Art. 15 GDPR (EU General Data Protection Regulation) stipulates in detail which rights of information a data subject can assert against a controller. But how can this be implemented in practice? How far does the right to

information according to the GDPR go? The following article shows what those obliged to provide information should consider in order to fulfil their obligations towards those entitled to receive information.

Data is everywhere, and the computer is the network

It is actually a truism: information systems are not only complex, they are also interconnected, and they store an increasing amount of personal data from an increasing number of sources and they are more and more able to meaningfully link data. The possibilities to connect systems and existing data no longer come to an end at the wall of the data centre wall. With respect to cloud services (please also see Peter's contribution on Cloud computing), the former SUN advertising slogan "the computer is the network" rings truer than ever, though it is unlikely this was foreseen at the time. Whether data is processed online, i.e. "in the network", or offline, i.e. on local devices, is now primarily determined following economic considerations. It is hardly surprising that this makes it extremely difficult to understand how personal data is stored and processed, even in small companies.

The right to information: the foundation of data protection

Data protection laws have long attempted to counteract this lack of comprehensibility by establishing a legal right to information. An affected person, aptly referred to in the English version of the GDPR as a "data subject", must be able to find out who has stored what data about him or her, and when and at what occasion or from what source the data was collected. The right to information as stipulated in Art. 15 GDPR is therefore also a manifestation of the principle of transparency underlying the entire GDPR, Art. 5 GDPR. In addition, the obligation laid down in Art. 30 GDPR that a controller must prepare and maintain descriptions of its processing activities, and must collect them in a register, forces controllers to document their own processing procedures. Companies must therefore know exactly where what data can be found. Though it is often perceived to be a bureaucratic burden, one goal of the duty to keep a register of processing activities of the documentation is therefore to, first of all, put the person responsible in a position to provide information.

The plain reality: diversity

When preparing the processing descriptions and no later than when it comes to implementing the data deletion concept as required by the GDPR, many companies realise that they actually do not know exactly what data they have stored about a data subject, and for what reasons. It becomes even more difficult when they have to understand what data is stored in what systems. In practice, central master data systems, which directly or indirectly supply all other systems of a company with master data on the basis of a precise data flow plan, are the exception rather than the rule. Much more common is a zoo of various historically grown applications that barely communicate with each other or, where they do, only do so with the help of often complex middleware. Many of these systems therefore operate on the basis of partially redundant data stock. This means that what is already a considerable operational risk today can, due to the GDPR, now also become a stumbling block with fines attached to it.

The risk of the right to information

Once the GDPR became applicable, many companies received requests from persons who wanted to receive information about the data actually or even often only supposedly stored about them. Depending on the template letter used, they often made quite far-reaching demands. In contrast thereto, many applications still lack until today the technical support to provide such information. Data subjects usually only receive manually generated, static database extracts and no meaningful information about past data collections, data transfers to third parties and on data flows. Therefore the question of how far the right to information really goes is of particular importance.

The legal situation as it used to be: right to information according to Section 34 German Federal Data Protection Act (BDSG)

The right to information is by no means an invention of the authors of the GDPR. It was already stipulated in Section 34 of the German Federal Data Protection Act (*Bundesdatenschutzgestz*, BDSG-old), and those searching for itcould find numerous templates with requests for information, e.g. provided by data protection authorities or consumer protection associations. Section 34 BDSG-old stipulated that information could be requested about

- all data stored about the person entitled to receive the information;
- the origin of the data, i.e. where and when it was collected, or from whom the data originated;
- the respective purpose of the storage of the data; and,
- if the data was transmitted to third parties, all recipients or categories of recipients to whom the stored data was transmitted;
- with respect to scoring (Section 28b BDSG-old), there was also a detailed right to an explanation of individual aspects of the scoring procedure, including the recipients of the scores.

So, what is new in Art. 15 GDPR?

Not a whole lot. If you look at this list and compare it with Art. 15 GDPR, you will see considerable parallels:

- there is a right to information about all data that was stored about the person entitled to receive the information; about
- the processing purposes, categories of data, recipients of data including contract processors; about
- the storage time or deletion criteria; about
- the origin of the data, i.e. where and when it was collected, or from whom the data originated;
- information about automated decisions; and
- about possible transfers to third countries.

If you compare Art. 15 GDPR with Section 34 BDSG-old, it quickly becomes apparent that there are considerable parallels, and some older rules, such as the very detailed Section 34 para. 2 BDSG-old on scoring, now regulated in much less detail in the GDPR. The previously applicable principle that information had to be provided “without undue delay”, which practically meant that a period of two weeks was generally permissible and significantly longer response times were only permissible with good reason, appears to have become more favourable for companies as a result of the deadlines provided in Art. 12 para. 3 GDPR.

