Contribution to the public consultation on the Guidelines 01/2022 on data subject rights – the right of access

Dr. Diana Dimitrova[*], Laura Drechsler[**], Olga Gkotsopoulou[***] and Lina Jasmontaite[****]

Introduction

The Guidelines 01/2022 on data subject rights – Right of access ('the Guidance') are long awaited and form an important contribution for the better understanding of the right of access under the General Data Protection Regulation (GDPR). The right of access is often argued to be the most important individual right the GDPR grants to individuals and is strongly linked to the fundamental right to personal data protection (Article 8 Charter), as also noted by the European Data Protection Board (EDPB) in the Guidance.[1] We therefore welcome the adoption of the draft Guidance and the possibility to provide comments on it.

As legal researchers active in this area, we would also like to raise **three areas of concern** to the attention of the EDPB, where in our opinion some changes would be needed for the final version to ensure the full effectiveness of the right of access. These areas of concern are linked to **(1) the provision of the right of access**, **(2) the limitations and restrictions of the right of access**, and **(3) the scope of the Guidance**. This contribution will discuss each of these areas to formulate concrete questions to be answered for the final version of the Guidance. In light of the considerable length of the discussed Guidance, this contribution will not be able to discuss all potential issues arising from it but focus on those most linked to our own areas of expertise.

1. Provision of the right of access

1.1 Language, accessibility and intelligibility

Recognising the diversity among data subjects and the importance of inclusive participation, we welcome the reference to the provision of requested content in an accessible form, promoting and mainstreaming accessibility with respect to the enforcement of data protection law and the exercise of data subjects' rights. **All information and mechanisms for the request of this information should always be provided in an accessible format, as required by Article 12(1) GDPR**. We would like to bring the attention to **two main points** with respect to the envisaged concept of accessibility in view of assessing requests of the right of access: a) accessibility meaning barrier-free access to content requires **the case-by-case assessment of the requirements for content and format to be truly accessible by an individual**, including the provision of mechanisms for accessible communication and follow-ups between the data controller and the individual throughout the exercise of their right of access; and b) **requirements set for the sake**

[*] *Postdoctoral researcher at FIZ Karlsruhe-Leibniz Institute for Information Infrastructures and an Affiliated Researcher at the Law, Science, Technology and Society Research Group and Brussels Privacy Hub, Vrije Universiteit Brussel (Diana.Dimitrova@fiz-Karlsruhe.de).*

[**] *Research at Research Foundation Flanders (FWO), the Law, Science, Technology and Society Research Group and Brussels Privacy Hub, Vrije Universiteit Brussel (Laura.Drechsler@vub.be).*

[***] *Researcher at the Law, Science, Technology and Society Research Group and the Health and Ageing Law Lab, Vrije Universiteit Brussel (Olga.Gkotsopoulou@vub.be).*

[****] *Researcher at the Law, Science, Technology and Society Research Group and the Brussels Privacy Hub, Vrije Universiteit Brussel (Lina.Jasmontaite@vub.be).*

[1] European Data Protection Board, 'Guidelines 01/2022 on data subject rights – the right of access' (Version 1.0, 18 January 2022), p. 7.

of accessibility should not be viewed as a justification by data controllers for providing less information than required, limiting - instead of promoting - the right of access.

Specifically with respect to point (b) above, the Section 5.2.4. of the Guidelines currently provides for the possibility to use a layered approach 'when a controller processes a vast amount of personal data about the data subject and where there would be apparent difficulties for the data subject to grasp or comprehend the information if it were to be provided all at once'.[2] **The EDPB acknowledges that a layered approach is only one of the potential ways that can be used in this case and this approach can 'only be used under certain circumstances'. Nevertheless, the Guidance does not provide for those circumstances nor provide for other alternative ways.** Moreover, it is to be stressed that 'when deciding upon the format in which the copy of the personal data and the information under Article 15 should be provided, the controller needs to keep in mind that the format must enable the information to be presented in a way that is **both intelligible and easily accessible'** ***for the data subject concerned*** [emphasis], and in line with the particular needs specified by the latter.[3]

1.2 Identification of data subjects in line with Article 11 GDPR

In Section 3.1.1, the Guidance notes that controllers when dealing with a data subject request concerning the right to access, firstly, need to analyse whether it concerns personal data of the individual on whose behalf the request is made.[4] It also clarifies that 'pseudonymised data, which could be attributed to a natural person by the use of additional information, are personal data'.[5] The analysis of what constitutes personal data is further developed in section 4.1, which explains what personal data is subject to the right of access.[6] It clarifies that **identifiability of the data subject is the precondition to exercise the right of access**.[7] The two sections are closely related, and we believe that within the scope of these two sections there could be place for **further clarification on the application of Article 11** on processing which does not require identification.

