Comment

of the German Insurance Association (GDV)
ID-number 6437280268-55

on the
EDPB draft guidelines 01/2022 on data subject rights –
Right of access

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

Rue du Champs de Mars 23
B - 1050 Brussels
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Contact:
data protection/basic issues

E-Mail: **data-protection@gdv.de**

www.gdv.de

Executive summary

The German insurance industry welcomes the draft guidelines on the right to access. The EDPB manages to clarify a lot of open questions left by the open wording in Art. 15 GDPR and reduce legal certainty. However, certain deliberations should be amended in order to enable solutions which guarantee a fair and proportionate balance between the data subjects rights and legitimate interests of controllers. These concern the following topics:

1. teleological reduction of Art. 15 GDPR
2. exemptions to the right to access by virtue of national procedural law
3. Manifestly unfounded or excessive requests
4. The interplay between the right to access and the obligation to erase data
5. Possibility to refer the data subject to past access requests
6. Further copies in the sense of Art. 15 (3) GDPR
7. Modalities of the request for further specification of information
8. Information on the processing and on data subject rights according to Art. 15 (1) (a) to (h) and 15 (2) GDPR

Introduction

Of all the obligations required by the GDPR, the fulfilment of right to access in Art. 15 GDPR is among the most difficult for the insurance sector. Due to the nature of insurance business, our member companies regularly receive many requests for access, which pose major operational challenges to them. The personal data of customers necessary for the performance of insurance contracts often amounts to a three-digit or four-digit number of pages of paper, the perusal of which - and if necessary redaction of certain information – requires massive effort. In many cases, the information given is afterwards used against the insurance company for completely different purposes. There is likely no business sector with a comparable amount of long-term contracts involving regular written correspondence between data subject and controller. The German Insurance Association is therefore grateful for the opportunity to give feedback on the draft guidelines on the right to access. We recognize that the EDPB acknowledges the difficult position insurance companies are in by referring to them in the guidelines and would like to give additional input.

1. Teleological reduction of Art. 15 GDPR

According to the EDPB, the goals the data subject pursues when making use of their right of access shall not matter when assessing the validity of their request (page 9 para. 13).

Both the legislator (rct. 63) and the ECJ emphasize that the purpose of the right to access is to allow the data subject to be aware of and verify the lawfulness of the processing and, if necessary, to be able to exercise the data subjects' rights. While Art. 15 GDPR does not require the data subject to provide the controller with the reasons for their request, if it becomes apparent that exclusively goals foreign to data protection are being pursued, the right to access must be considered inapplicable at the factual level. Such requests cannot merely be considered excessive pursuant to Article 12 (5) GDPR. They already do not correspond to the requirements and limits of Art. 15 GDPR established by the legislator and the ECJ. Even if it remains difficult for controllers to prove that the data subject intends to exploit the right to access for goals not even remotely related to the protection of their personal data, the EDPB should not rule out that option as it would unduly encroach on controller’s rights.

2. Exemptions from the right to access by virtue of national procedural law

The EDPB states in footnote 7 on page 9 that access may be denied on the grounds or the suspicion that the data requested could be intended by

the data subject for use in legal claims if applicable national procedural rules adopted **in accordance with Art. 23 GDPR** determine boundaries of the information to be provided to or exchanged between the parties.

In our opinion, the possibility to rely on an exemption to the right to access based on national procedural law cannot be made conditional on the question whether that law is adopted in accordance with Art. 23 GDPR. Such national procedural rules often greatly predate the GDPR and are as such not based on the latter. As procedural law remains in the competence of the member states, the GDPR cannot retroactively determine additional prerequisites.

3. Manifestly unfounded and Excessive requests pursuant to Art. 12 (5) GDPR

The guidelines state that Art. 12 (5) GDPR should be interpreted narrowly (page 53 para. 173). A request should not be regarded as excessive on the ground that the data subject intends to use the data to file further claims against the controller (page 56 para. 187). In contrast, a request may be found excessive if:

- the individual makes the request, but at the same time offers to withdraw it in return for some form of benefit from the controller or
- the request is malicious in intent and is being used to harass a controller or its employees with no other purposes than to cause disruption, for example based on the fact that:
    - the individual has explicitly stated that it intends to cause disruption and nothing else or
    - the individual systematically sends different requests to a controller as part of a campaign with the intention and the effect to cause disruption.

The statement that a request should not be regarded as excessive if the data subject intends to use the data to file further claims against the controller is problematic, unless the further claims solely concern compliance with data protection regulation. It would otherwise disregard and contradict national procedural law. It also does not differ much in comparison to both examples the EDPB considers possibly excessive. In all these cases, the data subject pursues goals fully unrelated to its rights to data protection. The only difference being that in those two examples described by the EDPB in detail, there is not only just strong evidence of the data subject pursuing goals foreign to data protection, but the data subject itself outright declares that to be the case. However, whether a request for access is excessive cannot be made dependent on the question whether the data subject expressly makes its abusive intentions known. We therefore recommend amending para. 186-188 to state that a request for access can

be considered excessive if it is from the perspective of an objective third party apparent that the data subject only pursues goals unrelated to data protection.

