

TRANSPARENCY OF DATA PROCESSING

Information on data protection | November 2022

Introduction

The constitutionally enshrined right to informational self-determination states that data subjects can generally 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 in the first place 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, the principle of transparency of data processing is one of the essential principles of the General Data Protection Regulation (GDPR).

The purpose and content of the transparency principle as well as practical implementation tips regarding the fulfillment of information obligations, obtaining consent and answering requests for information will be explained in the following article.

General information on the principle of transparency

Personal data must be processed lawfully, fairly and "in a transparent manner in relation to the data subject" according to Article 5(1) (a) of the GDPR. The last part of the regulation contains the principle of transparency of data processing, which applies to all data processing within the scope of the GDPR.

Purpose

Only if the processing of personal data is comprehensible to a data subject can he or she verify whether the data processing is carried out in a lawful manner. In order to make the processing of personal data by a controller fair and to equalize the imbalance of power and information that typically exists between the controller and the data subject, it is necessary to strike a balance by providing information and facilitating the exercise of rights. Providing information ideally enables a data subject to identify which of his or her personal data is being processed, how it is being processed, and for what purposes. This information is regularly required in order to verify the lawfulness of the data processing in the next step and subsequently to exercise personal rights, if necessary. The transparency of data processing thus serves not only to ensure traceability, but also to review data processing and subsequently possibly to assert and enforce claims by the data subjects.

Content

For natural persons, there should be transparency as to whether personal data concerning them are processed and to what extent this is done or will be done in the future (Recital 39 of the GDPR). The principle relates in particular to information about the identity of the controller, the purposes of the processing and other information ensuring fair and transparent processing, as well as the right of data subjects to obtain confirmation and information about which

personal data concerning them are being processed. Natural persons should be informed about the risks, rules, safeguards and rights related to the processing of personal data and how to exercise their rights in this regard. The exercise of rights pursuant to Articles 15 to 22 of the GDPR should be made easier for data subjects (Article 12(2) of the GDPR).

Practical implementation

The principle of transparency requires that all information and communications relating to the processing of personal data be concise, easily accessible and comprehensible, and written in plain and simple language (Article 12(1)(1), Recital 39, 58 of the GDPR).

The information shall be provided in writing or in another form, including electronically where appropriate. If requested by the data subject, information may also be provided orally, provided that the identity of the data subject has been proven in another form. In order to provide an easily perceptible overview of an intended data processing, information pursuant to Articles 13 and 14 of the GDPR may also be provided in combination with standardized icons.

Special features apply to the processing of personal data of children. If the processing is directed at children, information and notices should be provided in such clear and simple language that a child can understand them, due to their special vulnerability.

The easy accessibility of information pursuant to Articles 13 and 14 of the GDPR as well as of notifications and measures regarding data subjects' rights pursuant to Articles 15 to 22 and 34 of the GDPR are also supported by the fact that these are generally provided free of charge (Article 12(5)(1) of the GDPR). The request for an appropriate fee or even the refusal to act on the basis of a request can only be considered in exceptional cases where requests are manifestly unfounded or - in the case of frequent repetition - excessive, whereby the proof of the manifestly unfounded or excessive nature of the request must be provided by the controller.

Information obligations

In view of the principle of transparency, data controllers have certain information obligations towards data subjects under the GDPR. These are regulated in Articles 13 and 14 of the GDPR. In principle, the controller should not only inform the data subjects about the existence of a processing operation and its purposes, but also provide any other information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed. The information to be provided in detail is explicitly regulated in Articles 13 and 14 of the GDPR.

Article 13 of the GDPR: Collection of personal data from the data subject

Article 13 of the GDPR regulates the obligation to provide information in the event that personal data is collected directly from the data subject. According to Article 13(1) of the GDPR, the controller must inform the data subjects of his or her name and contact details, the purposes and legal basis of the data processing, the recipients of the personal data and information about any transfer of the data to third countries. In addition, information on the storage period and the existence of the data subject rights of the GDPR are also required, among other things.

Since in the case of Article 13 of the GDPR the personal data is collected directly from the data subject, the information should also be provided to the data subject directly at the time of collection.

For practical implementation, it is advisable, for example, to have information sheets available in advance that can be handed out to the data subjects. In the case of data processing in online contexts, the information is usually provided via the data protection declaration on a website.

Article 14 of the GDPR: Data collection not from the data subject

If personal data is not collected directly from the data subject, the obligation to provide information is based on Article 14 of the GDPR. In order to compensate for the lack of transparency caused by the fact that in this case the personal data do not originate from the data subject himself, the provision of additional information is necessary. This encompasses the categories of personal data that are processed, as well as information about the source of the personal data and, if applicable, whether they come from publicly available sources. Due to the nature of the data collection, this information is typically not automatically available to the data subjects when the data is collected.

Due to the nature of the data collection, a different deadline for providing the information also applies to Article 14 of the GDPR. Taking into account the specific circumstances of the processing of the personal data, the information must be provided here within a reasonable period of time after obtaining the personal data, but no later than within one month (Article 12(3)(a) of the GDPR). If the personal data is to be used for communication with the data subject, the information must be provided at the latest at the time of the first communication with him or her (Article 12(3)(b) of the GDPR), or, if disclosure to another recipient is intended, at the latest at the time of the first disclosure (Article 12(3)(c) of the GDPR).

For example, if personal data is used to communicate with the data subject, the information may be provided at the time of the first contact, for example as part of an enclosed notice sheet in the case of communication by e-mail.

Example: Data protection declaration

The fulfillment of information obligations with regard to the data processing that takes place on websites is regularly carried out by integrating a data protection declaration on the respective website. The principle of transparency must be observed in the design of the content, but also in the structure and integration of the data protection declaration.