Article 11(1) concerns situations where controllers process personal data, but the identification of individuals is not required (or no longer required). An illustrative example in this regard could be a clinical study, which relies on using data of human volunteers, where the controller has no possibility to directly or indirectly re-identify participating volunteers. Following the rationale of Article 11(2), if controllers can demonstrate that they are not able to identify the data subject, the controller shall inform the data subject accordingly, if possible. This subsequently results in a situation where data subject rights, including the right of access, cannot be exercised. In the aforementioned example, if the controller bought a pseudonymised data set from the hospital that was responsible for the collection of data, no information would be provided to the participating volunteers. At the same time, Article 11(2) notes that in cases where 'the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification', then the controller bears a duty to exercise an individual's request concerning the exercise of his or her rights.

[2] Ibid., p. 45.
[3] Ibid., p. 46.
[4] Ibid., p. 19.
[5] Ibid.
[6] Ibid., pp. 29-35.
[7] Ibid., pp. 33-34.

While we recognise that pseudonymised data could arguably reduce risks of the processing and 'make processing [subject] to more or less strict conditions, based on the flexibility allowed by the [data protection] rules',[8] we believe that ensuring legal certainty for data subjects through the Guidance concerning their rights should be a top priority. **We call for additional guidance and explanation on situations, in which data subjects, without knowing that their personal data are processed by the controller, could provide additional information, in order to exercise their right of access (i.e., Article 11 GDPR).** On the same note, we believe that in view of observed business practices further **clarification of the interaction between 11(2) and 12(6) GDPR is needed**. The two provisions should not be equated. Art 11(2) GDPR provides a data subject with the opportunity to confirm his or her identity from the perspective of the controller, whereas Article 12(6) allows a controller, who has **reasonable doubts** - the latter term is also very ambiguous and requires clarification- to request the provision of additional information necessary to confirm the identity of the data subject.

2. Limitations and restrictions of the right of access

2.1 The scope of Article 15(4) GDPR

The right of access is not absolute. The Guidance lists four types of limits and restrictions that could apply to the right of access and would result in individuals having either a reduced right of access or no right at all. These are: (1) Article 15(4) GDPR, (2) Article 23 GDPR, (3) Article 12(5) GDPR, and (4) Article 89(2) and (3) GDPR. **Due to the importance of the right of access for the fundamental right of personal data protection (Article 8 Charter), there is a need to ensure that these limitations and restrictions are applied restrictively and in light of the conditions applicable to restrictions to EU fundamental rights of Article 52(1) Charter**.[9] This is also reflected in Article 23 GDPR, which explicitly replicates these conditions and adds additional requirements.[10] The Guidance in its current form does not align with these outlined principles established by the EDPB itself in their guidance on Article 23 GDPR, for all of the noted limitations and restrictions. There is especially an issue with the restriction of Article 15(4) GDPR,[11] and the explanations surrounding abuse of the right of access.[12]

Article 15(4) provides that the 'right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others'.[13] The limitation of Article 15(4) differs from restrictions possible under Article 23 GDPR due to the fact that Article 15(4) can be applied by the controller confronted with an access request on a case-by-case basis, whereas any restrictions based on Article 23 GDPR need to be laid down in Member State or Union law. To ensure that controllers do not use this limitation unjustifiably, it must be clear when Article 15(4) applies. The EDPB argues that this limitation applies to the full component of access encompassed in the right of access, so not only to providing access in the form of a copy.[14] Since the wording of Article 15(4) only refers to the 'right to obtain a copy', we are deeply concerned by such an interpretation. There is **no textual**

[8] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (WP 136, 20 June 2007), p. 19.
[9] A connection between the conditions of Art. 52(1) Charter and the restrictions of data subject rights has also been made by the EDPB. See European Data Protection Board, 'Guidelines 10/2020 on restrictions under Article 23 GDPR' (Version 2.0, 13 October 2021), p. 6.
[10] Ibid.
[11] European Data Protection Board 2022 (n 1), pp. 49-52.
[12] Ibid., pp. 53-57.
[13] See also rec. 63 GDPR.
[14] European Data Protection Board 2022 (n 1), p. 50, para. 167.

basis in the GDPR allowing the limitation of the whole component of access, and we therefore would urge the EDPB to reconsider their approach and to confirm that this limitation only applies to access in the form of a copy.

