Contribution to the Public Consultation to the EDPB Guidelines 01/2022 on data subject rights - Right of access

Students of the Master Course
Law and Technology in Europe[1]
Utrecht University

1. SECTION 1

> 5. The practical aim of the right of access is to enable the natural persons to have the control over their own personal data. (…)All this should lead to more effective **enforcement** of the right of access by data subject in the digital age.

This is the only paragraph that mentions the enforcement of the right of access, and it remains a very general one. Following the example of the ICO Guidelines, it could be clarified that DPAs can take actions against controllers that fail to comply with their obligations by means of administrative fines pursuant to article 83 GDPR, warnings, reprimands, enforcement notices or even penalty notices.[2] It can be noted that in cases of non-compliance the data subjects are even entitled to bring the cases to the Court and request compensation for damages, either material or non-material, pursuant to Article 82 of the GDPR. In that essence, the Higher Regional Court of Vienna awarded the data subjects with compensation for late answer to the SAR[3], the CNIL imposed a fine on a controller for not complying with the obligations relating to SAR,[4] the Spanish DPA ordered the controller to comply with their obligations.[5] All these different aspects of the enforcement of the right of access should be summarized and included in EDPB Guidelines. **(Stamatia Beligianni)**.

> 9. The EDPB considers it necessary to provide more precise guidance on how the right of access has to be implemented in different situations. These guidelines aim at analysing the various aspects of the right of access.

Should the right to access not be immediately mentioned as a standard information within the website's pop up or icon? In the sense, to what extent are DS supposed to know their rights? Such a requirement could enforce the website's privacy policy compliance and creates a level-playing field for awareness of rights given the uneven knowledge of legal rights[6]. (**Lejla Bešić)**

2. AIM OF RIGHT OF ACCESS, STRUCTURE AND GENERAL PRINCIPLES

> 10 The right of access is thus designed to enable natural persons to have control over personal data relating to them in that it allows them, "*to be aware of, and verify, the lawfulness of the processing'.* More specifically, the purpose of the right of access is to make it possible for the data subject to understand how their personal data is being processed as well as the consequences of such processing, and to verify the accuracy of the data processed without having to justify their intention. (…)

[1] Law and Technology in Europe, https://www.uu.nl/masters/en/law-and-technology-europe
[2] Information Commission's Office. (2020). Right of access. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/
[3] REPUBLIK ÖSTERREICH Oberlandesgericht Wien. (2020). 11 R 153/20f, 154/20b. https://noyb.eu/sites/default/files/2020-12/BVI-209_geschw%C3%A4rzt.pdf
[4] Commission Nationale de l'Informatique et des Libertés. (2022, 19 January). CNIL (France) SAN-2021-021. GDPRhub. https://gdprhub.eu/index.php?title=CNIL_(France)_-_SAN-2021-021
[5] Agencia Española de Protección de Datos. (2021, 15 December). AEPD (Spain) -R/00852/2021. GDPRhub. https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_R/00852/2021
[6] M. Sideri, S. Gritzalis, ‚Are we really informed on the Rights GDPR guarantees?' Human Aspects of Information Security and Assurance (2020)

It is disturbing to see that the right of access to determine the *lawfulness* of processing is rarely used by data subjects,[7] which points to a lack of awareness from data subjects about their rights. In this regard, it can be suggested that the EDPB create awareness by supporting online projects, such as Bits of Freedom's Privacy *Inzage* Machine and Citizen Lab and Open Effect's Access My Info, which assist individuals to generate access request letters. These projects identified here have been designed to create awareness for individuals about their rights in terms of Article 15 [8]. (**Roberto de Alcantara 1**)

The word "**sufficient**" could be understood in the sense that controllers just need to comply with the minimum when providing subject's rights. However, article 15 provides a complete ownership of subjects' personal data, with the corresponding limitations, not only the sufficient data to comply with regulations. Moreover, section 2.3.1 on completeness of the information explicitly states the right to obtain "full disclosure of data". For this reason, it would be more consistent to avoid the use of words that claim for measure, such as "sufficient", as it arises the question of who is supposed to measure what is sufficient and what is not concerning access to personal data. (**Isabel Sierra Rubio 1**)

The Guidelines missed opportunity to address the ***collective dimension of access rights***. An empirical study has illustrated that compliance with DSARs *in practice* was either completely absent or lacked transparency in their answers.[9] Interestingly, however, the study does not find that this renders the use of DSARs useless. Instead, it advocates for using the right in a collective manner, thereby (i) creating greater awareness and incentivizes discussions among data subjects and controllers and (ii) increase empowerment.[10] Thus, DSARs should be used collectively and aim at empowerment and transparency at a societal level. This is further argued in literature as it can counter information asymmetries, but also follows from the framework of the GDPR (Article 80(1) GDPR allows non-profit organisations to make complaints and litigate in the name of data subjects; national DPAs are established to monitor and enforce the GDPR; and organizations' DPOs monitor the compliance with the GDPR).[11] For these reasons, it is urged that the EDB recognizes the collective dimension of the right of access. **(Rijk Rouppe van der Voort)**

> 12. In accordance with CJEU decisions, the right of access serves the purpose of guaranteeing the protection of the data subjects' right of privacy and data protection with regard to the processing of data relating to them and may facilitate the exercise of their rights flowing from, for example, Art. 16 to 19, 21 to 22 and 82 GDPR. (…)

The guidelines are correct in stating that the exercise of the right of access pursuant to Article 15 is an individual right on its own and not a condition upon the exercise of the other rights listed. However, the converse as stated in the paragraph is also true but can be better restated. To this end the EDPB should consider rephrasing this paragraph by confirming that the other rights data subjects are entitled to under Chapter III, such as the right to rectification (Art. 16), the right to erasure (Art. 17) and portability are more **effectively** exercised if the data subject has access to his or her data[12]. Therefore, to a certain extent, the effective exercise of the other rights does depend on the right of access. (**Roberto de Alcantara 2**)

> 16. Art. 15 can be broken down into eight different elements as listed in the table below:

A model response to an access request can be attached to the guidelines as an annex to clarify the process for data controllers and data subjects. This could be achieved by creating a general template for a fictitious data subject which shows the various categories that need to be added, such as the purpose of processing, recipients of data, the categories of data etc. The additional personal data needed for verification of the identity can be added to provide an example of how it can be done. This is especially helpful to smaller companies who are not as familiar with access requests and

---

[7] Rene Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively exercising the right of access: individual effort, societal effect" (2018) 15
[8] ibid 17
[9] Mahieu, R. L., Asghari, H., & van Eeten, M. (2018). Collectively exercising the right of access: Individual effort, societal effect. *Internet Policy Review, 7*(3), 1-23. https://doi.org/10.14763/2018.3.927.
[10] Ibid.
[11] Mahieu, R., & Ausloos, J. (2020). Recognising and enabling the collective dimension of the GDPR and the right of access, page 11. https://doi.org/10.31228/osf.io/b5dwm.
[12] Jef Ausloos, Michael Veale and Rene Mahieu, 'Getting Data Subject Rights Right' (2019) 17

do not have a DPO. This template is not necessarily meant to be used by companies as a standard template. However, it is more meant to give an idea of what a proper response to an access request looks like. (**Elena Sheikhbahaei)**

> 19. (…) The obligation to provide access to the data does not depend on the type or source of those data. It applies to its full extent even in cases where the requesting person had initially provided the controller with the data, because its aim is to let the data subject know about the actual processing of those data by the controller.

The paragraph states that the obligation of the data controllers to provide access to data "applies to its full extent even in cases where the requesting person had initially provided the controller with the data". The wording of this part of the paragraph appears to be slightly confusing. In all cases, data controllers have access to the data due to the data subject's previous actions. The lawfulness of the processing is based on certain legal bases, such as the consent of the data subject through which the latter provides access to his/her data. Therefore, the question regarding which are the "other cases" - besides the cases "where the requesting person had initially provided the controller with the data" arise. More specifically, someone could argue that the wording leaves the impression that there are some cases in which the requesting persons would not be able to have access to their data due to the fact that they initially provided the controller with them. (**Eleni Arampatzi**)

> 20. The third component of the right of access is the information on the processing and on data subject rights that the controller has to provide under Art. 15(1)(a) to (h) and 15(2). Such information could be based on text taken, for example, from the **privacy notice** of the controller11 or from the controller's record of processing activities referred to in Art. 30 GDPR, but may have to be updated and tailored to the data subject making the request. (…)

Referring to **a privacy policy** in order to provide the data subject with information pursuant to Art.15(1)(a) - (h) does not meet the controller's transparency obligations as further discussed in paragraph 112. It is understandable that tailoring each individual right of access request may be onerous, especially for big companies that receive a lot of daily requests. However, big companies that receive numerous requests also have a lot of resources and they employ automation in a lot of their daily operations. (**Joanna Taneva)**

As it has been concluded from the use of empirical evidence, controllers often reply to access requests by disclosing only general information which is 'already available in the privacy policy/notice/statement'[13] of these controllers. Consequently, this information is not always tailored to the data subjects who wish to obtain data that correspond to their specific situation. (**Olga Lampousi**)

> 23. The **obligation to provide a copy** is not to be understood as an additional right of the data subject, but as modality of providing access to the data. it strengthens the rights of access to the data and helps to interpret this right because it makes clear, that access to the data under Art. 15(1) comprises complete information on all data and cannot be understood as granting only a summary of the data. (…)

The scope of Article 15(3) and thus the width of the copy coincides with the definition of personal data as provided for in Article 4(1) GDPR. A position paper by the EDPB held the view that, included in the scope of personal data, are special categories of personal data (as per the provisions of Article 9)[14]. The interpretation of the EDPB regarding the access of 'complete' information on 'all' data is on point and supported by the ruling of the German Federal Supreme Court[15], which made clear that the scope of the right to access is to include, inter alia, a request for 'all data'. Such a request would be regarded as a sufficiently precise request. Furthermore, access may not be limited to data which is not yet known to the data subject. This view seems to be supported by the ICO Guidance Document to the General Data Protection Regulation which does not refer to any 'requirement' that data exist at the time of the access request. (**Roberto de Alcantara 3)**

---

[13] Ausloos, J., Veale, M., & Mahieu, R. (2019). Getting Data Subject Rights Right: A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance. *JIPITEC*, 10(3): 283-309. https://doi.org/10.31228/osf.io/e2thg. p 293.

