Management of data subject rights

How to answer requests for data access and co. properly.

A white paper by Stefan Hessel, LL.M. and Christina Kiefer, LL.M.

Status 05/2023

Data subject rights as part of data protection compliance

The General Data Protection Regulation (GDPR) grants data subjects numerous rights to protect their data. As the flip side of the coin, the rights of data subjects result in corresponding obligations for those responsible for data processing - the controllers. Due to the multitude and complexity of the data subject rights, it is essential to develop internal company processes in order to properly comply with these obligations. In particular, data subjects have the following rights:

- Right to information
- Right of access
- Right to rectification
- Right to erasure and restriction of processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making

Right of access

The core of the data subject rights is the right of access under Art. 15 of the GDPR. Under this provision, every data subject in principle has the right to obtain from the controller confirmation as to whether and which personal data concerning him or her are being processed. The provision of information often only enables the assertion of further data subject rights. In order to avoid sanctions, numerous points must be observed when processing requests for access and information from data subjects. In the past, individual data subjects have been awarded damages not only for failure to provide confirmation and/or access and information, but also for incomplete[1] or late provision.[2]

It is becoming increasingly apparent that the assertion of the right of access under Art. 15 of the GDPR will become an essential part of labour law disputes.[3] It is therefore in the interest of every employer to keep a record of processing activities and to carefully document the processed employee data in order to be prepared for

[1] LAG (Higher Labour Court) Berlin-Brandenburg, judgment of 18/11/2021 – 10 Sa 443/21, available at: https://openjur.de/u/2389586.html, last retrieved: 10/05/2023.

[2] ArbG (Labour Court) Düsseldorf, judgment of 05/03/2020 – 9 Ca 6557/18, available at: https://openjur.de/u/2202048.html, last retrieved: 10/05/2023.

[3] News report: Hessian Higher Labour Court comments on the right to information in data protection law in accordance with Art. 15 GDPR, available at: https://www.reuschlaw.de/en/news/hessian-higher-labour-court-comments-on-the-right-to-information-in-data-protection-law-in-accordance-with-article-15-gdpr/, last retrieved: 10/05/2023.

possible claims for access and information. This applies even if only a small amount of customer or employee data is processed.

Ideally, internal processes and policies should be established to ensure that requests for confirmation, access and information are properly responded to – at best, before the first request reaches the company, as the response must be made within one month and the deadline may only be extended to two months in exceptional cases. Depending on the technical system used, it may be necessary to first enable the export of personal data. If such problems are not addressed until the first request is made, there is a risk that the answer will not be provided within the deadline. A late response may already result in fines or claims for damages.

Limitations of the right of access

The right of access under Art. 15 GDPR is not without limitations. When designing processes and internal policies, it is therefore important to consider in which cases access can be refused. A refusal to grant access can be justified, for example, in the case of excessive and obviously unjustified requests. It also follows from the recitals of the GDPR that the controller can demand specification if the data subject requests information about a large amount of data. In labour court proceedings, the assertion of the right of access for the inappropriate purpose of merely preparing a labour law claim and reaching a supposedly related reversal of the burden of presentation and proof was also rejected.[4]

It remains to be seen whether these efforts will be sustained in the long term. The legal definition of the contours of the right of access has not yet been completed. The evaluations by courts and supervisory authorities are still in flux. At present, however, there is a tendency towards a broad interpretation of the right of access. Currently, the European Court of Justice (ECJ) has ruled on the right of access that data subjects - when asserting the right to a copy under Art. 15 (3) of the GDPR - must be given a faithful and intelligible reproduction of all personal data.[5] In the light of this decision, it is to be expected that data subjects will increasingly make use of their right of access in the future. It is therefore advisable to observe further developments in order to be able to make any necessary adjustments to internal processes in good time.

Further practical difficulties arise in connection with the identification of the data subject. On the one hand, the exercise of data subject rights must not be rendered overly difficult by excessive requirements for proof of identity. National supervisory authorities have already imposed fines where the grant of access was made dependent on an overly burdensome proof of identity of the data subject.[6] On the other hand, legal consequences are threatened if personal data are unlawfully passed on to unauthorised persons. In the past, for example, a mobile phone provider had to pay a fine of € 900,000 for disclosing a customer's mobile phone

[4] LAG (Higher Labour Court) Saxony, judgment of 17/02/2021 – 2 Sa 63/20, available at: https://rewis.io/service/pdf/urteile/jgn-17-02-2021-2-sa-6320.pdf, last retrieved: 10/05/2023.