The EDPB also proposes for the controller to assess the application of Article 15(4) taking account of the principle of proportionality and 'the likelihood and severity of the risks present in the communication' as one of its elements.[15] This suggests that the controller should use a **risk-based approach in order to determine the scope of the right of access**. There is no textual basis in Article 15 GDPR indicating a risk-based assessment. As the Article 29 Working Party has pointed out in their statement on the risk-based approach of 2014 'even with the adoption of a risk-based approach – there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively "low risk"'.[16] **We are not convinced that risk should be a relevant factor for the application of the right of access**. Rather, in a case where the right to obtain a copy of the right of access results in a conflict between different rights and interests, a 'balancing' or 'reconciliation' should take place that ensures that each of the conflicting rights can be guaranteed to the maximum extent. We would therefore suggest for the EDPB to delete the references to 'risk' and 'likelihood', when describing the assessment of Article 15(4), whose three steps seem otherwise very much aligned with the idea of 'balancing' and 'reconciliation'.

When discussing the limitations possible under Article 15(4), the EDPB rightly notes that these limitations are not applicable to the information component of the right of access (Article 15(1)(a)-(h) GDPR).[17] However, example 3 involving 'GAMER X' seems to suggest otherwise. In this example, it is argued that a gaming platform does not have to 'reveal any part of the technical operating of the anti-cheat software even if this information is relating to GAMER X' due to 'trade secrets'.[18] Article 15(1)(h) requires controllers to provide information about automated decision-making, including 'meaningful information about the logic involved...'. From the outset it seems that taking into account the finding that the exception of Article 15(4) does not apply to the information component, this information duty does require some information about the anti-cheat software to be revealed to the data subject. As will be discussed in the following section, the information provision with relation to automated decision-making has received rather little attention in the Guidance. It would therefore be of great use, if the EDPB could **clarify its practical application in this example thereby also clarifying the relation of trade secrets, Article 15(4) and Article 15(1)(h) GDPR**.

2.2 'Abusive' access requests

For the first time, the EDPB clarifies with some detail the provision on 'abusive' uses of data subject rights regulated in Article 12(5) GDPR. Article 12(5) GDPR states that controllers may 'refuse to act' upon a request or charge a fee, when a request is either 'manifestly unfounded' or 'excessive'. The terms 'manifestly unfounded' and 'excessive' are not further defined in the GDPR, though they also appear when it comes to situations when data protection authorities (DPAs)

[15] European Data Protection Board 2022 (n 1), p. 51, para. 171.
[16] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (WP 218, 30 May 2014), p. 2.
[17] European Data Protection Board 2022 (n 1), p. 50, para. 167.
[18] Ibid., p. 52.

under the GDPR can refuse to act upon a request or charge a fee.[19] The same provisions also exist in the Law Enforcement Directive (LED).[20] **The clarifications provided in the Guidance are therefore especially welcome, though it should have been made explicit whether the same considerations apply to DPAs and/or under the LED**.

When assessing the details of the clarifications, some aspects remain however unclear, making it difficult to ensure that these limits are used in a restrictive way. First, the explanation of what constitutes a 'manifestly unfounded' request, does not include any details, beside the fact that a request that is not in the scope of the GDPR should 'not be regarded as manifestly unfounded'[21] and that a request is not automatically 'manifestly unfounded' because previously submitted requests by the individual concerned were found to be abusive.[22] Even the provided example only concerns a request that should **not** (*emphasis by the authors*) be considered 'manifestly unfounded'. We would invite the EDPB to **add some details on what constitutes a 'manifestly unfounded' request, ideally also including an example of such a request, as was done for explaining the concept of 'excessive'**.

Continuing on the concept of 'excessive', we note a potential contradiction. Controllers are advised that requests are not 'excessive' just because there are 'no reasons' for submitting the request.[23] In addition, at several parts in the Guidance, the EDPB points out that the 'aim' of the data subject posing the access request is not a relevant consideration for controllers.[24] One example of excessive requests for the EDPB is however a request for access 'malicious in intent'.[25] **It is hard to see how controllers should on the one hand not consider the 'aim' of data subjects, while on the other, they can use 'malicious' intent to justify not responding to a request.** This will make it especially difficult to differentiate between individuals who 'systematically sends different requests to a controller as part of a campaign, e.g. once a week, with the intention and the effect of causing disruption' (excessive according to the Guidance),[26] and an individual who does the same but where weekly might actually constitute a 'reasonable interval' according to the Guidance.[27] It is also difficult to square this finding, with the statement of the EDPB that in case it is 'possible to provide the information easily by electronic means or by remote access to a secure system, which means that complying with such requests actually doesn't strain the controller, it is unlikely that subsequent requests can be regarded as excessive'.[28] We invite the EDPB to further clarify how to understand these different - potentially contradictory - statements together.