[14] GDPRHub, Article 15(3)

[15] BGH, Urteil vom 15.06.2021 - VI ZR 576/19

28. If the data subject asks for **an additional copy** after the first request was made, questions may arise on whether this should be regarded as **a new request**, or whether the data subject wants an additional copy of the data in the sense of Art. 15(3)(2), in which case a fee for an additional copy may be charged. (…)

(1) The current guidelines do not provide guidance on the severity of the fees involved for additional copies. An empirical study[16] refers to the possibility to charge a reasonable fee for SAR, however, this still does not constitute a clear explanation as to what this definition could entail. A lack of clarity could lead to potential abuse of data controllers by implementing excessive fees to prevent data subjects from making SAR too often. (2) It is unclear what should be the timeframe in between each SAR to not be considered excessive. The above example refers to making SAR a week after the first week, but it can be borderline to being excessive. (**Magdalena Rangelova**)

30. Concerning the allocation of **costs** in cases of requests for an additional copy, Art. 15(3) establishes that the controller may charge a **reasonable fee** based on the administrative costs that are caused by the request. (…)

Based on a case in 2013, it was determined that '*in order to ensure that fees levied when the right to access personal data is exercised [..], the level of those fees must not exceed the cost of communicating such data'*. [17] Similarly, this interpretation of fees could be applied in cases where a data controller may charge a reasonable fee for additional requests for copies or for 'unfounded and excessive' requests by ensuring that the levying fees do not exceed the administrative costs and communication costs. The ICO provided some examples to organizations regarding the determination of administrative costs for copies or 'unfounded and excessive' requests.[18] These elements ensure that the process is efficient and that there are no overlaps in activities performed by the data controller during the process. In a comparable way, this guideline could provide such examples for data controllers to determine the administrative costs that are caused by the additional request for copies or unfounded and excessive requests. It would be beneficial to include on the requesting access page a notice banner addressed to the data subject with the necessary information regarding the possibility of administrative costs for copies or 'unfounded and excessive' requests. This way, the data subject can decide whether they wish to proceed with their request and take the risk that their request may be found unfounded and excessive to the extent that they may be charged an administrative cost. Furthermore, the notice would also highlight that for additional copies the data controller may charge a fee. In this way, it can be avoided that data subjects make abusive requests to burden the data controller. [19] **(Thalis Cabral)**

32. In the event of **a request by electronic form means,** information shall be provided by electronic means where possible and unless otherwise requested by the data subject (see Art. 12(3)). (…)

The Guidelines refers to PDF files. It is indeed commonly used but regarding accessibility[20] and popularity of the PDF files, studies have shown that data subjects do not prefer providing information in a mentioned form. About 99.6 % of study participants chose webpage structure rather PDF.[21]An additional study showed that one of the main causes of frustration on the internet is inaccessible pdf files and followed difficulties.[22] In order to prevent additional

[16] Inge Graef, Martin Husovec And Jasper Van Den Boom. (2020). Spill-overs in datagovernance: Uncovering the uneasyrelationship between the GDPR's right to data portability and EU sector-specific data access regimes. *Journal of European Consumer and Market Law = EuCML*, 9(1).

[17] Case 486/12 X EU:C:2013:836 [2013] (preliminary ruling concerns the interpretation of Article 12 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

[18] Information Commissioner's Office, 'What Should We Consider When Responding to a Request?' (Information Commissioner's Office) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-should-we-consider-when-responding-to-a-request/#fee > accessible, 26 February 2021

[19] Centre for Information Policy Leadership, 'Data Subject Rights under the GDPR in a Global Data Driven and Connected World' (2020 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_data_subject_rights_under_the_gdpr_in_a_global_data_driven_and_connected_world__8_july_2020_.pdf > accessible, 27 February 2022 18

[20] Roger Hudson, "PDFs and Accessibility", 2004. Available on http://usability.com.au/2004/05/pdfs-and-accessibility/ , accessed on 25.02.2022.

[21] Wild G., Craddock D. (2016) Are PDFs an Accessible Solution?. In: Miesenberger K., Bühler C., Penaz P. (eds) Computers Helping People with Special Needs. ICCHP 2016. Lecture Notes in Computer Science, vol 9758. Springer, Cham.

[22] Jonathan Lazar and others, 'What Frustrates Screen Reader Users on the Web: A Study of 100 Blind Users' (2007) 22 International Journal of Human–Computer Interaction 247.

complications, the wording of the Guidelines should be adjusted so it could not be interpreted as PDF usage is in any way suggested. **(Marina Mijuskovic)**

Providing information under Article 15 of the GDPR only in a PDF designed for printing and not analysis[23] might not comply with the requirement of providing information in a 'concise, transparent, intelligible and easily accessible form.' Namely, if a controller had a very large amount of data points on a data subject, the lack of a friendly format could negatively affect the data subject's comprehension of the provided information. That could, in turn, have a negative effect on the exercise of her other rights. Hence, controllers should be encouraged to also provide information in an open format intended to be both machine- and human-readable, such as XML.[24] **(Eva Opsenica)**

34. When data subjects make a request for access to their data, in principle, the information referred to in Art. 15 GDPR must always be provided in full. (…)

A possible issue concerning data requests is whether a data controller can consider that a SAR is already satisfied if another controller provided the same personal data to another request. For instance, in a Spanish case, a data subject requested the City hall of Gata and another authority to get access to his personal data. The data subject requested the same personal data used to calculate a local tax in both SARs. The authority replied; however, the City hall refused the request because the authority had already answered the same request. The Spanish DPA held that, although the requested personal data were the same in both cases, the municipality should have answered the request independently from the Authority.[25] Since similar tensions might arise in other cases too, the Guideline should consider not only data processing of joint controllers but situations when two or more independent data controllers process the same personal data and a data subject requests access from all of them. (**Patrik Kovács**)

Situations will often arise where multiple data controllers can be determined. On the other hand, both the CJEU and the EDPB have made clear that joint responsibility does not necessarily lead to the same responsibilities.[26] The EDPB merely limits the Guidelines to stating that joint controllership does not affect the right of a data subject to make his DSAR vis-á-vis either one of the controllers. However, as illustrated by Mahieu et al.,[27] the current "networked settings" combined with the broad legal definition of a data controller leads to the undesirable situation where many different data controllers can be distinguished, such as both a social medium and a hosted fan page or a social medium and a website that links to that medium. From the perspective of the (small) data controller, it seems problematic that data subjects can exercise their DSAR vis-á-vis both controllers (ie. the 'big' social medium and the 'small' website/fan page). Due to a lacking overview of data flows, power imbalances and specialized units that process personal data,[28] compliance with certain DSARs can sometimes realistically be impossible. Therefore, it is recommended that the Guidelines address this issue by either (i) addressing the potential power imbalance between data controllers through laying the responsibility of compliance at the 'big' data controller or (ii) giving further reasons as to why also the 'small' data controllers will have to comply equally. **(Rijk Rouppe van der Voort)**

35. Data subjects have the right to obtain, with the exceptions mentioned below, **full disclosure** of all data relating to them. Unless explicitly requested otherwise by the data subject, a request to exercise the right of access shall be understood in general terms, encompassing all personal data concerning the data subject 14. Limiting access to part of the information may be considered in the following cases (…)

---

[23] Ausloos J., Veale M., & Mahieu R. (2019). Getting Data Subjects Rights Right. *JIPITEC*, 10(3), 283-309, 286. https://doi.org/10.31228/osf.io/e2thg

[24] Information Commissioner's Office. *Right to data portability: What is XML?* ico. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/?q=privacy+noticeshttps%3A%2F%2Fico.org.uk%2Ffor-organisations%2Fguide-to-the-general-data-protection-regulation-gdpr%2Findividual-rights%2Fright-to-be-informed%2F%3Fq%3Dprivacy+notices#ib17

[25] Agencia Espanola Proteccion Datos (AEPD). (2021). Case: PS/00040/2020. https://gdprhub.eu/index.php?title=AEPD_-_PS/00040/2020 accessed 24 February 2022.

[26] Case C-25/17. Jehova's witnesses (CJEU July 10, 2018); European Data Protection Board (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para 58.

[27] Mahieu, R., van Hoboken, J., & Asghari, H. (2019). Responsibility for Data Protection in Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 10(1), 85-105, 100.

[28] Ibid.

