Response to EDPB consultation on draft guidelines on data subject rights of access

Our reference:	COB-DAT-22-09	Date:	16 March 2022
Referring to:	Guidelines 01/2022 on data subject rights - Right of access		
Contact person:	Danilo Gattullo Policy advisor, Conduct of business	E-mail:	gattullo@insuranceeurope.eu
Pages:	6	Transparency Register ID no.:	33213703459-54

Insurance Europe welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft guidelines on the right of access under the General Data Protection Regulation (GDPR). Insurance Europe welcomes the draft guidelines as they provide clarity on how to handle practical cases of data access requests and the obligations that must be adhered to.

Insurance Europe is, however, concerned that, in certain cases, the guidelines' interpretation of the right of access would result in a more burdensome handling of data access requests without any clear benefits for the data subjects.

For example, responding to a broad access request by providing all the personal data and processing activities around an individual in one go would risk overloading the data subject with information that is less usable or understandable. Controllers should therefore be able to reliably respond to these requests as needed by providing information in different layers and to facilitate the data subject's understanding of the data.

Insurance Europe therefore invites the EDPB to provide the necessary clarifications on the issues described below.

Aim of the right of access and general principles

- Teleological reduction of Article 15 GDPR (paragraph 13)

  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 (paragraph 13).

  Both the legislator (Recital 63) and the ECJ emphasise 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 Article 15 GDPR does not require the data subject to provide the controller with the reasons for their request, if it becomes apparent that only 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 Article 15 GDPR established by the legislator and the ECJ.

Insurance Europe aisbl • rue Champ de Mars,23 B-1050 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

Recommendation: Even if it remains difficult for controllers to prove that the data subject intends to exploit the right to access for goals not 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.

- Further copies in the sense of Article 15 (3) GDPR (paragraph 28)

In paragraph 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.

Recommendation: 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.

- Modalities of the request for further specification of information (paragraph 35)

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. paragraph 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.

Recommendation: The controller should 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.

- The interplay between the right to access and the obligation to erase data (paragraphs 38-39)

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

Recommendation: 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 pieces of information on contracts and insurance cases) in one go. These routines must 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. Insurers 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 Article 12 (3) GDPR).

On another note, according to Article 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 the industry's view, the obligation to fulfil Article 15 GDPR is such a legal obligation pursuant to Article 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 a great amount of information has to be provided and 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 difficult for the data subject to gain an overview of all the data processing by the controller.

Scope of the right of access

- Definition of personal data (paragraph 95)

The example provided in paragraph 95 (a job interview) shows that the comments and assessments made by the HR officer during the interview must be considered as personal data.

If this concept were to be applied also to the assessments made by a surveyor through internal memos, considerations made in case of alleged fraud and more in general, all the internal documentation containing evaluations/remarks/comments on situations related to the data subjects should be communicated to the data subjects themselves. This would entail unjustified disclosure of such activities which are strictly related to the undertaking's common operation and should remain as such.

Therefore, the industry does not share the EDPB's interpretation on the matter, also considering that, following a joint reading of Article 4(1)1 e Article 5(1)(d) GDPR, subjective evaluations — being opinions of the controller expressed for the controller's internal purposes — cannot be considered as personal data by definition, particularly because they do not meet the fundamental requirement of data accuracy, being subjective by nature, discretional, partial or even incorrect, as all personal evaluations.

This is also proven by the objective and irrefutable circumstance by which subjective evaluations should never undergo erasure or rectification by the controller upon request of the data subject, rightly because they do not respond to the fundamental requirement of data accuracy.

Recommendation: The EDPB should clarify that internal documentation related to personal evaluations are not to be considered personal data as they do not meet the fundamental requirement of data accuracy.

- Personal data which "are being processed" (paragraph 108)

The guidelines state that "In case there is an access request at the moment where there are more personal data relating to the data subject in the backup than in the live system or different personal data […] the controller needs to […] where technically feasible provide access as requested by the data subject, including to personal data stored in the back-up".

Recommendation: This access to data stored in the back up copy seems disproportionate as the right of access already applies to data in production and archived data. Back-up data is personal data stored solely

for the purpose of restoring the data in the case of a data loss event and therefore should not be included in the scope of the right of access.

