Preventing abuse of the right of access under data protection law

Opinion on the Guidelines of the European Data Protection Board on the Right of Access under Article 15 of the GDPR

March 2022

Summary

The right of access according to Art. 15 of the GDPR increasingly poses challenges for employers. Particularly in the case of long-term employment relationships, data can accumulate in hardly manageable quantities. The scope and reach of the right to information and the right to be provided with a copy of the personal data processed are largely unclear. In addition, the right to information is increasingly used in an inappropriate manner in labour court disputes in order to gain a better negotiating position. However, the right to information was not created to strengthen the position of employees in legal disputes that do not concern data protection. The aim of the entitlement is to enable data subjects to obtain transparent and easily accessible information so that they can verify the lawfulness of the processing and the accuracy of the data processed.

For companies, clarification of the scope of the right to information is therefore of central importance in order to ensure legally secure handling in practice and to set limits to unjustified requests. However, the guidelines fall short of these expectations.

The right of access under Art. 15 of the GDPR is interpreted very comprehensively in the guidelines. Exceptions and limitations to the right of access, which are laid out in the GDPR, are only interpreted in a very restrictive manner. This leads to an unjustifiable inappropriate distribution of risks. According to the understanding of the guidelines, the right of access should enable the respective data subjects to check whether the data concerning them are correct and the processing is lawful. The right of access includes information on whether data relating to the data subject is being processed, access to the data and information on the processing, such as the purpose of the data processing, categories of data and the recipient of the data. A request for information does not need to be justified and may only be refused if it is manifestly not related to data protection, manifestly unfounded or excessive in view of the circumstances of the individual case, especially in the case of repeated requests. Random requests or requests sent to obviously incorrect addresses do not have to be processed.

Scope of application - pseudonymised data

According to the guidelines, information should also refer to pseudonymised data. Pseudonymisation means that personal data of a data subject can only be identified with the addition of further information. This ensures compliance with the principle of data minimisation and safeguards the protection of personal data of data subjects. According to the understanding of the GDPR in Art. 32, pseudonymisation is a technical protection measure for risk minimisation. If Article 15 of the GDPR also includes pseudonymised data, this means an unjustifiable effort for the responsible person (employer), as the personal reference to the person requesting information must first be re-established by returning the pseudonymisation. The effort involved

is disproportionate to the potential risk to the data subjects. A restrictive interpretation that pseudonymised data is not covered by the right to information would take into account the interests of employers and employees alike.

Scope – Completeness of information

The processing of the request for information is often organisationally complex as well as time-consuming and therefore involves a high use of resources for the employer.

- In the case of large amounts of stored information that have accumulated over many years of employment, for example, the controller may require that the request for information be specified (Recital 63,s. 7). This is rightly referred to in the Guidelines. This right should not be weakened by obliging the controller to provide "overview information" about the data processing taking place already at this stage (p. 15, Section 35 lit. b)).

- It should be clarified that the obligation to provide information does not apply to internal notes and memos. In view of a long period of employment, it can be assumed that personal data of employees are often contained in handwritten notes and internal memos. If the responsible employer's obligation to provide information also referred to such internal notes, the claim would hardly be manageable in practice and proper provision of information would be almost impossible in practice.

- In addition, the right to information as well as the right to be provided with a copy of the personal data processed should only refer to information that is not already known or available to the person requesting information. This concerns, among other things, e-mail correspondence that the data subject has conducted himself/herself. The provision of the entire e-mail traffic of the data subject does not correspond to the protective purpose of the right to information. This also applies to data that is already accessible to the data subject, e.g. if the data subject as an employee can view his or her employee profile and the corresponding data is stored there. The aim of Art. 15 GDPR is not to obtain a complete copy of all documents in which personal data of the data subject are contained in any way. Such a broad interpretation of the right of access would be disproportionate.

- The EDPB's view that access must include the disclosure of specific deletion periods also leads to an inappropriate balance of interests (Section 116). According to this, the information would include the complete presentation and explanation of a company's document retention policy. This represents a disproportionate effort for responsible parties.

- Finally, the EDPB's guidance provides that even if the retention period is short, the controller shall take appropriate measures to make this data available in the event of a request for information from the data subject. This requirement contradicts the principle of purpose limitation (Art. 5 GDPR). For example, video recordings that originate from video surveillance of the workplace or company premises must be deleted by the employer after a short period of time, in Germany after 48 hours. The retention of already deleted data (possibly by third parties) is not compatible with the meaning of deletion requirements under data protection law, because it is then not or cannot be deleted.

Limits to the right of access

The Guidelines only provide exceptions to the provision of information within very narrow limits. Accordingly, these exceptions include quantitative aspects of an abuse of rights ("excessive requests", Art. 12 (5) sentence 2 GDPR), conflicting rights of third parties (Art. 15 (4) GDPR) or legislative restrictions of the Member States (Art. 23 GDPR).

- However, according to the wording of Article 12 (5) sentence 2 GDPR, the exceptions are not limited to quantitative aspects. Precisely because of the addition of "in particular", other similar aspects can also lead to a restriction under this exception provision, especially with regard to the processing effort of qualitative issues. Within this framework, it should be possible in the future to restrict blanket requests for information by employees after a qualitative consideration of the right to information of the employee concerned.

- Limits to the request for information should be clarified, especially in the event of a court dispute. In labour court disputes, the right to information is often used in practice for purposes other than those intended. The intention of the legislator was not to provide employees with information and means of presentation and evidence by means of a request for information, which the employee would then use to the employer's disadvantage in a legal dispute with the employer. In the context of the right to information, the employer's civil procedural rights must also be taken into account and brought into an appropriate balance with the interests of the employee. This should already be clarified at European level. In order to counteract an abusive procedural assertion of the claim for information, a statement by the EDSA on the limitation of the amount in dispute of the non-pecuniary claim for information would make sense. A limit of e.g. € 500.00 would be appropriate.

Process of providing information

- The Guidelines provide the provision of information in two steps ("layered approach"), e.g. when large amounts of data are provided. In the first step, the data subject should be given an overview of the processing and his or her rights under Art. 15 Abs. 1 lit. a-h and Art. 15 Abs. 2 GDPR. In the second step, the controller shall provide the data subject with a copy of the personal data that were the subject of the processing (Art. 15 Abs. 3 GDPR). However, this step-by-step provision of information raises practical issues that are not considered in the Guidelines. Accordingly, if the controller takes two steps to provide information, the time limit must run separately for each of the two steps. This also follows from the wording of Art. 12 Abs. 3 GDPR, which requires a separate time limit for each individual request for information. The possibility of providing information step by step must be practicable, which is only possible with an adjusted time window. It is not acceptable that the scope of information is extended in favour of the data subject while the rights of the controller are restricted without exception.

- It should be clarified that the provision of information can also be fulfilled by the possibility of inspecting the documents at the controller's premises.

Ansprechpartner:
BDA | DIE ARBEITGEBER
Bundesvereinigung der Deutschen Arbeitgeberverbände

Arbeitsrecht und Tarifpolitik
T +49 30 2033-1200
arbeitsrecht@arbeitgeber.de