[5] ECJ, judgment of 04/05/2023 – C-487/21, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CJ0487, last retrieved: 10/05/2023.

[6] Decision of the Spanish data protection supervisory authority AEPD, fine notice available at: https://www.aepd.es/es/documento/ps-00003-2021.pdf, last retrieved: 10/05/2023.

number without authorisation.[7] It is quite a challenge to find a legally compliant balance between the protection of data subject information and the simple granting of data subject rights.

Right to information

Irrespective of any existing data subject request, the controller has the obligation to sufficiently inform the data subject about the processing of his or her personal data. According to Art. 13 of the GDPR, this obligation arises where data are collected from the data subject himself or herself. In practice, this obligation is mostly fulfilled by using a privacy statement. However, also if the data are collected from third parties, the controller is obliged to inform the data subject according to Art. 14 of the GDPR. This requires nothing less than that the controller approaches the data subject on its own initiative. This applies even if there has been no direct contact between the controller and the data subject before or only data that are already publicly available are processed. However, the controller is not obliged to collect further data about the data subject solely for the purpose of implementing the GDPR. In order to avoid sanctions, internal processes must ensure that data subjects are informed in a timely and comprehensive manner about the processing of their data.

Right to rectification

The right to rectification gives the data subject the right to obtain from the controller the rectification without undue delay of inaccurate personal data. In addition, he or she has the right to request the completion of incomplete personal data. These rights are based on the general principle of data accuracy according to Art. 5 (1) (d) of the GDPR. Since the stored data often form the basis of a decision vis-à-vis the data subject, the data subject has an interest in their completeness and accuracy. Since the correction must be made without undue delay if a request is made and the data subject must be informed of the action taken in response to the request within one month at the latest, internal procedures for processing such requests are indispensable.

Right to erasure

According to Art. 17 of the GDPR, data subjects can request the erasure of their personal data under certain conditions. This right, also known as the "right to be forgotten", is intended to ensure that individuals themselves can make sure that their personal data are definitely only processed for as long as there is a legal basis for doing so.

As in the case of the right to rectification, the request for erasure must be complied with without undue delay if the conditions are fulfilled and the data subject must be informed of the measures taken after one month at the latest, so that here, too, arrangements must be made for prompt routine handling of such requests.

Right to data portability

In addition, there is the right to data portability according to Art. 20 of the GDPR. This ensures that the data subjects can receive their personal data in a structured, commonly used and machine-readable format. In addition, the data subject has the right to transmit these data or have them transmitted to another controller without hindrance. On the one

[7] LG (Regional Court) Bonn, judgment of 11/11/2020 – 29 OWi 1/20, available at: https://www.justiz.nrw.de/nrwe/lgs/bonn/lg_bonn/j2020/29_OWi_1_20_Urteil_20201111.html, last retrieved: 10/05/2023.

hand, this allows the data subjects to control their own data and, on the other hand, makes it easier to change providers.[8]

Currently, there is still uncertainty about the scope of application of the regulation. The applicability to social media accounts, playlists, but also cloud storage, purchase histories or the transfer of address lists from one email provider to another is being discussed.[9] It is therefore advisable to carefully examine whether a company processes data that must be made available to the data subjects in the form provided for by Art. 20 of the GDPR. These considerations should also include the "Data Act" planned by the EU Commission, which is intended to extend the rights of access to be granted by companies to non-personal data in the future.[10]

Right to object

The data subject may also have the right to object to lawful processing. According to Art. 21 of the GDPR, this right exists, for example, in the case of processing of personal data for the performance of a task in the public interest or for the protection of the controller's legitimate interests. In this case, the controller must check whether there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject. Otherwise, no further processing may take place. If personal data are processed for direct marketing purposes, the processing must be discontinued immediately if the data subject objects.