It should be noted, however, that the previously relatively low threat of a fine of up to EUR 50,000 (Section 43 para. 1 no. 8a – 8c in conjunction with Section 43 para. 3 BDSG-old) has been replaced by the at least theoretically possible draconian penalties stipulated in Art. 83 GDPR. However, it remains to be seen whether they will actually be imposed in the event of missing or incorrect information. The main problem could be that a lot of information provided to date subjects could not be complete. Consumer protection associations are likely to pay particular attention to publications such as this one from the German Customer Advocacy Group “Stiftung Warentest” (German).

https://youtu.be/7XwHmOkNUhw

Relentless: enforcement of rights to information in the United Kingdom

The “right to data transferability” under Art. 20 GDPR, on the other hand, can be described as a new feature of the GDPR – if you wish to understand this as constituting a special, far-reaching form of the right to information.

This right is indeed a significant extension of the obligations of the persons responsible.

Content and form of providing information

Art. 15 GDPR only contains a brief description of the form in which the information is to be provided: According to paragraph 3, "a copy of the personal data undergoing processing" must be provided. Electronic enquiries must be answered electronically, unless requested otherwise. An appropriate fee may be charged for the provision of additional copies to cover any administrative costs. Some of our clients have asked themselves whether they really have to provide "copies", i.e. duplicates of the data records. This would negatively impact the readability and it can be very time and cost intensive, especially with complex databases.

In order to answer this question, a judgment of the Court of Justice of the European Union (CJEU) from 2014, i.e. even before the adoption of the GDPR but during the time when consultations relating to it were already taking place, can provide valuable information. In the reasons of the decisions (CJEU, judgment dated 17/07/2014, cases no. C-141/12 and C-372-12), the CJEU commented, among other things, on the scope of the right to information.

In the cases under consideration it was disputed whether the right to information – at that time still contained in the EU Data Protection Directive and the corresponding national transpositions – also gave rise to a right to receive a copy of the entire original document containing the data or whether it was sufficient to provide the information in the form of an overview of the stored data.

The CJEU ruled that the data subject is not entitled to receive a copy of the entire document (see paragraph 57f. of the CJEU decision). The right to information provides the data subject with the right to receive from the person responsible for the processing an intelligible communication about the data that is subject to the processing as well as information available on the origin of the data, unobstructed and without constraint, at reasonable intervals and without undue delay or excessive cost. The information must be complete, but as long as the communication is "intelligible", the EU Data Protection Directive does not specify the concrete form in which the communication has to be made. "Intelligible" means that the information "enables the data subject to obtain knowledge of this data and to verify that it is accurate and processed in accordance with the Directive". The data subject is to be put in a position to check whether he or she can exercise further rights to which he or she is entitled.

This purpose is also fulfilled if the information is provided in a form other than by a copy of the original data or documents. In order to ensure that the data subject does not have access to information other than the personal data concerning himself or herself, such other information contained in the relevant document could be made illegible (see paragraph 59 of the CJEU decision).

Application to the GDPR

The GDPR does not contain a more specific definition of the form in which the information has to be provided. In contrast to the EU Data Protection Directive, however, there are only very limited possibilities for national legislators to implement more specific rules. It therefore makes sense to apply the basic idea of the CJEU decision to Art. 15 para. 3 GDPR: the right to information does not extend to such an extent that the data subject has to be provided with parts of databases which may also contain data from other data subjects. It is sufficient to provide the data in a complete (!) and at the same time, legible and intelligible form. In fact, the idea of "intelligibility" as put forward by the CJEU can also be found in Art. 12 para. 1 GDPR. According to this, information must be transmitted in a "concise, transparent, intelligible and easily accessible form, using clear and plain language". A mere database dump as a PDF, as Max Schrems once received from Facebook, would

therefore not meet these requirements.

Summary

The right to information pursuant to Art. 15 GDPR introduces only a few really new requirements. Those who were already in control of their information processes as part of their obligations under BDSG-old will only have had to make a few changes when the GDPR became applicable. In this context the shorter and more compact rules of the GDPR can be understood as a requirement to provide data subjects with the relevant information in a prepared and legible form. The controller does not have to adhere to any demands going beyond this.

For the practical implementation of the processes to provide information, controllers should take a holistic approach: the requirement of having to have a deletion concept and a process description force them anyway to become “able to provide information”. Herein lies great potential for controllers to create a process to implement the only apparently tormenting, quasi-tortuous demands of the legislator, giving the whole approach a melody as well as a structure.

Torquemada dances the Spanish Inquisition. Source: History of the World, Part 1 (1981)

Titelbild / Cover picture: Copyright © fotolia