According to paragraphs 35 and 150 of the Guideline, data subjects have the right to a complete and 'full summary' of their data. However, it might be difficult for the data subjects to know whether the provided data is fully complete. Therefore, the Guideline should also offer some recommendations concerning practices that can help the data subjects evaluate the completeness of the given information. For instance, Mahieu et al. described in their study that matching responses might be helpful in this question: if data subjects can obtain personal data from related or similar organisations, then the data subject can have a better judgment on the completeness of individual answers.[29] (**Patrik Kovács**)

Requests for access to data are frequently accommodated by controllers through recital of generic information already available in their privacy policy/notice/statement.[30] This practice was seen as problematic for Ausloos et al. as the answer should tailor the information to the specific situation of the data subject making the request. (**Roberto de Alcantara 4)**

It is unclear to what extent the controller must take measures in order to comply with the SAR as to what data to provide. It seems clear from the outset that the controller is not obliged to search for personal data of the subject when this is unreasonable or disproportionate to the importance of providing access to the information.[31] It is recommended that the Guidelines include *factors* for the data controller to consider when assessing the reasonability and proportionality of the search for personal data. These may include, but are not necessarily limited to:
- the circumstances of the request;
- any difficulties involved in finding the information; and
- the fundamental nature of the right of access.[32] **(Rijk Rouppe van der Voort)**

While providing information on how to deal with large amounts of data and its complete delivery to the data subject, this section concerning completeness of the information omits the fact that the completeness of information is rather unrealistic, and if not, almost unfeasible for controllers in many circumstances. As showed in research carried out in 2018, out of 80% of replies from controllers on SAR, most of it was somehow incomplete.[33] Not only when delivering data but also on the way of retrieving the data, controllers may find themselves in front of an impossible task, being asked to provide all data retrieved from subjects. As an example, the controller may not have the data at the precise moment[34] when it is requested because it has been already **deleted**, but it may have **shared it with third parties** that still have that data stored. Although this information might have been shared with the data subject in the privacy notice, there is ambiguity with the completeness of information duty. It is unclear whether controllers have to share which data is shared with third parties as part of completeness duty even when the controller already deleted that information. Technically, data is not stored or processed by that controller anymore, but for the subject, that data is still processed and stored by a different party. In a Judgment of June 2021, The German Federal Supreme Court stated that the right of access is only satisfied when "information provided represents the total scope owed" and that the main factor to decide on this is a declaration from the controller that the information is complete.[35] Moreover, in a different case that analyses the right of access from a broader scope, the controller was asked to provide information of all existing data.[36] Court decisions and empirical research seem to arrive to different conclusions, and it is unclear what 'completeness' means in practice, as the theory may not always be applicable. (**Isabel Sierra Rubio 2**)

> 37. The assessment of the data being processed shall reflect as close as possible the situation when the controller receives the request and the response should cover all data available at that point in time. (…)

Neither the GDPR nor the Guideline determines under what circumstances personal data might be considered erased or deleted. This question is a crucial factor if the data controller must answer a SAR because it might happen that some

[29] Mahieu, R.L.P., Asghari, H. & van Eeten, M. (2018). Collectively exercising the right of access: individual effort, societal effect. *Internet Policy Review, 7*(3). DOI: 10.14763/2018.3.927
[30] Ausloos, J., Mahieu, R., & Veale, M. (2019). Getting Data Subject Rights Right. *JIPITEC, 10*, 283-309, 285, para 55.
[31] Information Commissioner's Office. (2021, May 20). *Guidance on the right of access*, p. 28. ico.org.uk. Retrieved February 24, 2022, from https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf.
[32] Ibid.
[33] Asghari, H., Biemen, T.V., & Warnier, M. (2021). Amplifying Privacy: Scaling Up Transparency Research Through Delegated Access Requests. ArXiv, abs/2106.06844.
[34] This relates as well to section 2.3.3 of these Guidelines, which analyses time reference point of assessment
[35] Judgment of 15 June 2021, Case No. VI ZR 576/19, Federal Supreme Court Germany
[36] Judgment of 8 June 2021, Case No. 16 A 1582/20, Higher Administrative Court of Munster

'deleted' data still exist in another form or another system, while the data controller assumes it is deleted.[37] The result of such a situation is that the data controller is still obliged to provide those personal data for a request, whereas the data controller might think there is no such obligation. Consequently, the Guideline should clarify when personal data is genuinely erased to avoid these situations. (**Patrik Kovács**)

3. ASSESSMENT OF ACCESS REQUESTS

42. Therefore, the controllers should be proactively ready to handle the requests for access to personal data.(…)

The ICO provides various ways and methods which the controllers can use to prepare and be ready for such access requests.[38] I believe these need to be added to this guideline to ensure maximum clarity and compliance. (**Elena Sheikhbahaei**)

Data controllers should be provided with a guiding answer template, as it can be helpful to a large extent for them in order to be acquainted with how *an appropriate reply* should be. The ICO has developed a basic reply template to help controllers document their processing activities.[39] This particular documentation template helps controllers to fill in a variety of specific categories which are, inter alia, the purpose of processing, the name and contact details of possible joint controllers, categories of individuals and categories of personal data. By following such template, omitting information by controllers will be prevented, contributing to a better approach of the *appropriate reply* measure. (**Olga Lampousi**)

44. Under the GDPR, the scope of the request shall **only cover personal data**. Therefore, any request for information about other issues, including general information about the controller, its business models or its processing activities not related to personal data, is not to be considered as a request made pursuant to Art. 15 GDPR (…)

Regulation on a framework for the free flow of non-personal data in the European Union'[40] foresees a 'mixed' dataset scenario. Article 2(2) provides that in the case of a dataset comprised of both personal and non-personal data where the respective datasets are inextricably linked, the data protection rights and obligations arising under the GDPR shall take precedence and apply fully to the whole mixed dataset, even if the personal data represents a small part of the set.[41] It can therefore be argued that this provision, to a certain extent extends the scope of application of Art. 4(1) GDPR to include non-personal data. This argument is supported by the decision of the German Federal Supreme Court[42], which makes clear that the scope of the right to access is to include, inter alia, a request for 'all data'. The EDPB could investigate introducing an exception to a request for information that could be considered non-personal data, but only if it can be proved to be inextricably linked to the data subject's personal data. **(Roberto de Alcantara 5)**

50. (…) in case of any doubts it is recommended for the controller to ask the data subject making the request to **specify the subject matter of the request.**

The specifics surrounding data processing, both from the legal and technical perspective, may not be fully comprehended by DS, who are usually lay people. If a DC uses technical or legal jargon when requesting DS to specify the request, it may lead to intimidation of the DS and abandonment of the initial request. This tactic, which traces back

[37] Information Commissioner's Office (2014) *Deleting personal data* p2 https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf accessed 21 February 2022.
[38] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/how-should-we-prepare/
[39] Information Commissioner's Office. (2021). Guide to the General Data Protection Regulation (GDPR). Retrieved from https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf. p 183.
[40] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) PE/53/2018/REV/1 *OJ L 303, 28.11.2018, p. 59–68*
[41] Dionysia Kontotasiou, 'Non-personal Data: How to Handle It & the Opportunities for Businesses' (2019)
[42] BGH, Urteil vom 15.06.2021 - VI ZR 576/19

to sales tactics used on consumers[43], may enable DCs to get a better understanding of what type of DS they are dealing with and as a result may lead to behaviours categorized as *discourses of denial* by Norris et al (2017) in order to either wittingly or unwittingly obstruct the DS from exercising their right of access.*[44]* (**Urszula Baranowska)**

52. As noted previously, the GDPR does not impose any requirements on data subjects regarding the form of the request for access to the personal data. (…) 53. The EDPB encourages the controllers to provide the most **appropriate and user-friendly communication** channels, in line with Art. 12(2) and Art. 25, to enable the data subject to make an effective request (…)
54. It should be noted that the controller is not obliged to act on a request sent to a **random or incorrect email** (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights, if the controller has provided an appropriate communication channel, that can be used by the data subject.

The CNIL has pointed out that '[W]hile Article 25 does not explicitly seem to address designers, it allows us to look at and highlight "privacy design", how different design techniques are used in the staging of services for -and sometimes at the expense of- the protection of individual data, especially with regard to the major principles of transparency, consent and rights of individuals'[45] and that the exercise of data subjects rights, such as data access, 'is above all a matter of user pathway and context'. This includes, for example, that the information about the right of access and the channels provided are **easily accessible and prominently displayed to the data subjects** given that the right of access is instrumental to the exercise of other rights; that the form is not overly complicated or that it misleads data subjects about which right is being exercised (for example by bundling all data subjects right together). (**Phillipe Truan 2**)

Controllers cannot pose a mandatory form of the request for data subjects and self-service tools should be facilitators[46], though these download tools may limit the right of access by the way they are designed e.g. dark patterns[47]. Thus, patterns can hide, confuse, manipulate and coerce disclosure of personal data.[48] In relation to right of access, particularly important is Interface Interference as "any manipulation of the user interface that privileges specific actions over others".[49] Additionally, to download tool, practice showed that "when data subjects request access to additional information not included in 'download my data' functionalities (but mentioned in Article 15), they are often ignored".[50] Dark patterns make it even more difficult for disabled people and children to access personal data.[51]Therefore, the Guidelines shall consider measures and obligations of the controllers, including categories of children and disabled people. **(Marina Mijuskovic)**

58. In order to ensure the security of processing and minimize the risk of unauthorised disclosure of personal data, the controller must be able to identify the data subject, i.e. find out which data refer to the data subject, and confirm the identity of the person in case of doubts.

[43] Clawar S.C., (1977) Patters of intimidating the consumer *The Journal of Consumer Affairs* 11(2)
[44] Asghari H., Van Biemen T., Warnier M. (2021) Amplifying Privacy: Scaling up transparency research through delegated access requests *IEEE Technology and Consumer Protection 2021*
[45] CNIL 'Shaping Choices in the Digital World From dark patterns to data protection: the influence of ux/ui design on user empowerment' IP Reports Innovation and Foresight Nª 06 (2019) 10.
[46] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.;
[47] Ari Ezra Waldman, Cognitive biases, dark patterns, and the 'privacy paradox', Current Opinion in Psychology, Volume 31, 2020, Pages 105-109.
[48] ibid
[49] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, Paper 534, 1–14. page 7.
[50] Jef Ausloos, Michael Veale and Rene Mahieu, Getting Data Subject Right Right, A submission to the European data Protection Board from international data rights academics, to inform regulatory guidance, para 100. ; ef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4
[51]Ariel Bogle, "The internet thinks you're a robot, and other "dark patterns" people with disabilities face online", ABC Science, 13 July 2019, available on https://www.abc.net.au/news/science/2019-07-13/dark-patterns-online-captcha-accessibility-disability-community/11301054, accessed on 27.02.2022.

