BRANDI
RECHTSANWÄLTE

THE RIGHT OF ACCESS UNDER DATA PROTECTION LAW

Information on data protection I March 2022

Introduction

The right to informational self-determination is enshrined in constitutional law and states that data subjects can, in principle, decide which of their personal data may be processed by which body and for what purpose. In order to exercise this right, it is first necessary for data subjects to be informed about the situations in which personal data is processed and what information about their own person is available to a data controller. Based on this approach, data protection law provides extensive rights for individuals who are affected by the processing of personal data.

One of the central data subject rights under the concept of the General Data Protection Regulation (GDPR) is the right of access, which is enshrined alongside Article 15 of the GDPR in Article 8(2)(2) of the Charter of Fundamental Rights of the European Union. This states that a data subject has the right to request information from the controller as to whether personal data relating to him or her are being processed. If this is the case, the right of access also extends to the communication of the specific data and a more detailed explanation of their processing.

On January 18, 2022, the European Data Protection Board (EDPB) published a guideline on the right of access, in which it discusses the conditions and limits of the claim (Guidelines 01/2022 on data subject rights – Right of access). The guidelines can be used as a supplement for the correct handling of information claims.

Purpose and exercise of the right of access

Data subjects should have the opportunity to inform themselves about the processing of their personal data and to verify its lawfulness as well as the accuracy of the processed data. This makes it easier for data subjects to exercise other rights, such as the rights to the erasure or rectification of data. The assertion of the right of access can therefore serve as preparation for other claims, but is not a prerequisite for this.

Data subjects do not have to justify their request for information and do not have to follow a specific format in their request. The controller should provide appropriate and user-friendly communication channels, also in its own interest to organize the processes as effectively as possible. However, the data subject is not obliged to use specific communication channels; they can also send their request to another, general address of the data controller. Any situation in which a data subject with the right of access is required to follow a specific procedure for this purpose must therefore be avoided; if necessary, the request must be passed on internally.

Scope of the right of access

Pursuant to Article 15(1) of the GDPR, a data subject may first request confirmation as to whether personal data relating to him or her are being processed at all by the controller. Personal data is any information relating to an identified or identifiable natural person. „Processing" means any operation or set of operations which is performed upon personal data, whether or not by automatic means. If personal data relating to the data subject are processed, the data subject shall have a right to access the personal data. In addition, he or she has a right to access further information on the data processing mentioned in Article 15(1) of the GDPR. This includes, among other things, the purposes of processing, the categories of personal data processed, the recipients of the data, the storage period, the origin of the data and the utilization of automated decision-making, including profiling.

Article 15(1)(e) of the GDPR also requires information about data subjects' rights, namely about the existence of a right to the rectification or erasure of personal data, to the restriction of processing, or a right to object to processing. Information about the rights of the data subject are already regularly found in data protection declarations on the homepages of data controllers or in other data protection notices pursuant to Articles 13 and 14 of the GDPR. With regard to the general information obligations, according to Article 13(4) of the GDPR and Article 14(5)(a) of the GDPR, these do not exist if and to the extent that a data subject already has the information in question. However, such a provision is not found in Article 15 of the GDPR with regard to the right of access. Information regarding data subject rights must therefore be provided again when responding to a request for information under Article 15 of the GDPR. In this respect, it differs from the handling of deletion requests: If a data subject only requests the deletion of his or her data, there is no obligation to provide further information in addition to the deletion confirmation. If, on the other hand, a data subject asks for deletion, but would like to receive information about the stored data in accordance with Article 15 of the GDPR beforehand, the additional mandatory information must be provided. For the practical handling of such requests, it is therefore advisable to have appropriate templates available for both cases, which must then be adapted to the specific individual case.

If personal data are transferred to a third country or to an international organization, the data subject also has the right to be informed about the appropriate safeguards pursuant to Article 46 of the GDPR in connection with the transfer (Article 15(2) of the GDPR).

The scope of the duty to provide information is determined by the request of the data subject. The data controller must therefore check whether the request relates to all or only parts of the data processed on the data subject. If the data subject has not specified this, a request is generally to be understood as referring to all data processed on the data subject.

Practical handling of requests for access

The controller should make it easier for the data subject to exercise his or her rights. If the data subject's inquiries are not answered or not answered in a timely manner, the controller may face serious consequences, especially in the event of a complaint by the data subject to the competent data protection supervisory authority. Therefore, in order to respond in a legally compliant manner to incoming requests for information and other requests from data subjects, a coordinated and internally agreed procedure is recommended. To this end, it is prudent to define and document the procedures to be followed in advance.

Establishment of a communication channel for inquiries from data subjects

In order to be able to easily track inquiries from data subjects, it is advisable to set up a separate communication channel for data protection issues, for example an e-mail address provided to the data subjects in the data privacy statement and the data protection information.

In the event that data subjects do not use the specially established communication channel and employees of a data controller receive a data subject inquiry directly, a company procedure to be followed should be defined, for example, forwarding the inquiry to the data protection officer or another person responsible for responding.

Identity verification

Data controllers must prevent the personal data of the data subject from being disclosed, either inadvertently or through manipulation, to an unauthorized third party who may impersonate the data subject. Particular attention must be paid to this in the case of a verbal or electronic request. The company must therefore verify the identity of the inquirer before providing any information. This follows from Article 12(6) of the GDPR. Recital 64 of the GDPR states that the controller should use all reasonable means to verify the identity of a data subject seeking information, especially in the context of online services and in the case of online identifiers. However, a data controller should not store personal data solely for the purpose of responding to possible requests for information.

