noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

To: the European Data Protection Board

Subject: ***noyb observations on EDPB Guidelines 01/2022 on data subject rights – Rights of access (version for public consultation)***

Dear Ms Jelinek,

noyb welcomes the opportunity to submit comments on the EDPB Guidelines 01/2022 on data subject rights – Rights of access ("*the Guidelines*"). We submit the following observations for the consideration of the EDPB.

1. Introduction

noyb very much welcomes the recent Guidelines and congratulates the authors on the very detailed and useful guidance on the right to access. It is a very analytical document, based on rigorous legal analysis and consistent jurisprudential principles. In the interest of efficiency, our feedback is consequently only very short and focuses mainly on the elements that may benefit from further input. Nevertheless, we would like to express our utmost support for the general approach, for example:

- *noyb* agrees that access is instrumental to general transparency as well as the exercise of GDPR rights and that the scope of access follows the definition of personal data under Article 4(1) GDPR. Furthermore, *noyb* welcomes the statement that information under Article 15(1)(a) to (h) GDPR must be tailored to the specific access request and that the legal basis and recipients should be specifically mentioned.
- On the procedural side, *noyb* appreciates the sentiment that the data subject can define the scope of the request and that the data subject is not required to use a specific channel decided by the controller but may instead send the request to an official contact point of the controller.
- Moreover, it is useful to have clarified that authentication must use secure channels methods (i.e. email links and second factor authentication codes) which leaves very little room for ID documents requests. Lastly, *noyb* agrees that download tools cannot hinder the full access, leaving the responsibility for failures in this sense with the controller.

Beside *noyb*'s general agreement with the Guidelines, there are a few elements which *noyb* would like the EDPB to elaborate on.

2. Additional Feedback

noyb identified the following cases in which the guidelines could be improved:

2.1. Charter of Fundamental Rights, including Article 52(1) CFR

In our view, some of the (correct) findings in the Guidelines could be derived with a more solid legal underpinning by highlighting that the right to access is a right under Article 8(2) CFR, which must be interpreted using the proportionality test under Article 42 CFR. It seems to us, that a lack of detailed provisions in the GDPR could be filled by applying a proportionality test. So far some (correct) outcomes seem to lack such a legal basis or reasoning.

2.2. Differentiation between Article 13/14 and 15 GDPR

In our view the Guidelines could highlight in more detail the difference between a general *ex ante* information under Articles 13 and 14 GDPR and the specific and individualized *ex post* information under Article 15 GDPR.

While we acknowledge that the Guidelines seem to make this point using wording like "*tailoring*" or "*updating*" the information, it seems to us that the two provisions have a very different nature and may *de facto* overlap. In particular, the Guidelines seem to support a (problematic) practice of simply sending the privacy policy a second time as a standard procedure that only needs to be "adapted".

We worry that this wording could encourage controllers to continue a "copy/paste" approach. We would very much welcome if the Guidelines highlighted that the right to access is a right to be informed about the "real life" processing that actually took place (looking back), which may even be contrary to the information provided under Article 13 and 14 GDPR (looking forward).

Just like medication package insert, Articles 13 and 14 GDPR are aimed at giving general information to a data subject *before* swallowing the pill. The actual results may however be very different over time and per person. Just like a personal medical finding, Article 15 GDPR is aimed at giving this individualised information.

While we acknowledge that in some cases of simple processing operations (e.g. signing up to a newsletter) the planned processing and the actual processing are exactly the same, this should not be used as a standard assumption in the Guidelines.

2.3. Form of Identification

We would generally suggest to use the terms "identification" (finding the right person's data) and "authentication" (making sure the person that requests the data is actually the data subject), to make these two steps a bit clearer for readers.

While we support all other elements of the Guidelines in relation to authentication, we are missing a general statement as to the role of a data subject and a controller when determining the means for authentication. It seems to us that a data subject may choose to provide other means to proof that they are the right person, other than the ones foreseen by the controller. While the Guidelines highlight that, options are very different in the Member States (e.g. some use electronic signatures widely, others have a duty to show a paper ID). Controllers often require one specific way to authenticate, often inspired by the traditions of a certain jurisdiction.

A clear statement that data subjects may where appropriate choose to use another form of proper identification / authentication than the controllers foresees, would seem useful.

2.4. § 119 of the Guidelines: Guidance on Article 15(1)(h) GDPR and Automated Decision Making

The Guidelines refer to Article 15(1)(h) GDPR in § 119. According to the first sentence of that paragraph, in particular, every data subject should be informed in "*a meaningful way, inter alia, about the existence and underlying logic of automated decision-making including profiling concerning the data subject and about the significance and the envisaged consequences that such processing could have"*.

In general, the aforementioned sentence adds very little to the complex issue of information on profiling and automated decisions. This wording merely reproduces the content of Article 15(1)(h) GDPR. It is true that the EDPB makes a reference to some previous guidelines. However, this cross-reference does not help to precisely define the scope of the right of access and does not dissipate some very relevant doubts on the matter of algorithmic decisions which, conversely, would require a clear word from the EDPB.