An empirical study found that organizations gave full access to personal data to a person impersonating a data subject.[52] In a different 8.9% of data controllers disclosed personal data to users - regardless of the identity of the requester.[53] This suggests that SAR vulnerabilities and exploits are a problem. This may be the case because of a lack of proper authentication, for example because an unauthenticated user is allowed to access and change or request a change of a person's personal data (impersonating the targeted user).[54] **(Jasper Hille**)

> 61. Art. 12(2) states that the controller shall **not refuse to act on the request** of the data subject to exercise his or her rights, unless the controller demonstrates that it is not in a position to identify the data subject. In such circumstances, the data subject may, however, provide additional information enabling this identification (Art. 11(2)). (…)

The provision of article 11(2) GDPR should not be taken as an opportunity for the data controller to minimize its duties[55]. A non-exhaustive list of the types of information that data controllers could ask for would be welcomed, keeping in mind the proportionality assessment mentioned in paragraph 69. It should be stressed that additional information can only be required from the data subject when a *reasonable doubt* about his or her identity occurs, such as was ruled by the Berlin Administrative Court.[56] **(Solene).**

> 62. If the controller **has reasonable doubts** concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject (Art. 12(6)).

The Guideline should emphasize also that in case of reasonable doubts, data **controllers should also explain the nature of their doubts to the data subject,** the reasons of why they came to the conclusion that they need further information and describe how the additional information helps them in the verification process, especially if the data controller asks an official ID. This could strengthen the transparency of the processing, the data controller's accountability, and the data subjects' trust in data controllers. This question should be handled in the Guideline, because as the research of Urban et al. showed, when they sent SARs to different data controllers, none of the data controllers asking further information for verification touched upon these questions.[57] (**Patrik Kovács**)

> 63. (…) insofar as a digital communication channel already exists between the data subject and the controller and without prejudice to Art. 12(6) GDPR. The controllers must implement or re-use an authentication procedure in order to ascertain the identity of the data subjects requesting their personal data or exercising the rights granted by the GDPR 25

The Guidelines could provide examples of recommended methods. For instance, Di Martino et al. [58] determined the following list of recommended authentication methods:

1. Asking the data subject to confirm their request by sending an email from their registered email address the data controller already knows;
2. Call the data subject to verify their identity, if the data controller already knows a verified phone number of the data subject;

---

[52] M. Di Martino, P. Robyns, W. Weyts, P. Quax, W. Lamotte, and K. Andries, "Personal information leakage by abusing the {GDPR} 'right of access'," in Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019

[53] L. Bufalieri, M. L. Morgia, A. Mei and J. Stefa, "GDPR: When the Right to Access Personal Data Becomes a Threat," *2020 IEEE International Conference on Web Services (ICWS)*, 2020, p. 76, doi: 10.1109/ICWS49710.2020.00017.

[54] Boniface C., Fouad I., Bielova N., Lauradoux C., Santos C. (2019) Security Analysis of Subject Access Request Procedures. In: Naldi M., Italiano G., Rannenberg K., Medina M., Bourka A. (eds) Privacy Technologies and Policy. APF 2019. Lecture Notes in Computer Science, vol 11498. Springer, Cham. https://doi-org.proxy.library.uu.nl/10.1007/978-3-030-21752-5_12.

[55] WP29. (2017). *Opinion 3/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems.* WP29. European Commission on Data Protection

[56] VG Berlin. (2020). 1 K 90.19, ECLI:DE:VGBE:2020:0831.VG1K90.19.00

[57] Urban, T., Tatang, D., Degeling, M., Holz, T. and Pohlmann, N. (2019). A Study on Subject Data Access in Online Advertising After the GDPR. In C., Pérez-Solá, G., Navarro-Arribas, A. Biryukov and J. Garcia-Alfaro (Ed.). *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (1st ed., pp. 61-80). Springer

[58] Di Martino, M., Robyns, P., Weyts, W., Quax, P., Lamotte, W.L., Andries, K. (2019). Personal information leakage by abusing the GDPR "right of access". In Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019. USENIX Association (2019)

3. Request specific user data.

If small and medium enterprises have reasonable doubts concerning the data subject's identity, they should ask in the first line to confirm their request through their registered email address. If the data subject already used their registered address and the data controller still has reasonable doubts or does not have any registered email address of the data subject, then it could go to the third method and call the data subject.

However, if the data controller does not have any verified phone number of the data subject or still has doubts about the identity, it should ask the data subject for specific user data. This or a similar list of possible methods could strengthen the transparency of the SAR process and the accountability of the data controllers. Furthermore, small and medium-scale data processors could have some useful best practices at hand. (**Patrik Kovács**)

> 64. The controller should act upon the requests of data subjects for exercising their individual rights, unless it can demonstrate – through a justification in line with the principles of accountability (Art. 5(2)) - **that it is not in a position to identify the data subject (**Art. 11). The controller is not obligated to acquire additional information in order to identify the data subject for the sole purpose of complying with the request. However, it should not refuse to take such additional information.

It remains unclear how the data controller should respond to a request of access when it identifies a data subject but determines or has knowledge that the **data subject went missing**. When the person is declared missing, two outcomes are possible: finding the person or declaring the missing person dead due to a certain time limit. Furthermore, declaring a missing person dead may differ from country to country[59] in relation to the event that preceded the disappearance (e.g. fire or explosion), the circumstances surrounding the disappearance (e.g., war situation) and other factors such as age, illness and time elapsed since the disappearances.[60] These circumstances could confuse data controllers in relation to an appropriate response to data subject, install safeguard, and privacy measures. Thus, the Guidelines should provide additional information regarding data controllers' obligation when receiving requests of data subject that went missing or state that GDPR does not apply to the missing people's personal data but emphasizes the importance.[61] **(Marina Mijuskovic)**

> 65. In cases where the controller requests the provision of additional information necessary to confirm the identity of the data subject, the controller shall each time assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate (…)

Websites that implement a form to perform the request for access do not require further identification if the form is reachable only by a ***signed-in user*.** Other websites require to re-authenticate the data subject to finalize the request.[62] Perhaps the Guidelines can consider **defining 'additional information'** for purposes of information required for verification of the identification of data subjects to include the following (or a combination thereof):

(3) phone call
(4) questions about user personal data such as date of birth, username or address
(5) cookie ID
(6) address of email sender, and
(7) questions about the data that can be retrieved only from inside the account.[63] **(Roberto de Alcantara 7)**

I consider that more concrete explanations should be provided by the Guidelines regarding **what "*excessive demands*" corresponds to**. Particularly, to avoid any type of excessive demands, it would be useful if a list of unaccepted practices

---

[59] Presumption of Death Act 2013, 2013. https://www.legislation.gov.uk/ukpga/2013/13/contents/enacted,, accessed on 23.02.2022 ; Law on Declaring Missing Persons Dead and Proving Death NN 10/74, available on https://www.zakon.hr/z/380/Zakon-o-progla%C5%A1enju-nestalih-osoba-umrlima-i-dokazivanju-smrti , accessed on 22.02.2022

[60] Law on Declaring Missing Persons Dead and Proving Death NN 10/74, available on https://www.zakon.hr/z/380/Zakon-o-progla%C5%A1enju-nestalih-osoba-umrlima-i-dokazivanju-smrti , accessed on 22.02.2022.

[61] International Commssion on Missing Persons, Information Sheet On Personal Data Processing And Protection Reference: ICMP Policy on Personal Data Processing and Protection (ICMP.POL.DG.04.doc), available on https://www.icmp.int/wp-content/uploads/2017/11/icmp-dg-1356-6-W-doc-information-sheet-on-personal-data-processing-and-protection.pdf , accessed on 26.02.2022.

[62] H Luca Bufalieri, Massimo La Morgia, Alessandro Mei, Julinda Stefa, 'GDPR: When the Right to Access to Personal Data Becomes a Threat" (2020)

[63] ibid

were contained in the Guidelines. Specific reference shall be made on the organizations that compel the data subjects to prove their identity in person.[64] Therefore, the existence of **a figurative list** would offer some more clarity to the data controllers and make their job easier. (**Eleni Arampatzi**)

66. As a consequence, where information collected online is linked to pseudonyms or other unique identifiers, the controller can implement appropriate procedures enabling the requesting person to make a data access request and receive the data relating to them.

Although a lot of websites consider IP addresses as personal data in their privacy policies, it is not possible to access any data related to the IP addresses due the current network topology and the way IP addresses are allocated[65]. Therefore, internet users cannot prove that they have used an IP address and it´s easy for websites to deny IP-based subject access request in the terms of Art. 15 of the GDPR. The exercise of this right related with IP-address is extremely important to achieve transparency for internet users and to understand the extent of their online tracking[66]. (**Quezia Amaral Sayão**)

A data subject who is making a SAR via email and does not have an account with a login and a password on the controller's website, might provide an IP address as a way to prove his or her identity. Although a person can be identified by reference to an online identifier such as an IP address, in practice, IP-based SARs are often denied[67] due to the privacy risk of granting access to information logged against a 'non-obvious' identifier.[68] Namely, an IP address may be linked to multiple individuals or not linked to anyone.[69] Nevertheless, as data subjects without accounts also have the right of access[70] the issue of denying access in the case of IP-based SARs should be addressed in the Guidelines. For instance, the Guidelines could advocate for controllers using IPv6 instead of IPv4, since IPv6 allows for allocating a single user per IP address and which has also been endorsed by the European Commission as a suitable measure for facilitating identification.[71] Namely, due to the exhaustion of the limited number of IPv4 addresses, controllers use CGN technologies to share a single IP address among multiple users.[72] Conversely, there are around 340 **undecillion IPv6 addresses available** '*capable of acting as an identifier for each connected device on the planet*.'[73] Although this would not ensure that an IP address identified a data subject in every case since she could be using PETs,[74] it would reduce the likelihood of an IP address linked to multiple individuals. (**Eva Opsenica)**

