Feedback on Guidelines 01/2022 on data subject rights - Right of access

Contribution by Privacy Company (The Netherlands)

We appreciate the high-quality draft guidelines. As privacy professionals and as data subjects that have filed a substantial amount of access requests, we recognise many of the issues we encounter in practice in the guidelines. We want to offer a general perspective on the importance of the right to access that is often overlooked, and we have seven specific suggestions for additions to the guidelines relating to specific issues that we believe to be relevant.

1. Right to access serves a dual purpose

We regularly conduct DPIAs. When we assess the lawfulness of processing and the data subject risks, we always test the possibility of data subject access in practice. Such requests serve a dual purpose when we examine the processing operations by a third-party cloud service provider. Primarily as a test if access requests are properly handled by the service provider, but also to obtain information about the metadata the service provider is processing on its own servers. In our experience most service providers are relatively transparent about what they do with Content Data, but they can be quite resistant to disclose information about metadata such as remote diagnostic data, technical logs, security data, etc. Access requests are an essential tool to require such transparency from third-party service providers where substantial controller-processor audits are not feasible.

We want to suggest seven specific points we kindly ask you to include in the guidelines.

2. Compliance with the right to access affects the legal ground

For clarity's sake, we suggest to add to paragraph 10 in Section 2.1 that a refusal to provide access does not only result in a high risk for data subjects, but may also render the entire processing unlawful, due to the lack of a legal ground. An example of this can be found in the response of the Dutch Supervisory Authority to a prior consultation about Google Workspace.[1] We believe it would be valuable if the EDPB could include the reasoning of the Dutch Supervisory Authority in these guidelines to emphasise the importance of granting complete access when requested.

3. Assessment of risks when access is legitimately limited

Similarly, we suggest to add the following text between paragraphs 10 and 11, to help understand Recital 75 of the GDPR, and the ninth criterion from the EDPB to perform a DPIA.

"*Considering that the right of access isn't absolute there will always be processing operations where data subjects won't get full access to their personal data when they request access. For example, if secret camera surveillance is necessary in very specific circumstances, and data subjects are obviously refused access to the data during the authorised period of secret surveillance. If such circumstances lead to a*

[1] Response Dutch Supervisory Authority to request for advice from the Dutch universities and schools, URL: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z10598&did=2021D23167 The advice is included in Dutch in the attachment.

lawful access refusal, this still leads to a risk for data subjects. Unless the controller can design very effective mitigating measures, the controller must likely submit a prior consultation with the DPA."

4. Explain the scope of the right to access with a clear example

We suggest to add a specific example to paragraph 19, Section 2.2.1.2, to better explain the scope of the right of access, specifically for non-EU-based data organisations.

"A cloud service provider should not only provide access to the Content Data (including the Account Data) actively provided by its customer, but also provide access to all relevant metadata about the individual use of the service. This includes, but is not necessarily limited to: diagnostic data obtained from the end-user devices, service generated server logs, customer accessible audit logs (including registration of the individual behaviour of the administrators when they ask for access), personal data in and about Support Requests, personal data processed while interacting with external services through the platform, technical infrastructure generated data such as webserver access logs and network security logs."

5. Examples about time reference points

We suggest to add a new example to paragraph 38 in Section 2.3.3 to provide more guidance about possible mitigating measures when data are only processed for a short period of time.

"A service provider observes behavioural data from end user devices consisting of specific user identifiable events logged on the end user device, and centrally collected by the provider. The provider does not provide access to these personal data in reply to an access request, because it claims the data were anonymised or aggregated shortly after reception. Two possible mitigating measures are:

(i) Explain to the data subject (or to the data controller) what specific types of behaviour are observed, and how these data are processed. This includes an explanation about the differences between the collected data and the provided data.

(ii) Provide the data subject with near real time access, for example through a software client on the end user device to inspect the data as they are being collected from the device."

6. Structured or machine-readable data

When we professionally file data subject access requests, the responses are often voluminous, and difficult to understand and/or decode. To remediate this problem, we suggest adding the following text between paragraph 148 and 149:

"When considering if a chosen format to provide (a copy of) the data is appropriate, the machine-readability of the format must be considered. Especially when the volume of data is large, or the data structure is complex, data subjects need tooling to help them understand the data. For example, when providing many documents in PDF format, preventing the user from performing text searches on the document can significantly hinder the data subject's understanding of the data. When the data consists of large tables of data the data subject might require spreadsheet software to help filter or sort the data and thus a format like CSV might be more appropriate than a PDF. Transforming the data to such a format should be interpreted as a means to provide access to the data in an understandable form and should not be refused simply because the controller uses a proprietary format internally."

7. Data protection by design and by default and security obligations

Both article 25 and 32 include obligations for a data controller to protect the rights of natural persons. In practice we see multiple controllers who use privacy by design and security measure as a reason to refuse access to personal data. For example: processors who pseudonymise controller-supplied personal data. They may claim they are unable to re-identify the data, because they want to protect the data subject's privacy, and hence, cannot comply (or help the controller to comply) with access requests. Another frequently mentioned refusal reason from providers is that they have implemented strict measures to prevent internal employees from accessing (for the employee identifiable) personal data. The engineering effort required to develop access tooling is often cited as prohibitive. We kindly ask the EDPB to remind providers of their obligation to develop access tools by design.

We suggest including the following paragraph between paragraph 164 and 165:
Article 25 GDPR requires data controllers to implement appropriate measures to meet the requirements of the GDPR. Article 32 requires controllers and processors to take appropriate measures to protect the rights of natural persons. Both these obligations include the obligation to design and implement measures to support data subject access rights. A controller therefore may not simply assert that either or both of these articles legitimise not providing access. If circumstances require balancing the right of access with other rights and the data subject's access rights are negatively impacted by the choices made by the controller, it is likely that the controller must consult the DPA in an art. 36 GDPR prior consultation.

8. Summary of invalid refusal reasons

We suggest to provide an extra paragraph about invalid refusal reasons in the Guidelines, after paragraph 172 in Section 6.2. Such a summary would be extremely helpful in practice for privacy professionals to quote in discussions with processors and joint controllers about compliance with the access rights.

"*Though a controller may sometimes refuse access based on the company confidentiality of the data (such as described in the example of paragraph 171), this cannot be the case when such data are already publicly available (for example through reverse engineering). Access to security logging is especially important for the data subject to assess the compliance of the processing, including possible onward transfers to third parties or unauthorised access. If a controller refuses access because he is unable to reliably identify the data subject, he should accept all means to identify, including a cookie identifier, as explained in the example about cookies in paragraph 67. Additionally, a controller many not categorically refuse access because the systems are engineered to prevent access to personal data. [See the new text proposed by us in paragraph 7 of this contribution.]. Finally, access may not be refused with a reference to a third party if parties are joint controllers. If they are, they must design a mechanism to provide access to these data, as explained in Section 2.3, paragraph 34. Similarly, if a data subject files a data subject access request with a controller, the controller may not refer to a (possibly non-cooperative) data processor, but should contractually ensure that the processor provides the requested access.*"