3. Scope of the Guidance

3.1 Need for more guidance on the exercise of the right of access in relation to automated decision-making

On p. 39 of the Guidance, the EDPB recommends that '(i)f possible, information under Art. 15(1)(h) has to be more specific in relation to the reasoning that led to specific decisions

[19] See Art. 57(4) GDPR.
[20] Arts. 12(4) and 46(4) LED.
[21] European Data Protection Board 2022 (n 1), p. 53, para. 176.
[22] Ibid., p. 53, para. 178.
[23] Ibid., p. 56, para. 187.
[24] Ibid., p. 9, para. 13.
[25] Ibid., p. 56, para. 188.
[26] Ibid., p. 56, para. 188.
[27] Ibid., p. 54, paras. 182-183.
[28] Ibid., p. 55, para. 184.

concerning the data subject who asked for access.' We welcome the fact that through this recommendation the EDPB has confirmed that Article 15(1)(h) GDPR applies to already taken individual decisions. We understand the reference to the 'reasoning' to mean that individuals are entitled to receive 'meaningful information about the logic involved' when an automated decision was taken and how abstract algorithms were applied in their individual case. However, we note that the EDPB seems to suggest that this information has to be provided only 'if possible'. The wording of Article 15(1)(h) does not include such a caveat. **Hence, the provision of the information on the reasoning is supposed to be the rule, unless an exception under Article 23 GDPR as transposed into national law or Union law applies.**

In addition, we invite the EDPB to provide further clarification on the following aspects for the information to be provided under Article 15(1)(h) GDPR: (1) **what information or types of information should be provided in relation to the reasoning**, e.g. factors taken into account, their interpretation and weight, a justification of the legality of the used logic, etc; (2) whether Article 15(1)(h) GDPR applies also to the **mere profiling activities which do not result in an automated decision being taken**, but which are usually nevertheless likely to influence automated and manual decisions and thus produce an impact on humans; and (3) what can be considered as examples of **other cases in which information about the logic or reasoning should be provided ('at least in those cases')** and in which the other safeguards in Article 15(1)(h) GDPR are supposed to apply. For example, whether the transparency requirements in Article 15(1)(h) GDPR should apply to partly automated decision-making processes, or even to non-automated decision-making based on (semi) automated personal data processing operations.

3.2 Need for guidelines on the right of access in the context of scientific research

Large amounts of personal data are being processed for the purposes of scientific research. As the Guidelines mention on p. 49, the GDPR contains special provisions for personal data processing for scientific research purposes. Indeed, Article 89(2) GDPR provides that 'Union or Member State law may provide for derogations from the rights referred to in Article(…) 15 (…) subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes'.

There is still a lot of uncertainty in academic literature and in practice about how to interpret the right of access to one's personal data and the derogations thereto in the framework of scientific research.[29] In particular, in view of the fact that the scientific purposes might be more broadly defined, **guidance is needed as to how to ensure the balance between respecting the right of access and the fulfilment of scientific purposes**, i.e. how researchers should create the appropriate processes for examining access requests, including what factors they should take into account in striking the balance, in order to ensure that refusals to provide access do not become the rule. We note that Article 89(2) GDPR clarifies that the derogations should be based on a legislative act, e.g. stemming from national law. Thus, ideally, the national law should provide guidance on this question.

[29] E.g. Ciara Staunton et al, 'The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks', 27 *European Journal of Human Genetics* (2019), pp. 1159-1167, available at https://www.nature.com/articles/s41431-019-0386-5; European Data Protection Board, 'Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research: Final Report' (August 2021), available at https://edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf.