Some SMS scams use the ***2FA system*** as a pretext to get access to a verification code sent to the data subjects' phone number in order to get access to their accounts. This type of scam goes by the name of **SMishing** and was included in Europol's Internet Organised Crime Assessment.[75] In such a scam, the victim would receive an SMS coming from the

[64] Thomas van Biemen (2018) "Personal Privacy in Practice: Putting the GDPR to test in a collective exercise of data subjects' right of access", Technical University of Delft, pp. 52-53.
[65] Supriya Adhatarao, Cédric Lauradoux, Cristiana Santos (2021) "Why IP-based Subject Access Requests Are Denied?"
[66] ibid
[67] Adhatarao, S., Lauradoux, C., & Santos, C. (2021, May 27). Why IP-based Subject Access requests are denied? *arXiv:2103.01019v2*. 9. https://doi.org/10.48550/arXiv.2103.01019
[68] Cormack A. (2016). Is the Subject Access Right Now Too Great a Threat to Privacy? *European Data Protection Law Review, 2(1)*, 15-27, 18. https://doi.org/10.21552/edpl/2016/1/5
[69] ibid
[70] Adhatarao, S., Lauradoux, C., & Santos, C. (2021, May 27). Why IP-based Subject Access requests are denied? *arXiv:2103.01019v2*. 2. https://doi.org/10.48550/arXiv.2103.01019
[71] European Commission, Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final of 13 September 2017, 3.1.
[72] Gözükara, F. (2021). Challenges and possible severe legal consequences of application users identification from CGN-Logs. *Forensic Science International: Investigation, 39, 301312*, 1-18, 1. https://doi.org/10.1016/j.fsidi.2021.301312; Europol. (2017, 17 October). *Are you sharing the same IP address as a criminal? Law enforcement call for the end of Carrier Grade NAT (CGN) to increase accountability online* [Press release]. https://www.europol.europa.eu/media-press/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online
[73] LeadBoxer ('Anna'). (2021, 9 May). What is IPv6 and Why Does it Matter? *leadboxer*. https://www.leadboxer.com/blog/what-is-ipv6-and-why-does-it-matter/
[74] Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., & Santos, C. (2019). Security analysis of subject access request procedures. *Annual Privacy Forum*, 1-20, 14. https://hal.inria.fr/hal-02072302
[75] EUROPOL. (2020). Internet Organised Crime Threat Assessment. European Union Agency for Law Enforcement Cooperation. 1-64, p. 45. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

same number as the one of the official organization. Therefore, it should be considered whether an authentication code is a secure way to verify the data subject's identity considering the possibility for fraud and account theft. Considering that serious consequences may follow for data subjects and data controllers, the EDPB should consider at least warning controllers about the eventuality of phishing scams in this example or adopting an entirely different example. (**Joanna Taneva)**

The double verification system has its flaws as it can be bypassed. Indeed, as an empirical study found, "… *even if such policy is adhered to – an adversary that has access to the mailbox of the subject, might still be able to bypass any* ***two-factor authentication*** *(which is potentially required when attempting to log in to the service by normal means)* ..."[76] (**Magdalena Rangelova**)

"**Adaptive authentication**" operates by creating a user profile, including information such as the user's geographical location, devices registered etc. Every request for authentication is evaluated basing on previous behaviour and the context, subsequently being assigned a risk score. Depending on that score, the user may be required to provide more or less credentials. An example of such situation is if the user tries authentication via an unregistered device or via an unknown geographical location, they may be prompted to answer an additional security question.[77] (**Urszula Baranowska)**

3.1. Proportionality assessment regarding identification of the requesting person

69. As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable identification of the requesting person. Therefore, the controller shall carry out a **proportionality assessment** (…)

Obliging data controllers to do a proportionality assessment, without any guidance regarding what would be proportionate in general, can be a burden on the data controller. It has been called likely that this attracts resistance from many controllers.[78] Article 15 GDPR does not include this proportionality test, and thus introducing this potential burden in the guidance can be controversial. (**Tomas Bagçe**)

Recently, the Dutch DPA fined a data controller for excessively asking for ID cards as proof of identification for access requests[79]. Controllers struggle with identification methods and the proportionality testsIt would be advisable to share best practices as part of the guideline or a reference can be made to such practices in the guideline for companies to learn from and enable them to comply easier. (**Elena Sheikhbahaei**)

The Guideline do not specify whether a higher due diligence needs to be observed when **sensitive personal data** is being shared. Perhaps it is good to introduce a special mechanism of disclosing sensitive data in such a way that the risk of it being shared with unauthorized persons is minimized. Indeed, As suggested by Martino et al. "the DC should avoid leaking personal data to unauthorized adversaries, it can respond to a DS by requesting the subject to verify their identity and thus ensure that the sensitive data is delivered to the right person".[80] (**Magdalena Rangelova**)

70. The controller should implement an authentication (verification of the data subject's identity) procedure in order to be certain of the identity of the persons requesting access to their data28 ,and ensure security of the processing throughout the process of handling an access requests in accordance with Art. 32, including for instance a secure channel for the data subjects to provide additional information. (…)

---

[76] Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax and Others. (2019). Personal Information Leakage by Abusing the GDPR "Right of Access". *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*.

[77] *What is adaptive authentication? Adaptive authentication and authorization improve cybersecurity.* One login by One Identity available at https://www.onelogin.com/learn/what-why-adaptive-authentication

[78] Feldman, R. J., Hickman, T., Lamm, J., Luo, H., & Sloane, C. T. (2022, February 16). EDPB issues guidelines on right of access under Art. 15 GDPR [Press release]. https://www.whitecase.com/publications/alert/edpb-issues-guidelines-right-access-under-art-15-gdpr

[79] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-boete-dpg-media-voor-onnodig-opvragen-identiteitsbewijs#subtopic-4542

[80] Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax And Others. (2019). Personal Information Leakage by Abusing the GDPR "Right of Access". *Proceedings of the Fifteenth Symposium on Usable Privacy and Security.*

This paragraph is intrinsically linked to the Revised Directive on Payment Services which discusses the idea of multi-factor authentication. What this document must immediately do is refer to the directive for the purposes of clarity and directness for all parties involved including the controller. (**Arystan Jazin**)

(1) The current guidelines do refer to authentication as means of verification of the data subject's identity, which, indeed, bears a lot of similarities to the Strong Customer Authentication process as described under the PSD2. Thus, I would like to bring to the EDPB's attention the potential overlap between the PSD2 and the GDPR. (**Magdalena Rangelova**)

> 72. In practice, authentication procedures often exist and controllers do not need to introduce additional safeguards to prevent unauthorised access to services. In order to enable individuals to access the data contained in their accounts (such as an e-mail account, an account on social networks or online shops), controllers are most likely to request the logging through the login and password of the user to authenticate, which in such cases should be sufficient to identify a data subject. Consequently, it is disproportionate to require a copy of an identity document in the event where the data subject making their requests are already authenticated by the controller.

After having myself exercised my right of access, I was stunned by the amount of information that was provided to me. Of due concern were **the logs of all my IP addresses** which, combined with the logs that showed my name and last name, made it very easy to identify ***and locate me*****.** Since cybercrime has risen exponentially during the pandemic,[81] it worries me that granting access to such personal data simply by knowing the email/username and password of someone is, in fact, a possibility. Therefore, it is in my opinion that the EDPB consider inserting as a best practice for data controllers to include an option (preferably upon creating an account), that allows the exercise of SAR only after providing concrete proof that allows the identification of the account owner.
The same applies on the **use of email to send data is opportune**, seeing as a staggering 23.6 million email accounts that fell victim to unauthorized access used "123456" as a password, with the victims also using the same password elsewhere, meaning that breaches in other websites put their email at risk, entailing that requesting access via the email connected to the account without further verification is a potential security risk.[82] (**Antonio Cannavacciuolo)**

The French Data Protection Agency CNIL recommends asking for a copy of the ID card only in the presence of reasonable doubt.[83] **[Solène Tobler]**

> 76. To follow the principle of data minimisation the controller should inform the data subject about the information that is not needed and about the possibility to blacken or hide those parts of the ID document. (…)

Blackening or blurring the unnecessary information in the case of ID cards and other official documents is a possible solution to protect the data subject from the threat of impersonation and leakage, but this practice does not protect the data subject's visible data from *impersonation*. A possible solution might be the practice provided by Boniface et al.: they proposed that the data subject could add watermarks to the document, which should contain two elements: (i) a validity period to prevent anyone from impersonating the data subject to the same data controller in the future and (ii) the name of the data controller to prevent anyone to use the copy with any other data controller. This procedure could satisfy the non-transferability property as well.[84] **(Patrik Kovács)**

This statement may present some problems which the EDPB needs to address: (1) the guidelines does not stipulate how it proposes to advise the data subject about the 'blackening' process; (2) what guarantees are there that the controller, when handed an ID document, is not going to capture and utilize the additional personal information submitted; and (3) the provision does not inspire confidence by providing a sanction should the controller use the information/data. **(Roberto de Alcantara**)

---

[81] EUROPOL. (2021). Internet Organised Crime Threat Assessment. Luxembourg: Publications Office of the European Union, pp. 8-9. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime
[82] Bufalieri, L. (2020). GDPR: When the Right to Access Personal Data Becomes a Threat. Rome, Italy, p.7 https://www.researchgate.net/publication/341175731_GDPR_When_the_Right_to_Access_Personal_Data_Becomes_a_Threat
[83] CNIL. (2020). Professionnels : comment répondre à une demande de droit d'accès ?, Commission nationale de l'informatique et des libertés, URL: https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces
[84] Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., Santos, C. (2019). Security analysis of subject access request procedures how to authenticate data subjects safely when they request for their data. In: M. Naldi, G.F. Italiano, K. Rannenberg, M. Medina, A. Bourka, (Ed.) *Privacy Technologies and Policy* (1st ed, pp. 182–209). Springer

78. Taking the above into account, where an ID is requested (and this is both in line with national law and justified and proportionate under the GDPR), the controller must implement **safeguards** to prevent unlawful processing of the ID. Notwithstanding any applicable national provisions regarding ID verification, this may include not making a copy or deletion of a copy of an ID immediately after the successful verification of the identity of the data subject.

