation has not changed between the first and second request for information. However, a frequent repetition of requests for information without any valid reasons speaks in principle of an abuse of rights. The same regularly applies to applications that serve the sole purpose of causing the responsible party effort and harassment ([AG Pforzheim, decision dated 05.08.2022 – Ref. 4 C 1845/21](#)) or that refer to information that is already available ([OLG Düsseldorf, decision dated 13.07.2023 – Ref. I-13 U 102/22, I-13 U 44/23](#)). A high processing effort for the controller ([LG Heidelberg, decision dated 21.02.2020 – Ref. 4 O 6/19](#)) or the pursuit of objectives unrelated to data protection ([ECJ, decision dated 26.10.2023 – Ref. C-307/22](#); we reported in [December 2023](#)) do not in themselves constitute an abuse of rights.

The ECJ's decision on the abusive nature of requests to the supervisory authority

As part of a preliminary reference, the ECJ recently had to deal with the similar question of when requests, in this specific case com-

plaints, from a data subject to a data protection authority are to be considered excessive and therefore abusive and a referral of the matter can therefore be refused ([ECJ, decision dated 09.01.2025 – Ref. C-416/23](#)).

In the case underlying the decision, a data subject lodged a complaint with the Austrian data protection authority because a company did not respond to his request for information within one month. The data protection authority refused to deal with the complaint as it was excessive. The data subject had previously submitted 77 similar complaints within 20 months and regularly contacted the authority by telephone to describe further facts. After the Federal Administrative Court upheld the complaint lodged by the data subject against the decision of the supervisory authority, the Austrian data protection authority turned to the Administrative Court, which subsequently referred various questions to the ECJ for answers. The Administrative Court wanted to know whether the term “requests” in Art. 57 (4) GDPR also includes “complaints” pursuant to Art. 77 (1) GDPR, whether it is sufficient for the existence of an “excessive request” that a data subject makes a certain number of requests or whether an intention of abuse is also required and whether the supervisory authority is free to choose whether to charge a reasonable administrative fee or refuse to process “manifestly unfounded” or “excessive” requests.

The ECJ first states that the term “request” is to be understood broadly, which is why “complaints” also fall under the term. In addition to systemic considerations, this view is supported in particular by the aim of the GDPR to ensure a consistent and high level of protection for natural persons and to strengthen the rights of data subjects. The ECJ pointed out that it is important to ensure the proper functioning of the supervisory authorities, which means, among other things, that they are not hindered in their work by manifestly unfounded or excessive complaints. The ECJ also stated that, according to the wording of Art. 57 (4) GDPR, requests can be “excessive”, especially in the case of frequent repetition. However, it is not clear from the wording whether a high number alone is sufficient for classification as excessive or whether an intention to abuse is also required. In this context, the court points out that a large number of complaints can also be the direct consequence of a large number of cases in which no response was given to various requests for information from a data subject to one or more controllers or in which the request was refused. In this respect, setting a maximum number would impair the rights of the person concerned. The processing of complaints should therefore not be made dependent solely on the number of complaints submitted. Rather, it must be established in each individual case that there is also an intention of abuse on the part of the person concerned, for which a high number of complaints alone is not sufficient. The examination must take into account all relevant circumstances. An intention to abuse can be established, for example, if complaints are submitted without this being objectively necessary to protect rights under the regulation. Abuse can also be considered if a person submits a large number of complaints concerning a large number of responsi-

ble persons to whom the person concerned has no particular connection and the content of the complaints reveals the intention to paralyze the authority. Finally, the court also states that a supervisory authority can choose, by means of a reasoned decision, whether to impose a reasonable fee or refuse to take action in the event of excessive requests. As part of its decision, the authority must take all relevant circumstances into account. It must also ensure that the option chosen is appropriate, necessary and proportionate.

Transferability of the decision to the right of access

The ECJ’s statements on the abusive nature of requests to supervisory authorities can also be applied, at least in part, to the assertion of claims for information against data controllers. The relevant provisions of Art. 12 (5) (2) and Art. 57 (4) (1) GDPR are largely identical in terms of content.

In particular, the finding that a high number of requests alone is generally not sufficient to justify abusive conduct, as there may be noteworthy reasons for repeating the request, is consistent with previous considerations in case law and literature. The same applies to the statement that it is generally necessary to consider the individual case, taking into account all relevant circumstances. A new addition to the previous considerations is that an intent to abuse must also be considered if the data subject’s requests concern a large number of controllers to whom the data subject has no particular connection and no interest in the actual information is apparent.

The statements that authorities should not be hindered in their work by manifestly unfounded or excessive complaints, however, can hardly be applied to the right of access, since it is not the aim of the GDPR to ensure the proper functioning of responsible companies. Furthermore, the ECJ has already ruled that the right of access can be asserted independently of a justification or data protection objectives, so that the consideration that an intention to abuse can be established if requests are submitted without reference to the protection of rights under the regulations cannot be transferred either.

Conclusion

The proper handling of requests for information is of particular importance for companies, as the right of access under Art. 15 GDPR is one of the central rights of data subjects and the responsible company faces severe consequences if it does not comply with the request without justification. Whether a data subject’s request is abusive or not must be assessed on a case-by-case basis, taking into account all other circumstances. As there are currently no generally applicable Supreme Court guidelines for assessing the abusive nature of a right of access, this should not be affirmed prematurely. In cases of doubt, it is advisable to consult the data protection officer.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net

