Memorandum **Confidential**

To	European Data Protection Board
From	Stibbe Brussels Stibbe Amsterdam
Date	11 March 2022
Re	Comments on the Guidelines 01/2022 on data subject rights – Right of access

Stibbe Brussels and Amsterdam welcome the EDPB Guidelines 01/2022 on the right of access and we herewith submit our comments regarding the latter.

In view of this Consultation, Stibbe hosted a roundtable discussion for several of its clients who have ample experience with the exercise of the right of access. The comments below are a summary of the main concerns and remarks expressed by our clients.

The right of access is an important right of data subjects, enabling them to become aware of and verify the lawfulness of the processing of their personal data. Practice shows, however, that the exercise of this right can be burdensome. The right of access needs to remain manageable, and it need not overshoot its objective. The right of access can be interpreted and applied in such a way that provides data subjects the envisioned transparency, while taking practical considerations and possibilities for compliance into consideration as well.

In addition to this general remark, this Consultation contains comments and suggestions relating to specific topics that are addressed in the EDPB Guidelines 01/2022 on the right of access. Our comments and suggestions relate to different paragraphs of the Guidelines relating to the following topics:

- Who can request access?
- How should access be requested?
- What to do upon receiving a request?
- What should a response contain?
- How to provide information?

1 WHO CAN REQUEST ACCESS?

(a) *The exercise of the right to access by proxy through intermediaries*

We welcome that the EDPB considers the gradually increasing role played by intermediaries. In addition to the two issues discussed in the Guidelines[1], we wish to point out the increasing role and impact of automatically generated access requests submitted through intermediaries. Often, a specific or reasoned access request seems not to underlie such requests. Irrespective of the processing of personal data by intermediaries, this development carries with it the risk of increasing the administrative burden that controllers face. In turn, this could result in data subjects having to wait longer than one month to hear back, even in case they submitted a specific or reasoned access request. More fundamentally, this could result in the right of access heading towards becoming unworkable in practice. There should be room to take the administrative, economic and practical considerations of controllers and processors into consideration when interpreting and applying the right of access.

We therefore suggest specifying in the Guidelines that controllers must be allowed to refer data subjects to their own access request procedures. In addition, we note that considering administrative, economic and practical considerations is legitimate, without this detracting from the overall objective of the right of access.

(b) *The beneficiary of a request by proxy*

On the question "who can request access?" the Guidelines clarify the following:

> *"Although the right of access is generally exercised by the data subjects as it pertains to them, it is possible for a third party to make a request on behalf of the data subject."* (§79)

We are of the opinion that this clarification still leaves margin for misinterpretation as to the extent to which this right can be exercised by a third party.

We believe there is a difference between *making* a request and *benefitting from* a request. The Guidelines do not clarify whether a third party, when making a request, should also be the party *receiving* the personal data from the controller. Allowing a third party to make a request to access personal data *and* to also *receive* that personal data can amount to a risk for the data subjects to whom the requested personal data relates. A third party could for example request to obtain personal data on behalf of data subjects on a large scale with harmful intentions. Examples could be a large-scale request launched by a competitor of the controller or by a labour union aiming to compare salaries of employees. We do recognize that the processing of personal data received by a proxy for other purposes than the purposes related to the exercise of the access request, would qualify the proxy as controller for such purposes. Yet, we believe the controller transferring the personal data to the proxy should assess the risk and probability of the proxy processing the personal data for purposes incompatible with the aim of the right to access, based on the accountability principle in article 5.2 GDPR.

[1] Paragraphs 87 to 89.

We therefore suggest specifying in the Guidelines that, where possible, the requested personal data should be provided to the data subject itself when a proxy launches the request.

2 HOW SHOULD ACCESS BE REQUESTED?

In respect of the question "how should access be requested?" and whether the data subject should specify a reason for its request, the Guidelines specify the following:

> *"Controllers should not assess "why" the data subject is requesting access, but only "what" the data subject is requesting"* (§13).

Although a data subject is entitled to request access to its personal data without justifying his or her request, specifying the reasons of such request can be beneficial for both the controller and the data subject himself. The reason behind a request might provide a controller a valuable insight in what the data subject expects and how it could respond to that expectation as efficient and clear as possible. This would lower the burden for a controller, as well as strengthen the extent to which a data subject can exercise his or her access right. Controllers could provide the *possibility* to data subjects to, voluntarily, submit the reasons for their request through, for example, a blank box.