In a study conducted in 2020,[85] the ID card of one of the authors was modified to appear as being clearly *tampered* with (i.e., false), with the first ID card being redacted (hiding the non-required information as per para.75) and, in case it wasn't accepted, then the non-redacted ID card would be used. Out of the 25 controllers to whom the ID card was sent to, 21 accepted the ID card, while 4 refused the redacted ID card, but only to then accept the non-redacted one; therefore, they were able to receive data each time while using the tampered document. The conclusion was that serious doubts arose about whether controllers possessed the correct technology and expertise to conduct an efficient assessment of the veracity of ID cards.[86] The EDPB may consider assessing which verification procedures of ID cards may be needed, not only to protect controllers from lawsuits, but especially to protect the personal data of data subjects. **(Antonio Cannavacciuolo**)

It might be helpful to suggest that the controller add the following additional information to the note[87] (1) what ID documents the data subject provided; (2) the date which the data subject verified the ID document; and (3) details of who at the controller company verified the ID document. (**Roberto de Alcantara)**

3.2. Requests via third party/proxies

79. 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**. This may apply to, among others, acting through a proxy or legal guardians on behalf of minors, as well as acting through other entities via online portals. (…)

In the case of **minors**, the request for the right to access by the guardian or parents would require further identification of the persons. (**Dina Kristina Denso**)

80. In doing so, national laws governing legal representation (e.g. powers of attorney), which may impose specific requirements for demonstrating authorization to make a request on behalf of the data subject, should be taken into account, since the GDPR does not regulate this issue. (…)

The EDPB interpretation then obliges the data controller to be able to assess whether the power of attorney fulfills those foreign laws. This is a huge burden, not only for small data controllers. It would be a good idea to revise this interpretation. (**Tomas Baçe**)

Whereas the third party who is requesting the data must provide evidence of their authority to make SAR.[88] However, it is unclear whether the following (example) scenario would be considered as a data breach and lead to sanctions under the GDPR, or whether it would be a breach of national law, or whether it can result in double jeopardy: if a third party makes a request for data on behalf of the data subject; that third party provides proof, which authorizes to act on behalf of the data subject; however, the proof is fabricated; the data controller does not realize and shares the information with an unauthorized person. (**Magdalena Rangelova**)

The EDPB does not make clear what 'appropriate' documentation is needed if the request is from a third country outside of Europe. The ICO Guidance Document on the GDPR provides for the acceptance of signed letters of authority as valid evidence of proof of authorization, which differs from a power of attorney which is a notarised document. The EDPB could provide a list of appropriate documentation, which could include a letter of authority (**Roberto de Alcantara**)

[85] Bufalieri, L. (2020). GDPR: When the Right to Access Personal Data Becomes a Threat. Rome, Italy: Department of Computer Science, Sapienza University of Rome, pp.7-8 https://www.researchgate.net/publication/341175731_GDPR_When_the_Right_to_Access_Personal_Data_Becomes_a_Threat
[86] ibid
[87] ICO Guidance on right of access
[88] ibid

The literature has considered the possibility to delegate the right of access to researchers, which will massively facilitate research in this field.[89] Considering that there are already derogations for data processing for research purposes (Art. 89 GDPR), it is not impossible to introduce a "delegated access"[90] for researchers in relation to Art.15 GDPR. However, it is worrying that the Guidelines merely refer to delegated access regarding legal representation and authorisation via power of attorney. It must be pointed out that representation is not limited to representation by a legal professional in all jurisdictions.[91] For example, Dutch property law allows non-legal representation regarding legal deeds.[92] Therefore, it is advisable that the EDPB changes this paragraph to refer to "representation" rather than "legal representation" and "written declaration" rather than "power of attorney". This is because studies have shown that data controllers are under the impression that requests made by third parties are unlawful, when in fact they are just not covered by the GDPR, but by national law.[93] This will ensure that data controllers in Member States, which allow non-legal representation, are not mislead that proxy requests are only possible via a legal representative. **(Joanna Taneva)**

> 81. While the exercise of the right of access to personal data of deceased persons amounts to another example of access by a third party other than the data subject, Recital 27 specifies that the GDPR does not apply to the personal data of deceased persons. (…)

Will the controller still need to comply with the data request under the terms of Art. 15 of the GDPR for its representatives and/or heirs? By the time of the data processing and the request, the GDRP and the obligations to comply with Article 15 were valid. This question remains unanswered by the Guidelines. It seems the answers is yes considering the relevance of the right of access which can (i) be considered as a *sine qua non* for meaningfully exercising other data subject rights, (ii) be used to monitor controllers' compliance and (ii) be used as a due process guarantee.[94] (**Quezia Amaral Sayão)**

While in countries like the Netherlands, there are no regulation[95] on this matter, other countries such as Portugal imposed obligations with respect to the processing of personal data of the deceased person, e.g., the request for access of the deceased person´s data only will be applicable for a limited period after the date of death[96]. Nevertheless, some platforms such as Facebook, which operates all over Europe, states in their "Terms of Service" that the access of the platform by a party representing a deceased person (and the consequent opportunity to request data based on Art. 15 of the GDPR) is not possible, only if the deceased person has had previously indicated a "legacy contact"[97]. A question remains unclear: is this conduct legitimate? Since there are different legal interpretations of what can be considered as "transferable property of data"[98] and there is an absence of general rules in this matter, guidance will be appropriate. **(Quezia Amaral Sayão)**

Missing persons are no accounted in this section. Personal data of missing person is often widely shared. Nevertheless, these personal data can be private, embarrassing or distressing for the missing person.[99] Therefore, the Guidelines should reflect on the personal data of the missing person and specify if the GDPR apply to the personal data of missing persons, as has been done in paragraph 81. regarding personal data of deceased persons.[100] **(Marina Mijuskovic)**

---

[89] ibid
[90] ibid
[91] Asghari, H., van Biemen, T., & Warnier, M. (2021). Amplifying Privacy: Scaling Up Transparency Research Through Delegated Access Requests. 5th Workshop on Technology and Consumer Protection (ConPro '21), 1–7, 3. https://www.ieee-security.org/TC/SPW2021/ConPro/papers/asghari-conpro21.pdf
[92] Ibid.
[93] Ibid.
[94] ibid
[95] Gabel D. and Hickman T. (2019, 13 November). *GDPR Guide to National Implementation – A practical guide to national GDPR compliance requirements across the EEA*. White & Case Technology Newsflash Retrieved February 28, 2022, from https://www.whitecase.com/publications/article/gdpr-guide-national-implementation#q2
[96] ibid
[97] Facebook (2022, 4 January). *Terms of Service.* Item 5 (5). Retrieved February 28, 2022, from https://www.facebook.com/terms.php
[98] Bacchi, U. R. (2019, 14 February). *Who owns your Facebook profile when you´re dead*? Mint. Retrieved February 28, 2022, from https://www.livemint.com/technology/tech-news/who-owns-your-facebook-profile-when-you-re-dead-1550116101037.html
[99] Guidance: Privacy and missing people, available on https://www.bbc.co.uk/editorialguidelines/guidance/missing-people/ , date of access 25.02.2022.
[100] International Commission on Missing Persons, Processing Data On Missing Refugees and Migrants, The Hague, 2016.

82. Children deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerning their rights in relation to the processing of personal data 34. Any information and communication to a child, where personal data of a child are processed, should be in such a clear and plain language that the child can easily understand

This seems a rather vague and illusory statement, especially taking into consideration that no additional guidance is provided in the matter. A child in most cases, legally (UNCRC, art 1) is an individual under the age of 18. However, the cognitive capabilities of, for example, a 17-year-old and a 13-year-old vary to a great extent. Therefore, it may be difficult to apply a unified standard of "plain language". Moreover, considering that simplifying privacy policies by controllers has not had much success, it is questionable whether controllers will be able to adapt them sufficiently for children's understanding.[101] (**Urszula Baranowska)**

It can be recommended that web design and architecture of websites be used to communicate effectively and clearly with children. The use of icons, pictures, videos, color schemes and other UX/UI design tools has been encouraged by the CNIL to attract the attention of young users towards the information communicated to them. The French DPA also recommends, particularly when dealing with children, to integrate the information into the user experience during the sign-in process, in order to encourage users to read the provided text or, even better, watch the provided video.[102] The architecture and design of the web page should also facilitate the exercise of their rights by children. In line with article 12 of the International Convention on the Rights of the Child establishing the right of every child to freely express their view, children should be given the tools to express themselves. Using this legal source, the CNIL recommends the creation of processes allowing children to have autonomy when dealing with their data online.[103] [**Solène Tobler]**

It is not clarified what information should be provided to the children regarding their personal data. The data controller must provide children with the same information about how he/she uses their personal data, as he/she would provide to adults. The processing will be fair if there is the same need for transparency, as this gives an individual control and choice[104]. **(Evangelia Cheiladaki)**

Any privacy notice directing to children shall be clear. However, it is easily understandable that the target children' audience is diverse in age. This means that the data controller shall provide several versions of the notification for different ages. If the data controller decides to only have one version of the privacy notice, he/she must make sure that it is accessible to all different ages and understandable to everyone, even to the youngest audience[105]. **(Evangelia Cheiladaki)**

Guidelines in section 3.4.1. distinguish children as a vulnerable category in relation to which they need to be approached with more caution regarding their data. In accordance with Strategy for the Rights of Persons with Disabilities[106] another category should be included in Guidelines, for example, people with disabilities.[107]These people face complications in using general functions on the internet where study concerning searching, navigation, understanding information on the internet has shown that 38% of the participants found functions difficult.[108] In

[101] Buitelaar J.C. (2018) Child's Best Interest and Informational Self-Determination: What the GDPR can learn from Children's Rights *International Data Privacy Law 8(4)*

[102] CNIL. (2021). *Recommandation 6: Renforcer l'Information et les Droits des Mineurs par le Design. Cnil.fr. URL: https://www.cnil.fr/fr/recommandation-6-renforcer-linformation-et-les-droits-des-mineurs-par-le-design*

[103] CNIL. (2021). *Recommandation 2: Encourager les Mineurs à Exercer Leurs Droits*. Cnil.fr. URL: https://www.cnil.fr/fr/recommandation-2-encourager-les-mineurs-exercer-leurs-droits

[104] Information Commission's Office. (2020, 21 October). Right of access. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/?template=pdf&patch=19#link8 Accessed 28 February 2022

[105] ibid

[106] European Commission, Union of Equality, "Strategy for the Rights of Persons with Disabilities 2021-2030"

[107] Eurpoean Parlament, European disability policy, „From defining disability to adopting a strategy 2010-2020", page 3 and 18.