For example, with regards to the derogations to data subject rights, Article 89(2) GDPR mentions that the derogations should be subject to the safeguards in Article 89(1) GDPR. **We invite the EDPB to specify what the minimum adequate safeguards could be when the right of access is restricted.** Such harmonized guidance would be a welcome addition to the guidance on (scientific) research already provided by the European Data Protection Supervisor (EDPS).[30]

3.3 The right of access under the GDPR and under the LED

Sometimes it might be difficult to determine whether the GDPR or the LED applies to the processing of certain sets of personal data. This is especially true in the context of databases which are used simultaneously for law enforcement, and migration and border control purposes, where both the GDPR and the LED might apply in parallel. Relevant examples are the upcoming ETIAS and EES Regulations and the Schengen Information System. Especially the ETIAS Regulation envisages a risk screening of the concerned Third Country Nationals (TCNs), via profiling, for risks related both to irregular migration and security threats.[31] **It might be sometimes practically difficult to delineate in these situations the applicability of the GDPR and the applicability of the LED. This poses problems for the exercise of the right of access, because in substance the right of access under the GDPR differs from the one under the LED.** For example, the right of access under Article 14 LED does not explicitly provide for decision-making and profiling transparency.[32]

This situation might put the data subject at a disadvantage and create uncertainties also to the controllers. **This uncertainty about the applicable law could also stem from the fact that law enforcement tasks could be amongst the grounds for restricting the right of access under the GDPR (Article 23 (1) (d) GDPR), i.e. by controllers who are subject to the GDPR and not to the LED, if there is a legislative measure in national or Union law.** This possibility further blurs the lines between the GDPR and the LED. In this context, it can be especially confusing to determine which authority effectively takes the decision to restrict the right of access: the controller who is subject to the GDPR or the law enforcement authority which is subject to the LED. This question has an impact on whether the right of access under the GDPR or under the LED applies. The Guidance should therefore include some explanations on how to distinguish the application of the right of access under the GDPR from the right of access under the LED in situations described above. The Guidance should especially explain how controllers should react in cases in which it might not be clear which legal framework applies and where this is an important question due to the substantive differences in the right of access. **These problems also demonstrates how important it is that guidelines also on the LED are issued**.

4. Conclusions

To conclude, we would like to thank again the EDPB for the opportunity to comment on the Guidelines 01/2022. We believe that ensuring legal certainty for data subjects concerning the exercise of their right to access and for data controllers with respect to the facilitation of this right

[30] European Data Protection Supervisor, 'Opinion 10/2017 EDPS Opinion on safeguards and derogations under Article 89 GDPR in the context of a proposal for a Regulation on integrated farm statistics', (20 November 2017); European Data Protection Supervisor, 'A Preliminary Opinion on data protection and scientific research', (6 January 2020).

[31] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (2018) OJ L 236/ 1, Art. 33.

[32] See discussion in Diana Dimitrova, *Data Subject Rights: The Rights of Access and Rectification in the Area of Freedom, Security and Justice* (PhD Thesis at the Vrije Universiteit Brussel, August 2021).

should be the key objective of this Guidance. To this end, we request the EDPB to consider the following in the revision of the Guidance:

1. In the context of barrier-free access, provide alternatives to a layered approach with respect to the right of access.
2. Clarify the 'certain circumstances' under which a layered approach could be used by data controllers.
3. Clarify the relation between Article 11(2) GDPR and Article 12(6) and the circumstances under which data subjects are able to provide additional information to the relevant controller under Article 11(2) in order to exercise their data subjects rights.
4. Clarify the meaning of the term 'reasonable doubts' within the meaning of Article 12(6) GDPR.
5. Reconsider whether the scope of the limitation of Article 15(4) GDPR should be extended to the whole component of access of the right of access in light of the clear wording of Article 15(4) noting only access in the form of a copy.
6. Reconsider whether 'risk' or 'likelihood' should be relevant considerations when assessing the scope of the right of access based on Article 15(4) GDPR.
7. Clarify how Article 15(4) when applied in the context of trade secrets interacts with the information obligation of Article 15(1)(h) for automated decision-making.
8. Clarify whether the provided explanations on 'manifestly unfounded' and 'excessive' requests of Article 12(5) GDPR also apply to DPAs confronted with requests (Article 57(4) GDPR) or for the LED?
9. Clarify the meaning of 'manifestly unfounded' and provide an example for a 'manifestly unfounded' request.
10. Clarify how controllers cannot consider the aim of data subjects for access requests while also considering malicious intent when assessing whether a request is 'excessive'.
11. Provide examples about the information or types of information in relation to the reasoning in the framework of automated decision-making systems, e.g. factors taken into account, their interpretation and weight, a justification of the legality of the used logic.
12. Provide examples about other cases 'at least in those cases' in which the safeguards in Article 15(1)(h) GDPR are supposed to apply, e.g. the mere profiling activities which do not result in an automated decision being taken and other semi-automated decisions.
13. Clarify the derogations to the right of access in the context of scientific research.
14. Provide guidelines on the right of access under the LED.
15. Clarify how to handle access requests where it might not be clear whether the GDPR or the LED applies, considering that the right of access under the LED and under the GDPR are substantively different.