- Possibility to refer the data subject to past access requests (paragraph 109)

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 paragraph 109).

Recommendation: 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.

How can a controller provide access

- Layered approach (paragraphs 141-145)

In this section, the guidelines explain that in the case of vast amounts of data, a layered approach could be used by the controller. The EDPB also mentions that the use of a layered approach should not be confused with the possibility for the controllers to request that the data subject specifies the information or processing activities to which the request relates, as prescribed in Recital 63 GDPR. However, the two elements are not mutually exclusive and could be used to better answer to the data subject's request.

Recommendation: In this section, it is advisable to clarify that the controller may ask the data subject for more information concerning their access request. The first layer of information could consist of an overview of all the processing operations concerning the data subject with the second layer consisting of additional data specified by the data subject.

- Information on the processing and on data subject rights according to Article 15 (1) (a) to (h) and 15 (2) GDPR (paragraphs 110-120)

The EDPB states on paragraphs 110-120 that the information required by Article 15 (1) (a) to (h) and (2) need to be tailored to the data subject making the request for access. In another words, controllers must provide the data subject with tailored information based on the "actual case of the data subject" and that general information would not be sufficient.

According to the EDPB, for example, the data controller should not just offer a list of third parties to which personal data are communicated, but specify their activities, any sub-activities and leases.

Taking into account the high number of third parties who contribute to the pursuit of the insurance activity, this information could instead be less usable by the data subject, due to the excess of details, and could also possibly fall within those activities which would involve a disproportionate and excessive effort by the controller.

Recommendation: In order to offer essential and truly transparent and effective information, as well as to limit the impact on the controller's operations, it would be advisable if the controller could implement a

layered approach. Controllers could as a first step provide access to the information required by Article 15 (1) (a) – (h) and (2) in a general manner — similarly to a privacy notice — and then ask the data subject whether more tailored information needs to be provided. Unless the data subject explicitly requests such tailored information after being asked for specification, a general overview of processing activities should be able to fulfil the controller's obligation.

- Oral information and on-site access

In the executive summary, the EDPB state that "the main modality for providing access is to provide the data subject with a copy of their data but other modalities (such as oral information and on-site access) can be foreseen if the data subject requests it". However, the EDPB statement does not take into account various circumstances of the nature and type of data.

Indeed, the security process for an external person to have temporary access to the place of consultation, like suggested by the EDPB, is cumbersome to put in place. It would also be necessary to specify how to document information given orally or to supervise access on site.

Recommendation: The paragraph should be rephrased: "Other modalities of access can be asked by the data subject*, if they are appropriate in view of the volume of data and information to be communicated".*

Limits and restrictions of right of access

- Manifestly unfounded and excessive requests pursuant to Article 12 (5) GDPR (paragraph 173/187)

The guidelines state that Articles 12 (5) GDPR should be interpreted narrowly (paragraph 173). A request should not be regarded as excessive on the grounds that the data subject intends to use the data to file further claims against the controller (paragraph 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.

Recommendation: 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. It disregards and contradicts 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. The industry therefore recommends amending paragraphs 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.

It should be noted that such requests are also manifestly unfounded since they do not correspond with what the legislator intended when introducing the right to access.

Need for additional clarifications

The EDPB is also invited to provide additional clarification on the following points:

- Exercising the right of access through portals / channels provided by a third party (paragraph 88).
  - The guidelines determine that "the first issue controllers need to deal with when facing these circumstances refers to ensuring that the third party is acting legitimately on behalf of the data subject, as it is necessary to make sure that no data is disclosed to unauthorized parties". This sentence raises questions on how such verification of identity should take place. The EDPB is invited to provide further clarifications on this point.

- *Data request channels:* on page 2, the guidelines state that "the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller". The EDPB could provide further examples of possible official request channels that could be set up by companies.

- *Interpersonal communications:* on page 3, the guidelines explain that the right of access refers to personal data concerning the person making the request. This should not, however, be interpreted overly restrictively and may include data that could concern other persons too, for example communication history involving incoming and outgoing messages. Given the potential involvement of other parties (processers/sub-processors) and the impact on third persons, the EDPB could provide further examples concerning this circumstance.