[108] Johansson, S., Gulliksen, J. & Gustavsson, C. Disability digital divide: the use of the internet, smartphones, computers and tablets among people with disabilities in Sweden. *Univ Access Inf Soc* **20,** 105–120 (2021).

addition, many websites do not have a design that facilitates or allows access for disabled people.[109] Among other recognized difficulties[110] digital society poses more challenges[111]and affects awareness of the risk, consequences in relation to their personal data, Therefore Guidelines should provide additional information regarding people with disabilities and their right of access. **(Marina Mijuskovic)**

83. Children are data subjects in their own right and, as such, the right of access belongs to the child. Depending on the maturity and capacity of the child, acting on behalf of the child by the holder of the parental responsibility could be needed.

The EDPB could provide an age that could serve as a starting point where competency is presumed. The ICO Guidelines mention for example that the age of 12 could be a good starting point.[112] It will also be helpful if it is clarified if data controllers should treat children the same when there are special categories of personal data at stake or if the age of competency may change according to nature of the personal data. **(Stamatia Beligianni**)

There is concern on how the EBPD intends to address the issue of data format and its complexity when applied to children, bearing in mind the obligation on data controllers to provide conditions necessary to render the complex data intelligible. One such possible solution to address data complexity is to adopt the layered approach advocated by the A29WP.[113] The EDPB is urged to explore ways to simplify the request process for children and to prescribe a 'simplified' format of the data (if possible), easy to understand for children, to be used. **(Roberto de Alcantara)**

Further information on the matter is not provided in the guidance, for example who will oversee whether a child is mature enough to exercise their own rights. If such evaluation were to be granted solely to the parents, it could potentially be a gateway to the parents violating children's best interest and their privacy. (**Urszula Baranowska)**

This paragraph could further explain the standard of maturity and capacity. The standard should be not only restricted in nature age, but also needs to consider about children's growth background, language skills or other factors. The data controller should consider transferring the data to the child's agent only if, after these considerations, the controller has reasonable grounds to believe that the child cannot understand the data and cannot make the best judgment about his or her own interests. **(Shuoyuan Jiang)**

This paragraph could lead to different range of age due to the different national laws where the medium is based on from the national laws where the children are nationals. There should be a consensus on the choice of law regulating the matter of children and their rights to access in order to avoid confusion. (**Dina Kristina Denso)**

84. The best interests of the child should be the leading consideration in all decisions taken with respect to the exercise of the right of access in the context of children, in particular where the right of access is exercised on behalf of the child, for example by the holder of parental authority.

Not clear who will be in charge of evaluating what the child's best interest is. The ICO guidance on the matter states that in most cases, access is granted to the parent. This relies to a great extent on the controller's subjective opinion, with limited information on what the intentions of a parent are, and whether they are contrary to best interests of the child. Examples of situations in which it is evidently not in child's best interest could be helpful. (**Urszula Baranowska**)

---

[109] Sarah Katz, „The Inaccessible Internet – As life moves online, gaps in digital accessibility mean milions of disabled American are being left behind.", FutureTense, availiable on https://slate.com/technology/2020/05/disabled-digital-accessibility-pandemic.html , accessed 23.02.2022.

[110] Eurostat, Statistics Explained, Disability statics backgorund – European health and social integrating survey, November 2015., availiable on https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Disability_statistics_background_-_European_health_and_social_integration_survey , accessed on 23.02.2022.

[111] Elisabeth Ward, „Understanding disability in a digital society", TechShare Pro 2020, available on https://bighack.org/accessibility-understanding-disability-in-a-digital-society/ , accesed on 23.02.2020.

[112] Information Commission's Office. (2020, 21 October). Right of access. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/

[113] Jef Ausloos, Michael Veale and Rene Mahieu, 'Getting Data Subject Rights Right' (2019) 20

85. Due to the special protection of children's personal data contained in the GDPR, the controller shall take appropriate measures to avoid any disclosure of personal data of a minor to an unauthorised person

Some examples are needed: a) the data controller could ask for the child's ID (if the request is from the child), b) the data controller could ask for parents'/guardians' ID (if the parent or guardian exercise the child's rights on their behalf if the child authorizes this)[114], c) further ID's verification by sending a passcode in child's/parents'/guardians' phone. (**Evangelia Cheiladaki**)

The EDPB should clarify what happens in controversial cases, like the one that one parent has custody of the child, and the other parent does not, but they share the parental responsibility. It should be clear if a parent without custody of the child can be considered an authorised person or not. This situation may lead to confusion for data controllers that will not know whether they must provide access to the requested data or not. An example like this could be added, it would be helpful, and it would clarify that if both parents share the parental responsibility, they are both entitled to make a subject access request on behalf of the child.[115] The parent with custody does not outweigh the parent that does not have custody in relation to the right of access of the child, unless there are specific circumstances that would excuse a differentiated treatment, like for example a court order that prohibits the communication of one parent with the child.[116] (**Stamatia Beligianni**)

88. 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 unauthorised parties.

The issue mentioned in this paragraph is made in the context of third party portals or channels used to exercise the right of access. The guidance does not, in any way, propose ways to improve this. It would be helpful if there was some kind of harmonised way for third party portals and channels to proof their power of attorney is legitimate. The current EU proposal for a European Digital Identity aims to allow people to identify themselves online, and allows people to sign eSignatures to sign legal documents. If implemented correctly, this could potentially serve as a solution as third parties would be able to use the eSignature signed by the data subject to proof they are acting legitimately. If the guidance could implement this in the text, or another system, this would lead to more harmonization in delegated requests. **(Tomas Baçe)**

Paragraph 66 and the WP29 Guidelines on the right to data portability deal with the problem of data subjects and online pseudonyms,[117] but this paragraph offers no solution for the situation in which a data controller has no means to directly contact the data subject for which the third party is exercising the subject access rights request. Does this mean such situation resolves in the same way a situation in which the data controller is unable to identify the data subject resolves? (**Jasper Hille**)

4. SCOPE OF THE RIGHT OF ACCESS

95. In Nowak, the CJEU made a broader analysis and found that written answers submitted by a candidate at a professional examination and any comments of an examiner with respect to those answers constitute personal data concerning the exam candidate. (…)

The Guidelines should also distinguish IP addresses as a specific category of personal data. Namely, the classification of IP addresses into static and dynamic affects its definition as personal data.[118] Due to specificity, the concern arises

[114] Information Commission's Office. (2020, 21 October). Right of access. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/ Accessed 28 February 2022
[115] Hellenic Data Protection Authority. (2020, March 24) *HDPA-4/2020.* GDPRhub. https://gdprhub.eu/index.php?title=HDPA_-_4/2020
[116] Ibidem.
[117] WP29 Guidelines on the right to data portability, p.13-14.
[118] Alessandro El Khoury, "Personal Data, Algorithms and Profiling in the EU: Overcoming the Binary Notion of Personal Data through Quantum Mechanics", Erasmus Law Review, 3, (2018):165-177,

when the data controller has to respond to IP-based Subject Access Request.[119]Conducted studies have shown that stable and unique IP addresses can be assigned to the data subject[120] and that IP addresses can be tracked regarding accountless users but also that it is not possible to access any data related to the IP addresses used while visiting their websites as an accountless user due to identification issues.[121] **(Marina Mijuskovic)**

It is unclear whether SAR should be executed in the following (example) situation: a bank is suspicious of the activities of a data subject (*natural person who has a business but acts in his name*) and is performing an ongoing investigation to determine whether that individual is laundering money or committing fraud; meanwhile, data subject makes a request to access his files including and all possible credit and risk assessments (subjective information in the form of assessment).[122] This comment relates to both paragraph 95 and paragraph 96 of these Guidelines. (**Magdalena Rangelova**)

Example: An individual has a job interview with a company. In this context, the job applicant hands over a CV and an application letter. (…)

It would be interesting for these Guidelines to explain how data access requests should be handled in case the individual that has done a job interview and requests a SAR is still in the hiring process. In this case, where the subject requests a SAR while the hiring process is ongoing, the information collected from the interviews, as well as any scorecard created on the basis of that individual, should be considered as personal information.[123] As such, it should be shared with the data subject based on Article 15 GDPR. However, complying with GDPR provisions in the specific situation could violate principles of equal treatment and non-discrimination.[124] The individual that has specific information on the process of recruitment would be in a privileged position with respect to other candidates and generate a non-equal treatment for candidates. The collision of two different rights would leave controllers in a very difficult situation. (**Isabel Sierra Rubio 3**)

96. Thus, subject to the specific facts of the case, when assessing a specific request for access, the following types of data are, *inter alia*, to be provided by controllers without prejudice to Art. 15(4) GDPR (…)