The points in question will be discussed in the following.

2.4.1. "*referred to in Article 22(1) and (4) and, at least in those cases*"

Article 15(1)(h) GDPR only refers to paragraphs 1 and 4 of Article 22 GDPR. The EDPB might want to clarify that this does not limit the scope of Article 15(1)(h) GDPR and that the information it refers to must also be provided by the controller in case Article 22(1) GDPR does not apply, namely in cases of ADM that is not as impactful as required under Article 22(1) GDPR.

In this context, the Article 29 Working Party ("Working Party") has already pointed out that, "[i]*f the automated decision-making and profiling does not meet the Article 22(1) definition it is nevertheless good practice to provide the above information. In any event the controller must provide sufficient information to the data subject to make the processing fair, and meet all the other information requirements of Articles 13 and 14.*"[1] By calling the provision of the information "*good practice*", the Working Party seems to imply that the disclosure of information relies only on the good will of the controller. This interpretation is not supported by the system of the GDPR.

Article 15(1)(h) GDPR refers to the automated decision-making including profiling as "*processing*". As such, ADM, including profiling has to comply with all general principles of the GDPR, and in particular, personal data must be processed "*lawfully, fairly and in a transparent manner in relation to the data subject*"[2]. The Guidelines on Transparency[3] confirm such reading by highlighting the "*general principle that data subjects should not be taken by surprise by the processing of their personal data,* [and that this] *equally appl*[ies] *to profiling generally (not just profiling which is captured by Article 22), as a type of processing.*"[4] In other words, the Working Party clarifies that ADM including profiling[5], are typical processing operations under Article 4(2)

[1] Article 29 Data Protection Working Party [Working Party], Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251rev01, p. 25.

[2] Article 5(1)(a) GDPR.

[3] While only mentioning Articles 13 and 14 GDPR, the WP Guidelines on transparency under Regulation 2016/679, WP 260rev.01 [in the following: Guidelines on Transparency], are relevant due to the identical wording in Articles 13(2)(f), 14(2)(g) and Article 15(1)(h) GDPR: "*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*."

[4] Guidelines on Transparency, § 41.

[5] In this specific case, the Working Party only explicitly refers to "*profiling*". However, it must be implied that ADM is equally subject to the same logic. Indeed, ADM, especially when it involves profiling, fulfils the requirements of "*processing*" under Article 4(2) GDPR.

GDPR and, as such, must always be disclosed to the data subject to the extent necessary "*to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed*."[6]

Thus, in application of the above general GDPR principles, such information should not be seen as a mere "*good practice*". Rather, it is a real obligation. In other words, the phrase "*at least in those cases*" should be interpreted in the following way: The basic information regarding ADM and profiling must be provided regardless of the requirements of Article 22(1) and 22(4) GDPR being met. If those requirements are met, involving more impactful processing,[7] additional "*meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*" shall also be provided.[8]

2.4.2. "*meaningful information about the logic involved*"

The Guidelines do not provide further guidance on the definition of "*meaningful information about the logic involved*" in the context of Article 15(1)(h) GDPR, missing the opportunity to give controllers a simple way to comply with their information obligations.

Previously, the Working Party stated that the controller should inform the data subject in simple ways about the rationale behind the ADM including profiling but not necessarily give a *"complex explanation of the algorithms used or disclosure of the full algorithm".*[9] Furthermore, "*[t]he controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective 'weight' on an aggregate level)*"[10].

noyb would welcome further guidance by the EDPB in this regard, especially in order to avoid confusion due to extensive cross-referencing. In particular, *noyb* would like the EDPB to acknowledge the principle that "[c]*omplexity is no excuse for failing to provide information to the data subject*."[11]

2.4.3. "*envisaged consequences*"

Having clarified that the functioning of the algorithm, together with all the elements on which the individual decision is based, should be provided by the controller, it is now necessary to discuss the element that, in *noyb*'s view, should be subject to disclosure, namely the safeguards (if any) provided by the controller to counter the automated decision under Article 22(3) GDPR[12] (human overview, right to express the data subject's point of view and to contest the decision). Article 15(1)(h) GDPR makes no express reference to Article 22(3) GDPR with the completely untenable

---

[6] Recital 60 GDPR.

[7] Article 22(1) GDPR: „*decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*."

[8] In the context of Articles 13(2)(f) and 14(2)(g) GDPR, Mester comes to the same conclusion in *Taeger/Gabel, DSGVO-BDSG-TTDSG*, 4th edition 2022, Article 13, § 28. Due to the identical wording (see footnote 3), this interpretation must be transferred to Article 15(1)(h) GDPR.

[9] Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251rev01, p.25.

[10] Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251rev01, p. 27.

[11] Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251rev01, p. 25 footnote 40.

[12] Article 22(3) GDPR: "*In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interest, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*."

consequence that such information might not fall within the scope of the right of access. *noyb* considers that the EDPB should categorically reject this conclusion.