To ensure that data subjects can access the required information at any time and without great effort, the data protection statement must be integrated transparently into a website. This can be done, for example, via a link in the header or footer of the website. It is important here that the data protection declaration can be accessed from every sub-page. In order to prevent data subjects from long click paths, it should be possible to call it up with a single click.

To make it easier to find, it is a good idea to name the link explicitly, for example as "data protection declaration" or "data protection information".

The data protection declaration itself should also be designed transparently. Structuring the content with clearly highlighted headings can contribute to clarity and make information easier to find. The option of "folding in and out" of the text under individual headings can also help to provide an overview of the information provided.

In terms of content, care should be taken to provide complete information in accordance with Articles 13 and 14 of the GDPR. Clear, simple language also contributes to comprehensibility.

Example: Video surveillance

Video surveillance regularly involves the processing of personal data, about which the data subjects must be informed. At the national level, there are special regulations for video surveillance of publicly accessible areas, which also stipulate that the circumstances of the video surveillance must be disclosed and the responsible body must be named (Section 4(2) of the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)). These specific requirements supplement the general information requirements pursuant to Article 13 of the GDPR. As guidance for the provision of information in the context of video surveillance, the data protection supervisory authorities have in the meantime published guidance and samples in some cases.

According to the guidance of the supervisory authorities, it is possible to differentiate between the immediately required information provided in advance on an information sign and the complete information to be provided on a comprehensive information sign. It is then conceivable, for example, that the advance information sheet should first provide information about the type and method of video surveillance as well as the office responsible in accordance with Section 4(2) of the BDSG. All other information in accordance with the requirements of Article 13 of the GDPR could then be provided on the following information sheet, including, for example, information about the rights of the data subject. The advance information sheet should then be clearly visible to the data subjects and contain a reference to the information sheet to follow so that the data subjects know how to access the complete information. In this respect, reference can be made, for example, to a website (via a URL or the use of QR codes) or to employees who have access to corresponding fact sheets.

The recommendations of the supervisory authorities regarding information on video surveillance show that it can contribute to transparency not to "overload" the data subject directly with a lot of information and possibly overwhelm him or her, but to initially provide only the most important information and to give interested data subjects the opportunity to subsequently obtain more detailed information in a simple, easily accessible manner. Video surveillance can also be made more easily recognizable, for example by displaying a camera symbol on the information sign.

Transparency in obtaining consent

The principle of transparency is also reflected in the requirements for effective consent. Consent under data protection law must be given voluntarily. To ensure that consent is voluntary, the data subject must first be clear about what data processing he or she is to consent to in the first place. Consent under data protection law must therefore be given in an informed manner. The information should enable the data subject to understand the planned data processing and its purposes and, on this basis, to decide whether or not to give consent to the data processing. The information requi-

red for this must therefore be provided to the data subject before consent is given.

Not only the information, but also the request for consent should be made in clear language in an easily understandable and readily accessible form. It is important here that the request is clearly distinguishable from other facts.

For practical implementation, it is advisable to pre-formulate an understandable consent text that can be actively confirmed by the data subject, for example by signing it or by clicking a checkbox on a website. It is important that the data subject can obtain information about the details of the data processing prior to the confirmation action, for example, via an explicit reference to the linked data protection declaration or via additional data protection notices handed out. However, a combination of data protection notices and consent texts should be avoided so that the data subject can recognize when he or she is only informed by the data controller and when a declaration is required or desired from him or her.

Right of access according to Article 15 of the GDPR

One of the central rights of data subjects under the GDPR is the right of access, which is enshrined in Article 15 of the GDPR and also in Article 8(2)(2) of the Charter of Fundamental Rights of the European Union. Accordingly, 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.

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

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 by the controller at all. If personal data about the data subject is processed, the data subject has the right to obtain information about the personal data. In addition, he or she has a right to receive further information about the data processing, which is mentioned in Article 15(1) of the GDPR. This includes, among other things, the processing purposes, the categories of personal data processed, the recipients of the data, the storage period, the origin of the data and the existence of automated decision-making, including profiling. The information to be provided when asserting a right of access thus parallels the information required under Articles 13 and 14 of the GDPR.

Article 15(1)(e) of the GDPR also provides for information about data subjects' rights, namely about the existence of a right to rectification or erasure of personal data, or to restriction of processing,

or a right to object to processing. Information about the rights of the data subject can already be found regularly in the data protection declaration on the homepage of a data controller 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. However, such a provision is not found in Article 15 of the GDPR with regard to the right of access. The information about the data subject rights must therefore be provided again when answering a request for information pursuant to Article 15 of the GDPR.

In practical terms, transparency must also be ensured when providing the information. 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. The requirement of Article 15(3) of the GDPR, according to which the controller must provide the data subject with a copy of the personal data that is the subject of the processing, also serves transparency. Overall, it is advisable to establish and document a coordinated and internally agreed procedure for dealing with such requests in order to respond to such requests for information in a legally compliant manner.

Further details on the right of access under data protection law and in particular on the practical handling of requests for information can be found in our [March 2022 data protection newsletter](#), which is explicitly dedicated to this topic.

Conclusion

The principle of transparency of data processing is one of the essential elements of the GDPR and serves not only the traceability and verifiability of data processing for data subjects, but also the exercise of data subjects' rights.

Information about data processing should be provided to data subjects in a precise, easily accessible and understandable manner and in clear and simple language. The principle of transparency is given particular expression in the information obligations pursuant to Articles 13 and 14 of the GDPR and in the right of data subjects to request information about personal data relating to them.

In order to inform data subjects transparently about the processing of their personal data, it is recommended that data controllers establish coordinated procedures for the provision of information in advance. The preparation of information sheets, the design of data protection declarations and the wording of comprehensible consent texts help to make data processing comprehensible and understandable for the data subjects.

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