



YOUR BUSINESS • JUNE 2020

How do I answer a request for access to personal data?

What you need to know.

As a company, do you process personal data (for more information on the concept of « personal data », see [GDPR toolkit - personal data](#))? If so, it would be best to prepare yourself for a data subject access request. After all, as soon as your company processes personal data, the GDPR applies and the data subject has the right to access his or her personal data in accordance with Article 15 GDPR. In concrete terms, the right of access means that the data subject can ask your company (i) whether or not personal data relating to him or her are being processed, (ii) to receive a copy of those personal data and (iii) to obtain information about their processing.

As a company, can you invoke any exception under the GDPR? The basic principle is that you, as a company, cannot refuse an access request. The European Court of Justice has already ruled that a data subject has the right to inspect his or her written examination answers and the examiner's comments on them, because these are personal data. The Italian Court of Cassation has decided that an employee must be given access to the evaluation documents that his employer kept on him or her. Moreover, the underlying motives for the request are irrelevant. In practice it is therefore possible that the data subject will subsequently use the information (in proceedings) against your company. Although you cannot refuse an access request, Article 15.4 GDPR expressly provides that the right of access to personal data may not affect the rights and freedoms of others, including trade secrets and intellectual property rights. In practice, you will have to remove or anonymise this information about third parties.

Today, it seems to be accepted that this right of access does not automatically include a right to a copy of the document containing the personal data and, in any case, does not entail a right of access to the data systems. As a company, however, you are at least obliged to provide the data subject with an overview of the personal data processed in a comprehensible form. This overview is adequate if it enables the data subject to know which personal data are processed and check whether they are accurate and have been processed in compliance with the GDPR.

A request for access must be answered within one month. This period starts as soon as the request is

• • • contrast • • • •

sufficiently clear (who is submitting the request? what is being asked for?). Responding late to a request also constitutes an infringement of the GDPR and can be sanctioned.

What you need to do.

As a company, the first thing you have to do is be prepared for an access request. It is therefore advisable to draw up a procedure for this, e.g. an internal step-by-step plan or standard e-mails, and to give a specific internal person the responsibility for answering these requests. Furthermore, it is advisable to give your employees, especially HR and those in close contact with customers, clear instructions on how to handle the processing of personal data and, in particular, how to take notes.

When you receive an access request from a data subject, it is important that you verify the latter's identity, for example by means of an e-mail address, customer number, a copy of the front side of the ID card or a two-factor authentication via mobile phone. If you provide information about the data subject to the wrong person, this will be considered a data breach.

As soon as you are certain about the identity of the data subject, you must check whether your company is processing personal data about him or her. However, you may always ask the data subject to specify his or her request if your company processes a large amount of personal data. If your company is not processing personal data about the data subject, it is sufficient that you communicate this to the latter. If your company is processing personal data about the data subject, you will at least have to provide an overview of the personal data processed in a comprehensible form. In so doing, you will have to remove or anonymise the information about third parties before granting the right of access. In addition, in accordance with Article 15.1 GDPR, you will have to provide certain information, which must also be included in a privacy statement, but then concretely applied to the data subject. The fact that you had already provided the data subject with a privacy statement does not release your company from this additional information obligation.

The procedure should enable you to reply to the access request within one month. Also take into account the fact that data subjects will not always use the standard procedure as provided for in the privacy statement, but might, for example, get in touch with their regular contact person at your company. So inform your employees about the internal person responsible for such requests and provide the necessary back-ups in case of prolonged absences.