We further argue that such requests are also manifestly unfounded since they do not correspond with what the legislator intended when introducing the right to access (compare with explanations under point 2).

4. The interplay between the right to access and the obligation to erase data

If the retention period for certain data ends before the timeframe to answer the request for access in Art. 12 (3) GDPR, access to that data shall be given prior to the end of the retention period (page 17 para. 38-39).

In practice, this will often not be possible when processing massive amounts of personal data, as is nearly always the case with data necessary to perform insurance contracts. In order to be able to properly fulfil the obligation to erase personal data after the end of retention periods, machine-based deletion routines need to be implemented which automatically delete the respective data (often hundreds of thousands of information on contracts and insurance cases) in one go. These routines have to be programmed several years in advance to ensure a timely erasure and they are executed automatically. Thus, they cannot be interrupted just because of a request for access. We would therefore argue that the right to access should be considered complied with if the information being given to the data subject accurately reflects the personal data processed at the time the controller grants the access (assuming the access is given at any point within the deadline established in Art. 12 (3) GDPR).

On another note, we would like to provide additional input, which could be helpful to controllers in cases where the amount of data processed does not quite reach the quantities outlined in the paragraph above: According to Art. 17 (3) (b) GDPR, the obligation to erase personal data does not apply to the extent that the processing is necessary for compliance with a legal obligation which requires processing by Union law for which the controller is subject. In our view, the obligation to fulfil Art. 15 GDPR is such a legal obligation pursuant to Art. 17 (3) (b) GDPR. Therefore, the guidelines should be amended to include the option to extend the deadline for the deletion of the data until the right to access has been fully complied with. Otherwise, in cases wherein the request for access only arrives shortly before the end of a retention period, controllers would have to resort to initially provide only access to the personal data which will soon have to be deleted and to only afterwards provide access to the rest of the information. Splitting up the information in such a way would make it more dif-

ficult for the data subject to gain an overview of all the data processing by the controller.

5. Possibility to refer the data subject to past access requests

The guidelines determine that a controller who has already complied with a data subject's request for access in the past cannot refer the data subject to that past information for future requests. The controller should not inform the data subject only of the mere changes in the personal data processed or the processing itself since the last request, unless the data subject expressly agrees to doing so (page 35 para. 109).

Controllers should be allowed to refer to recently provided access in cases in which new requests for access follow shortly after a request has just been complied with and wherein no significant changes to personal data processed or the data processing occurred. In these cases, it should be sufficient to only provide information on the changes since the last request if there were any.

6. Further copies in the sense of Art. 15 (3) GDPR

On page 13 para. 28, it is stated that whether a request concerns a new first copy or an additional copy is solely dependent on the content of the request. In contrast, neither the fact that the data subject placed a new request within a short interval nor the fact that no new data processing has happened shall be of relevance.

Solely focusing on the content of the request does not appear appropriate. Especially in cases in which there are only very short intervals between multiple requests for copies and where it is - with respect to the specific circumstances of the individual case - apparent that there have been no changes to the data processing, focus should also be on the question if the content of the copy itself is identical. In these cases, the controller should be allowed to refer to the copy/copies already provided or to charge a reasonable fee.

7. Modalities of the request for further specification of information

According to the guidelines, controllers who process large quantities of information relating to the data subject may request the data subject to specify the information or processing to which the request for access relates (pages 15 f. para. 35 (b)). This possibility is linked to certain requirements. Among others, the controller may await the answer of the

data subject before providing additional data according to the data subject's wish, if the controller has provided the data subject with a clear overview of all processing operations that concern the data subject.

Under certain circumstances, the controller may not be able to give more than a general overview of processing operations that may concern the data subject before requesting specification. For example, personal data of a customer may have been stored with regard to a lawsuit in which the customer was only serving as a witness. In these cases, the information on the customer's involvement in the lawsuit will often not be linked to the general customer file. Without prior specification by the customer, it may be difficult for the controller to provide a clear overview of all processing operations that concern the data subject. The controller should rather be allowed to inform the data subject in a general way that there may be personal data stored elsewhere and ask for specification if the data subject wishes access to that data.

8. Information on the processing and on data subject rights according to Art. 15 (1) (a) to (h) and 15 (2) GDPR

The EDPB states on pages 35-39 para. 110-120 that the information required by Art. 15 (1) (a) to (h) and (2) need to be tailored to the data subject making the request for access. General information would not be sufficient.

While we understand the EDPB's line of thought, we also need to point out the massive efforts required for companies, which will often be disproportionate. We would rather propose that controllers can in a first step provide access to the information required by Art. 15 (1) (a) – (h) and (2) in a general manner similarly to a privacy notice and ask the data subject for specification if it wishes to receive more tailored information on one or all of these topics. Unless the data subject explicitly requests such tailored information after being asked for specification, information in a non-tailored manner should suffice to fulfil the controller's obligation.

Berlin, 11.03.2022