> **Example**: *Mario, a university student, decides to pay for part of his studies by working part time for a home delivery company as a rider. Mario searches online and discovers that there are two main companies to apply to, Delivery1 and Delivery2. Both companies provide a privacy policy in which they confirm the existence of ADM and describe the logic behind their operation. The only difference is that Delivery1, although not immediately informing its employees, has set up tools for human review of the automated decision under Article 22(3) GDPR. Delivery2, on the other hand, lacks them entirely. Not being aware of this difference, Mario subscribes to Delivery2. Immediately afterwards he makes an access request to know if there is any safeguard against ADM, but Delivery2 replies that such information is not required under Article 15 GDPR. Mario continues to work for the company but, following a knee injury, his performance declines to such an extent that he is dismissed from Delivery2's algorithm. If Mario had had an exhaustive answer to his access request, he would probably have decided to leave Delivery2 in favour of Delivery1 or another more guaranteed job*.

This example shows that "*envisaged consequences*" are not only the immediate consequences in connection with the algorithmic decision, but also the subsequent ones, possibly connected with the existence of enforceable rights.[13] In the light of the principles of foreseeability of consequences related to the processing of personal data, the EDPB should make it clear that the safeguards provided for in Article 22(3) GDPR should be openly and clearly shared by the controller.[14]

2.5. § 120 of the Guidelines: No Guidance on Article 15(2) GDPR

Finally, the Guidelines lack clear guidance on the interpretation of Article 15(2) GDPR. Here, the EPPB states that, "[i]*nformation about intended transfers of data to a third country or an international organisation, including the existence of a Commission adequacy decision or suitable safeguards, has to be given under Art. 13(1)(f) and 14(1)(f). In the context of a request for access under Art. 15, Art. 15(2) requires information on the appropriate safeguards pursuant to Art. 46 only in cases where transfer to a third country or an international organisation is actually taking place*."[15]

The EDPB should clarify that the right to be informed of the appropriate safeguards includes the right to obtain a copy of those safeguards or where such copies have been made available, as Article 13(1)(f) GDPR already stipulates. Considering that the purpose of both Article 13(1)(f) and Article 15(2) GDPR is to ensure the data subject's right to information, this principle must *a fortiori* be applicable following an access request pursuant to Article 15(2) GDPR.

Any other interpretation would conflict the logic of the right of access. Take the Standard Contractual Clauses[16] ("SCCs") under Article 46(2)(c) GDPR.[17] Generally, the SCCs are an invariable document, meaning that the parties cannot make changes to the clauses (and if they do, the SCCs automatically become *ad hoc* clauses subject to the prior authorisation of the DPA under

[13] See e.g. Gola in *Gola, Datenschutz-Grundverordnung*, 2nd edition 2018, Article 15, § 18 f.

[14] The fact that citizens are unable to foresee the consequences of the act is incompatible with fundamental principles of EU law, such as the principles of legal certainty and the protection of legitimate expectations. The principle of legal certainty means, in essence, that the individuals concerned must be able to ascertain the scope of their rights and to foresee the consequences of their actions. See, to that effect, CJEU judgments C 313/99 § 47, and of C 480/00, C 482/00, C 484/00, C 489/00 to C 491/00 and C 497/00 to C 499/00, § 85.

[15] EDPB Guidelines 01/2022 on data subject rights – Rights of access, § 120.

[16] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C/2021/3972.

[17] The same applies to all appropriate safeguards under Article 46(2) GDPR.

Article 46(3)GDPR). However, under the new SCC model, parties may add clauses which may potentially have an impact on the processing. Only the disclosure of the actual substance agreement would allow the data subject to review the lawfulness of the data transfer. Accordingly, a copy of the signed and dated agreement must be communicated.

The same "logic" extends, of course, also to the annexes of the SCCs.[18] Some of these documents, in fact, are crucial to assess the overall legitimacy of the transfer, in particular in relation to the additional security measures prescribed by *Schrems II*.[19] Take the case of the Transfer Impact Assessment ("TIA") referred to in Clause 14(d) of the SCCs. This clause only mentions an obligation to share the TIA the with the Supervisory Authority and do not speak of the disclosure to the data subject. However, the "silence" of the clause cannot be intended as a derogation to the general GDPR principle of transparency. As argued above, the GDPR clearly imposes disclosure of the TIA and the other annexes.

For the same reasons, the EDPB may want to highlight that not only the agreement but also its attachments must be disclosed.[20]

***

We hope these comments are useful for your work on the Guidelines and want to congratulate the authors once again on the general approach taken in these Guidelines. We are at your disposal should you have further questions or require additional clarifications.

Vienna, 11.3.2022

Max Schrems / Stefano Rossetti

[18] Both Articles 15(2) and 46 GDPR use "*appropriate safeguards*" as a meta term. If such appropriate safeguards can only be guaranteed by additional elements such as a TIA, these additional elements in turn fall under that meta term. As a result, additional elements must be disclosed pursuant to the same rules as the SCCs themselves.

[19] CJEU, C-311/18.

[20] It is crucial to note, in fact, that by virtue of the principle of informational self-determination, the data subject has the right to stop the transfer through his or her own choice, even before any decision by a DPA or a court can intervene (which is notoriously a long process).