Furthermore, in many cases the reasons behind access requests go beyond merely verifying compliance with data protection laws, which in this case could justify an inquiry in the reasons for the requests. An illustration of such situation can be found in the decision of 1 December 2021 of the Belgian Marktenhof where the Court ruled, based on the reasons of a data subject's request, i.e. a fishing expedition, that the latter committed an abuse of rights in respect of the GDPR.[2] Another example is a decision of the District Court of Rotterdam that recently concluded that a data subject abused the right of access to bypass Dutch procedural laws governing discovery claims.[3] The above examples show that an exercise of the right of access can sometimes be contrary to other rights and rules.

We invite the EDPB to acknowledge that under certain circumstances, the exercise of the access right can clash with other rights and freedoms.

In practice, the question for access often is an expression of a specific question or concern. A question to specify the *what* of the request may be sufficient. Sometimes however, a question to specify the *why* can help enormously to provide what the individual seeks in an efficient way.

[2] Brussel, 19e k., 1 December 2021.
[3] District Court of Rotterdam 23 February 2022, ECLI:NL:RBROT:2022:1437.

We therefore suggest the Guidelines to maintain the prohibition for a controller to *require* a reason for the exercise of the right to access, yet to recognize the benefits for both the data subject and the controller to obtain insight in the reasons for a request.

3 WHAT TO DO UPON RECEIVING A REQUEST?

The Guidelines elaborate on the possibilities for a controller to refuse an access request. Concerning the limitation of the right of access by article 12(5) GDPR, i.e. in case of manifestly unfounded or excessive requests, the Guidelines do not specify entirely how 'manifestly unfounded' should be interpreted. No examples are provided of situations which might justify a refusal based on the 'manifestly unfounded' exception. This leaves a large margin for misinterpretation and conflict, for example regarding the question whether there is a possibility to refuse to act on the request if it is manifestly intended for other purposes than to assess compliance with data protection laws. An example of such manifestly unfounded request would be an access request from a manager to determine whether a complaint for sexual harassment was filed by an employee.

Concerning requests being excessive, the Guidelines clarify that a request can be qualified as excessive due to a repetitive character. The element of repetitiveness refers to a data subject launching subsequent access requests. The Guidelines however do not clarify whether a request can be excessive when exercised by proxy on behalf of a substantial group of data subjects.

We would therefore argue for more clarifications on the grounds for refusal of a right to access. The definition of 'excessive' should be broadened and should also include a disproportionate large volume of data subject access requests exercised simultaneously and regardless of a controller's means.

4 WHAT SHOULD A RESPONSE CONTAIN?

(a) *The meaning of "a copy of the personal data undergoing processing"*

The right of access does not necessarily require controllers to provide the actual documents in which personal data are included.[4] For example, the GDPR requires controllers to keep records of the categories of personal data that they are processing and to inform data subjects about these categories.[5] Providing data subjects with an accurate and complete overview of their personal data would generally be sufficient for them to verify whether their personal data are actually being processed in accordance with what they have read in data protection statements. Providing an accurate and complete overview keeps the administrative burden limited and results in quicker turnaround times, which would be beneficial to data subjects. Although there may be reasons to provide underlying documentation in certain circumstances, we believe that the right of access should

[4] Paragraph 23 and 150.
[5] Articles 30(1)(c) and 14(1)(d) GDPR.

not become a right to demand copies of any communication or documentation that include personal data, both as a principle and in order not to overburden controllers.

We invite to EDPB to more explicitly re-iterate that the right of access does not include the right to receive any and all documentation in which personal data are included.

(b) ***Proportionality of the efforts of the controller***

As to the extent of the response of the controller to the data subjects' request, the Guidelines provide that:

> "*unless explicitly requested otherwise by the data subject, a request to exercise such rights of access shall be understood in general terms, encompassing all personal data concerning the data subject."* (§35)
>
> "*the right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subjects' request*." (§164)

There is an inherent risk of carving out the right of access by requiring the disclosure of *all* personal data of a data subject, especially when controllers cannot request data subjects for specification. For the data subject, this could amount to an overflow of information, depriving the access right from its benefits. For the controller, such obligation amounts to a significant hurdle in terms of costs and organization, to the extent that compliance is almost impossible. For the right of access to be effective, the criterion of proportionality should be taken into account. The fundamental freedom to conduct a business may generally not weigh heavier than the fundamental rights to privacy and data protection, but a fair balance needs to be struck as much as possible.[6] A disproportionate burden on controllers needs to be prevented and can be prevented within the context of its scope and purposes as set out in the GDPR. Ultimately, a disproportionate burden would be detrimental to the goal of the access right and the data subjects, who would be facing considerable delay in having their access request addressed.