If the controller has reasonable doubt about the identity of the natural person making the request for information, they may request additional information necessary to confirm the identity of the data subject (Article 12(6) of the GDPR). According to the EDPB, the request for additional information must be proportionate to, among other things, the nature of the data processed and the harm, in order to avoid excessive data collection. In the cases referred to in Article 11(2) of the GDPR, the controller may only refuse to act on the data subject's request to exercise his or her right of access if the controller credibly demonstrates that they are unable to identify the data subject (Article 12(2)(2) of the GDPR).

To ensure identification, data subjects making an oral inquiry should be requested to submit a written request. In the case of an electronic request, it may also be advisable to request additional information to confirm the identity, for example a postal address stored in the customer account. In this respect, it is generally advisable to provide information only to the address stored in the customer account.

Form

After the information requested in the context of a request for information has been obtained internally, for example in the form of a database extract, the controller must provide the data subject with the necessary information. The information must be provided to the data subject free of charge (Article 12(5)(1) of the GDPR).

The information must be provided to the data subject in a precise, transparent, comprehensible and easily accessible form (Article 12(1)(1) of the GDPR). When responding to such requests, data controllers should therefore ensure, among other things, that the language used is clear and simple.

With regard to the right of access, Article 15(3) of the GDPR stipulates that the controller shall provide the data subject with a copy of the personal data that are the subject of the processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on the administrative costs. This does not necessarily mean a paper copy, but generally a transmission of the stored data. If the data subject makes the request electronically, the information shall be provided in a commonly used electronic format, unless the data subject indicates otherwise.

Deadline

The information must be provided to the data subject without undue delay, and in any case within one month of receipt of the request (Article 12(3)(1) of the GDPR). Within this period, the processing of the request must be completed and the result must be available to the data subject. This means that existing claims for information must be completely fulfilled within the one-month period.

The deadline may be extended by up to two months if the complexity and/or number of requests makes this necesssary. The data controller must inform the data subject about the extension of the time limit and the reasons for it within one month of receiving the request.

In practice, it is usually advisable to first send the data subject a brief interim message confirming receipt of the request and offering the prospect of a prompt, final response.

Internal documentation

In order to prove the proper handling of requests for information and other data subject inquiries, and to fulfill the accountability obligation pursuant to Article 5(2) of the GDPR, all external inquiries and their responses must be documented internally. For this purpose, it may be justified to retain both the request and the related correspondence for a certain period of time. This can be justified by the company's legitimate interest in providing evidence of the proper handling of data subject inquiries pursuant to Article 6(1)(1)(f) of the GDPR. The data subject must be informed of the retention of correspondence for purposes of proof. This can be done directly in the first interim communication to the data subject, for example.

Restrictions on the right of access

The GDPR provides for certain limitations to the right of access. The EDPB points out in its policy regarding the limitations that the right of access is not subject to the general condition of proportionality in terms of the effort that the controller must make to respond to the data subject's request.

According to Article 15(4) of the GDPR, the right to obtain a copy of personal data must not affect the rights and freedoms of other individuals. Recital 63 p. 5 of the GDPR cites trade secrets, intellectual property rights and copyright in software as examples of such rights and freedoms. However, according to Recital 63 p. 7 of the

GDPR, the application of the exception rule should not lead to a denial of all information to the data subject. Instead, the EDPB recommends for these cases that the parts that may have a negative impact on the rights and freedoms of others be omitted or made illegible when providing the information. In practical implementation, such parts can, for example, be blacked out.

In the case of manifestly unfounded or - especially in the case of frequent repetition - excessive requests by a data subject, the controller may either charge a proportionate fee, taking into account the administrative costs of the communication or implementation of the requested measure, or refuse to act on the request (Article 12(5) of the GDPR). In this respect, the controller must provide evidence of the manifestly unfounded or excessive nature of the request. The exception provision must be interpreted narrowly. Since recital 63 p. 1 of the GDPR explicitly provides that a data subject should be able to exercise his or her right to information at reasonable intervals, not every repeated request for information is to be considered „excessive". According to the EDPB, the more frequently changes are made to the data controller's database, the more frequently a data subject may request information without this being considered excessive.

Restrictions on the right of access may also result from the national law of the European member states. A corresponding opening clause is provided for in Article 23 of the GDPR. In Germany, such restrictions are provided for in Sections 27 et seq. of the German Federal Data Protection Act (BDSG), to name one instance. According to Section 29(1)(2) of the BDSG, for example, the right of access does not exist if the information would disclose information that must be kept secret according to a legal provision or by its nature, in particular because of the overriding legitimate interests of a third party.

Conclusion

The right to information pursuant to Article 15 of the GDPR is an important aspect in exercising the right to informational self-determination. If requests for information are not answered or not answered in a timely manner, the data controller may face serious consequences. In order to respond in a legally compliant manner to incoming requests for information and other requests from data subjects, a coordinated and internally agreed procedure is to be recommended. To this end, it is prudent to define and document the procedures to be followed in advance.

Controllers must provide the data subjects with the necessary information in a precise, transparent, comprehensible and easily accessible form. In order to prevent the personal data of the data subject from being disclosed to an unauthorized third party by mistake or through manipulation, the controller must verify the identity of the inquirer before providing the information. Especially in cases of doubt, the data protection officer of a controller should assist in processing requests for information.

Johanna Schmale

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M johanna.schmale@brandi.net