



Request for access - an update

What you need to know.

The European Data Protection Board recently published [draft guidelines](#) on the right of access (Article 15 GDPR). The right of access is a crucial right under the GDPR. Indeed, it constitutes a 'gateway' to the exercise of other rights that the GDPR grants to affected individuals. The guidelines contain recommendations on how to implement a request for access in practice. So it's time for an update to our previous [Privacy Talk](#) on the right of access. To refresh you, we briefly analyse the core of the right of access below.

In terms of **content**, the right of access has three aspects. Data subjects have the right to (i) ask whether or not personal data relating to them are being processed, (ii) have access to these actual personal data relating to them - a general description or reference to the categories of personal data is not sufficient, and (iii) obtain additional information about the processing of their personal data (such as the purposes of the processing, the recipients involved, retention periods, etc.), tailored to the data subject making the request for access.

Article 15.3 GDPR further elaborates on the **modalities** that a reply to a request for access must meet, thereby supplementing Article 12 GDPR. For example, the data subject always has the right to receive an initial copy of his or her personal data free of charge. If the data subject subsequently requests additional copies, i.e. concerning the same personal data and the same processing period, companies may charge a reasonable fee based on the administrative costs specifically associated with the request. If the data subject submits the request for access electronically, and unless otherwise requested by the data subject, the information should be provided in a commonly used electronic form, i.e. in a format that does not oblige the data subject to purchase specific software.

In principle, a request for access cannot be refused. Nevertheless, some limited **exceptions** are provided. For example, Article 15.4 GDPR stipulates that the right to obtain a copy (the 2nd element of the right of access) shall not adversely affect the rights and freedoms of others, including those of the company concerned (e.g. in terms of business secrets, intellectual property rights, etc.). In this case, the data subject may only receive a copy in which such information has been rendered illegible. Companies may also reject a request for access in accordance with Article 12.5 GDPR if the request is manifestly unfounded or excessive, for example in the case of repeated requests (taking into account

• • • contrast • • • •

how often the personal data are changed and the burden of such a request on the company).

What you need to do.

In principle, you must respond to a request for access regardless of how this request is addressed to you. Thus, the data subject cannot be required to use the communication channels specifically provided by your company for this purpose. A request can be made to any official contact point of your company, such as the e-mail address of an account manager. The response period of 1 plus 2 months then begins to run in accordance with the provisions of [Regulation 1182/71 of the Council of 3 June 1971](#). On the other hand, if a request for access is sent to a completely random or apparently incorrect address (such as e.g. the e-mail address of the cleaning staff), you are not obliged to respond to it.

Companies must verify the identity of the person making the request and, if in doubt, request additional information. This additional information may not be more than is necessary to verify the identity, taking into account the type of the personal data that your company processes, the damage that could result from unauthorised disclosure of the personal data, etc. Do not automatically request a copy of the identity card, since doing so might be disproportionate. For example, a copy of the identity card may not be necessary to verify the identity of a data subject who never had to provide his or her identity card in the first place. In such a case, for example, your company may ask (non-intrusive) security questions. If the data subject does not respond to the request for additional information, you may refuse the request for access.

Unless explicitly stated otherwise, a request for access should be deemed to cover all personal data concerning the data subject. If you process large amounts of personal data, and you have doubts as to whether the request is really aimed at all of the processing operations concerning the data subject, you may ask the latter to specify his or her request. In that case, you should at the same time provide meaningful information to the data subject about all processing operations relevant to him or her, e.g. about the various business activities, different databases, etc. If the data subject confirms that he or she wishes to have access to all personal data concerning him or her, you must still provide full access.

Provided that you have requested the additional information regarding the identity and/or scope of the request without unreasonable delay after receiving it, the response period of 1 plus 2 months only begins to run as soon as you have received the necessary information from the data subject.

The right to a copy of the personal data does not automatically entail that you have to provide the data subject with a copy of the original documents containing his/her personal data. The right to a copy applies only to the personal data undergoing processing. It may therefore suffice to provide an overview of the personal data. It is important that access be provided in such a way that allows the data subject to retain his or her personal data and to come back to it. In other words, verbal information or on-site

• • • contrast • • • •

access is not sufficient, unless the data subject explicitly requests it.

The additional information under the right of access can be based on the information in the record of processing activities and the privacy statement of your company. It may be necessary to update or modify that information according to the specific data subject. For example, it is appropriate to list the recipients (by name) who have actually received the data subject's data. With regard to retention periods, it may be useful to indicate the specific time at which the data will be deleted, or to specify when the retention period actually begins. Please note that the exception of Article 15.4 GDPR does not apply to the right to additional information. Data subjects are therefore always entitled to additional information.

If the request for access involves a large amount of personal data, it may also be advisable to respond to the request for access by taking a layered approach, rather than providing all data and information to the data subject in bulk. In doing so, you should take into account what information the data subject would consider as most relevant. In the context of online data analytics, for example, information about what segment they have been put in should be included in a first layer, while a second layer may include personal data in a raw format about e.g. behaviour on a website.

Finally, make sure that no personal data of the data subject are deleted while you are dealing with the request for access. The reply to the access request should reflect the processing at the moment when the request was made. This therefore also concerns data that are possibly being incorrectly or unlawfully processed.