Right not to be subject to automated decision-making

An unusual provision in the context of the GDPR is Art. 22 of the GDPR, which grants the individual a right not to be subject to a certain procedure. This protects the data subjects against fully automated decisions being made against them. The provision does not regulate the data processing itself, but the subsequent decision based on the information obtained from the processing.[11] This right aims to ensure that no individual is subjected to fully automated decision-making that produces legal effects vis-à-vis him or her or otherwise significantly affects him or her. An example is the automatic rejection of an online credit application or an online recruitment procedure without human intervention. At the same time, the legislator has provided for exceptions. In the case of fully automated decision-making, it should be examined whether monitoring of the decision-making process by natural persons is necessary in order to avoid sanctions. With a view to the "Artificial Intelligence (AI) Act" (AI Act) currently planned by the EU Commission, companies must prepare themselves for far-reaching legal tightening when using AI anyway and implement appropriate measures at an early stage.[12]

---

[8] *Paal*, in: Paal/Pauly, DS-GVO BDSG, Art. 20 GDPR, para. 4.
[9] *Munz*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 20 GDPR, para. 2.
[10] EU Commission, Proposal for a Regulation of 23/02/2022, COM(2022) 68 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068, last retrieved: 10/05/2023.
[11] *Martini*, in: Paal/Pauly, DS-GVO BDSG, Art. 22 GDPR, para. 1.
[12] EU Commission, Proposal for a Regulation of 21/04/2021, COM(2021) 206 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206, last retrieved: 10/05/2023.

Creating structures for compliance

In order to properly fulfil the rights of data subjects, companies must be well prepared. This is especially true for the right of access, which has played the biggest role in practice to date. But compliance processes should also be in place for the other data subject rights in order to be prepared for any eventuality.

First of all, this includes making an inventory of the existing processes, the responsibilities as well as the IT systems and the processed data.

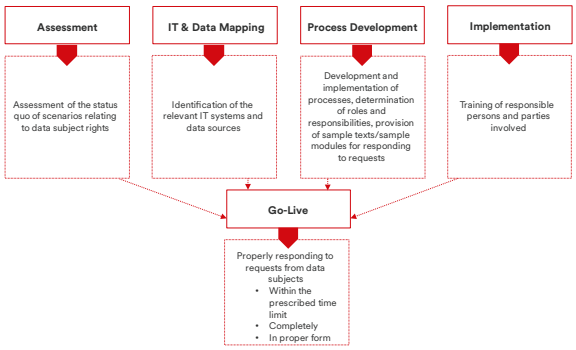

Figure 1: Management of data subject rights
© reuschlaw, 2023

In a second step, it should be analysed which specific requirements exist, to what extent data subject rights are to be granted and how requests are answered appropriately.

In order to avoid claims for damages and fines, processes should be implemented that ensure the timely and complete granting of data subject rights. Roles and responsibilities should be defined and employees should be sensitised, e.g. through training. The processes must be efficient, as the GDPR generally sets tight time limits for the granting of data subject rights and sanctions are already threatened in the event of late fulfilment of data subject rights.

In addition, the safeguarding of data subject rights should be tested in a trial run to ensure that the defined processes run smoothly in everyday life. In order to avoid liability traps, companies should therefore take preventive action and create the necessary structures.

What to expect in the case of breaches?

Even a late response to a request constitutes a breach of the GDPR and is subject to a fine. The same applies in the case of an incomplete or incorrect response. The fines of the data protection supervisory authorities are explicitly intended to have a deterrent effect and can quickly reach five- to six-digit amounts in the case of breaches of data subject rights.

In addition, even minor breaches may result in claims for damages by data subjects, which are increasingly also being asserted by NGOs and Legal Tech companies. So far, courts have generally awarded amounts in the low to mid four-digit range in damages proceedings. In a recent ruling, however, the ECJ decided that there is no threshold of seriousness for non-material damages claims in the case of breaches of the GDPR.[13] Due to such alleviated requirements for awarding damages, an increase in claims for damages is to be expected in the future. In this context, companies are facing the risk of a proliferation of judicial awards in the case of breaches of the GDPR.

However, even if the amount of a claim for damages may be manageable in individual cases: There is always the risk that

[13] ECJ, judgment of 04/05/2023 – C-300/21, available at: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-300/21, last retrieved: 10/05/2023.

incorrect handling of data subject rights will lead to a large number of complaints and companies will subsequently be confronted with a large number of claims for damages.

Comprehensive support

Data subject rights management is an indispensable part of a company's data protection compliance. Even if companies only process a small amount of customer data, numerous labour law disputes show that even the processing of employee data presents quite enough challenges for controllers.

We therefore offer comprehensive and exhaustive data protection advice on the design and implementation of effective processes to ensure compliance with data subject rights.

Next step: Get in touch

Take the first step now on the way to ensuring compliance with data subject rights as part of your data protection compliance and arrange an individual consultation with us. We would be pleased to explain the details of our approach to you in a personal meeting, answer your questions and prepare a suitable proposal for your company. Contact us now without obligation!

T + 49 681 / 859 160 0

E info@reuschlaw.de