In this regard, the litigation chamber of the Belgian Data Protection Authority ruled in 2021 that the obligation to give access to *all* personal data of the data subject did not include access personal data which would require disproportionate efforts for the controller when compared to the benefits for the data subject.[7] In this case, the litigation chamber recognized that the search for personal data in IT logs of the controller gave rise to a disproportionate effort for the controller. In doing so, the Belgian Litigation Chamber recognized that a balance should be struck between the fundamental rights and freedoms of the data subject on one hand and the efforts required from a controller on the other hand.

[6] Article 17 and 52 Charter of the Fundamental Rights of the European Union.
[7] Belgian Litigation Chamber, 15/2021, DOS-2018-06125, 9 February 2021.

Our proposal as to the Guidelines is to specify that controllers should be required to undertake a *reasonable and proportionate search* for personal data to respond to a data subject's request, as opposed to making extensive searches which go beyond what is reasonable and proportionate to that end.

(c) ***Requests for specification***

On requests for specification, the Guidelines provide that:

> "*a controller who processes a large quantity of information relating to the data subject may request the data subject to specify the information or processing to which the request relates before the information is delivered. This exceptional situation may exist for example in case of a company with several fields of activity or a public authority with different administrative units, if the controller found that numerous data relating to the data subject are processed in those branches as well as in cases where the controller has been collecting data upon frequent activities of the data subject for years."* (§35)

The request for specification can be a great tool for controllers to address an access request in an efficient and timely manner. It is therefore crucial to have a clear view on the specific circumstances in which a controller is entitled to request a data subject for specifications.

We believe that the Guidelines are insufficiently clear. The cited paragraph 35 refers to, among others, "where the controller has been collecting data upon *frequent activities* of the data subject for *years*". Such conditions give rise to a substantial margin for interpretation. For example, it is unclear whether the processing of personal data in an employment context would meet the condition of 'frequent activities'. We would therefore encourage the EPDB to clarify the aspects of "frequent activities" and 'for years'.

Considering that a specification of an access request can significantly alleviate the burden for a controller to respond adequately to an access request, we suggest the Guidelines should clearly articulate in which cases a controller might ask a data subject to specify his or her request.

5 HOW TO PROVIDE INFORMATION?

(a) ***Access via non-permanent means and confidentiality***

The Guidelines provide clarifications on modalities to respond to an access request:

> *"Such non-permanent modalities of access to the data could be, for example: oral information, inspection of files, onsite or remote access without possibility to download. These modalities may be*

appropriate ways of granting access for example in cases where it is in the interest of the data subject or the data subject asks for it." (§131)

Using non-permanent modalities to grant access to personal data can under some circumstances not only be beneficial for the data subject, but also for the controller. For example, when granting access to personal data containing commercially valuable or confidential information, blacklining some or all of the data might not fully exclude a risk of loss of commercially valuable information. In addition, blacklining a substantial volume of documents including personal data can impose significant costs on a controller. In some cases, the personal data itself might constitute commercially valuable information. One might think of the comments on an important contract written by the legal counsel of an organization. In such case, granting non-permanent access might provide a middle ground between the disclosure of such valuable information and a response to the request. In addition, we would also encourage the EDPB to suggest the possibility for controllers to conclude a confidentiality agreement with data subjects obtaining access to confidential information.

From the perspective of the data subject, providing access through oral information may be a better way to be informed in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Doing so would allow controllers to provide additional clarification and context on its processing operations and to immediately address follow-up questions. Furthermore, in practice, we are seeing that data subjects are usually not necessarily after access to their personal data but rather hope to have an underlying issue resolved. Providing access through oral information would best allow controllers and data subjects to address such issues by entering into a reciprocal conversation. Moreover, getting to the bottom of such issues could alleviate the administrative burden that controllers are faced with to a certain extent.

We therefore suggest that the Guidelines should recognize the possibility for a controller to grant access through non-permanent modalities for personal data when it can demonstrate justified reasons to do so.

(b) ***Fees imposed by processors***

The guidelines clarify that a response to an access request should come at no cost:

"*Under the first sentence of Art. 15(3) GDPR, the controller shall provide a free copy of the personal data which the processing relates to*" (§22)

It is clear that the controller is required to provide a copy without imposing any fees on the data subject. Where the controller relies on a processor for the processing of its personal data, such processor is required to provide assistance to the controller with regard to the responding to an access request, based on article 28 (3) (e) GDPR. In practice, processors will often contractually determine that they are entitled to a fee whenever their assistance is required to address an access request. This creates an imbalance between the burdens imposed on a controller, vis-à-vis a data processor.

We would therefore encourage the EDPB to elaborate on whether processors are allowed to charge fees to the controller when they are involved in the response to an access request. We invite the EDPB to investigate the practices of processors, especially those of well-known cloud service providers, in this respect.

***