Merely listing data that was not knowingly provided by the data subject may not enable him or her to do so. For instance, a credit score alone does not tell the data subject how it was calculated, thus, he or she cannot assess its correctness. This is worrisome given how credit bureaus face challenges in ensuring that the personal data they process are accurate.[125] For example, in 2021 the Irish Credit Bureau DAC was fined for a data breach that resulted in recording an incorrect payment history of 15,120 data subjects.[126] Considering this, the Guidelines should state that controllers need to indicate how data was reached in order to enable data subjects to assess its correctness. For instance, a controller could list the data that affected a credit score. In the context of personalisation, which is also mentioned under the category of inferred data, a controller could indicate the link between a data subject's transaction history (e.g., diet pills, books on dieting, etc.) and personalisation (e.g., personalised offers of dietary products). **(Eva Opsenica)**

The German Federal Supreme Court[127] made clear that the scope of the right to access is to include, inter alia, (1) a request for 'all data' is a sufficiently precise request and the access may not be limited to data which is not yet known to the data subject and (2) the right of access is satisfied when the information provided represents the total scope owed according to the stated intent of the data subject and an inaccuracy in the information provided that not result in the right not being satisfied. Rather, it has been suggested that the decisive factor being a declaration from the data subject

[119] Coline Boniface et al. Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data. APF 2019 - Annual Privacy Forum, Jun 2019, Rome, Italy. pp.1-20. ffhal-02072302f
[120] Vikas Mishra et al. Don't count me out: On the relevance of IP address in the tracking ecosystem. In WWW '20: The Web Conference 2020, pages 808–815. ACM / IW3C2, April 2020.
[121] Supriya Adhatarao, Cédric Lauradoux, Cristiana Santos, "Why IP-based Subject Access Requests Are Denied?", available on https://arxiv.org/abs/2103.01019 , accessed on 25.02.2022.
[122] Judgement of 20 December 2017, *Nowak*, Case C-434/16, EU:C:2017:994, para. 34.
[123] Ibidem, para 4
[124] Article 21 European Charter of Fundamental Rights
[125] Data Protection Commission Decision from 23 March 2021 in the matter of Irish Credit Bureau DAC, IN-19-7-2, para. 6.4. https://www.dataprotection.ie/sites/default/files/uploads/2021-05/Redacted_23.03.2021_Decision_IN-19-7-2.pdf
[126] Ibidem
[127] BGH, Urteil vom 15.06.2021 - VI ZR 576/19

that the information is complete, (5) if the information provided is noticeably insufficient to cover the subject, the data subject may request additional information.
The Higher Administrative Court of Munster[128] favors a broad interpretation of the right of access under which controllers are required to provide information relating to all existing personal data.
Limiting the request to information specified in Art. 15(1)(a-h) GDPR (the narrow interpretation) is insufficient. However, the German Federal[129] have identified situations in which the limitation of the right of access can serve to prevent abuse by data subjects. As a solution the EDPB could align this paragraph (96) with the view of the German Federal Supreme Court, and to rephrase the paragraph to read that, 'subject to the specific facts of the case, when assessing a specific request for access, all data relating to the data subject is to be provided by controllers without prejudice to Art. 15(4) GDPR.' (**Roberto de Alcantara)**

103. The classification of data as personal data concerning the data subject does however not depend upon the fact that those personal data also relate to someone else. It is thus possible that personal data relate to more than one individual at the same time. This does not automatically mean that access to personal data also relating to someone else should be granted, as the controller needs to comply with Art. 15(4) GDPR. **171.** With regard to Recital 4 GDPR and the rationale behind Art. 52(1) of the European Charter of Fundamental Rights, the right to protection of personal data is not an absolute right. (…)

In the context of establishing whether disclosure of personal data relating to multiple individuals would adversely affect the rights and freedoms of those individuals, the Guidelines should encourage controllers to seek consent from them to release data[130] before concluding if/to what extent access should be granted to the data subject making the SAR. Obtaining consent could grant the data subject (complete) access to information when applying Article 15(4) of the GDPR would otherwise lead to redaction/denial, thereby promoting his or her right of access. Nevertheless, this might not always be a feasible solution. It is unclear how the controller could contact individuals whose voice was (accidentally) processed by a virtual voice assistant. Namely, although the main user of the VVA will have an account and/or email,[131] individuals whose voice will be (accidentally) processed will not. (**Eva Opsenica**)

Whether or not the data controller opts to reveal information on a third party, he/she must answer to the requester and justify his/her decision to reveal or withhold information about a third party[132]. **(Evangelia Cheiladaki)**

In Referral C-579/21 (Pankki S), which is pending, a related question to this paragraph was raised. Could the information collected by the data controller concerning the person who processed the data subject's personal data and the time be considered as "personal data" on which the data subject has a right of access? The Guidelines could possibly give some clearer directions on how "concerning him or her" should be interpreted. Paragraph 104 states that the interpretation in question should not take place in an "*overly restrictive*" way, however, it remains unclear whether these categories of data could fall under the scope of Article 4(1) or the fact that they are related to the data of controller's employees excludes them from being considered as "personal data". (**Eleni Arampatzi**)

104. … the controller should inform the data subject about the fact that they may become controller in such case

It would be best to also add as a best practice the duty to clearly explain to the data subject also the obligations that would derive from becoming a controller. Although most of the general public, in the EU, is aware of the existence of the GDPR,[133] the same can't be said for whether they are aware of their rights.[134] Therefore, it can be inferred that the

[128] Case No. 16 A 1582/20)
[129] Bundesarbeitsgericht: 2 AZR 342/20 vom 27.04.2021
[130] Ausloos J., Veale M., & Mahieu R. (2019). Getting Data Subjects Rights Right. *JIPITEC*, 10(3), 283-309, 292. https://doi.org/10.31228/osf.io/e2thg
[131] European Data Protection Board. (2021). *Guidelines 02/2021 on virtual voice assistants (version 2.0)*, p. 3. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en
[132]Information Commission's Office. (2020, 21 October). Right of access. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/
[133] Johnson, J. (2019). Share of individuals in Europe aware of the General Data Protection Regulation (GDPR) as of October 2019, by country. Statista. https://www.statista.com/statistics/1175252/awareness-of-gdpr-by-country-europe/
[134] While specific research on the issue isn't widely available, small initiatives do exist. *See* Wolford, B. (2019). Do consumers know their GDPR data privacy rights? GDPR.EU. https://gdpr.eu/consumers-gdpr-data-privacy-rights/

average person can't be considered to possess such knowledge on the obligations of data controllers. (**Antonio Cannavacciuolo**)

Guidelines for data subjects should also be developed to highlight examples of when a data subject becomes a controller, providing the data subject with the necessary information regarding the responsibility and liability it may have as a data controller, as argued in an article by Finck.[135]A data subject is not aware of the obligations referred in Article 26. **(Thalis Cabral**)

Whilst the Court of Justice has undertaken a combination of a narrow interpretation of the household exemption with flexibility regarding the obligations for individuals as data controllers, simplified guidance should be provided to such data subject on the basic obligations, taking into account the lack of complex knowledge on the specificities of the GDPR and related laws.[136] (**Urszula Baranowska)**

> 105. Then again, there are situations in which the link between the data and several individuals may seem blurred to the controller, such as in the case of identity theft. In case of identity theft, a person fraudulently acts in the name of another person. (…)

The EDPB could clarify under what circumstances granting access to this kind of data may affect the (privacy) rights and freedoms of the perpetrator to such extend that it would be incompatible with art. 15(4) GDPR to grant access. (T**omas Baçe**)

The guidelines should also explain the meaning of the accuracy principle of art. 5(1)(d) GDPR in such cases. A controller is expected to keep the personal data of data subjects accurate, but when the personal data relating to a data subject becomes entangled with another person's because of impersonation, it may be unclear how to resolve the situation. One could argue that once a controller realizes a fraudster committed identity theft, any changed personal information should be rectified while simultaneously maintaining a separate record of the personal data that was changed or saved while the fraudster impersonated the original data subject, for example in line with how the ICO deals with 'mistakes' in their Guide.[137] (**Jasper Hille**)

> 108. Archived personal data needs to be distinguished from back-up data that is personal data stored solely for the purpose of restoring the data in the case of a data loss event. (…)

Backups/logs can be part of key design and default elements of the principle of security (integrity and confidentiality) according to the EDPB Guidelines on article 25.[138] By definition, backups are a copy of a dataset at a specific timeframe, as defined by the Storage Networking Industry Association.[139] Practically speaking, there are different approaches to backups and the manner in which alterations in personal data are stored.[140] Therefore, it may be very difficult for many data controllers to oversee the differences in personal data between the live system and back-up systems as logs don't necessarily contain data on such differences. The guidelines are unclear about what exactly is expected of controllers past being 'transparent about the situation' and should provide additional guidance. (**Jasper Hille**)

> 109. What remains to say is that the data subject is entitled to have access to all data processed relating to them, or to parts of the data, depending on the scope of the request (see also 2.3.1 on the completeness of the information and 3.1.1 for the analysis of the content of the request). (…)

---

[135] Michèle Finck, 'Cobwebs of control: the two imaginations of the data controller in EU law' [2021] IDPL 333
[136] ibid
[137] Information Commissioner's Office. (n.d.). Right to rectification - What should we do about data that records a mistake? ICO. Retrieved February 28, 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/
[138] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, p. 24.
[139] Storage Network Industry Association, '2015 Dictionary', p. 207, https://www.snia.org/sites/default/files/SNIADictionaryV2015-1_0.pdf.
[140] Politou, E.A., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. Comput. Law Secur. Rev., 34, 1247-1257.

Data subjects do/may not have the technical/legal knowledge to assess whether the reply is complete, or to judge the quality thereto[141], and that they are the weaker party vis-a-vis the organizations. To booster the right to access, citizens should be able to receive this data in an understandable way. These Guidelines discuss some means (e.g., layered approach) to tackle this challenge (in paragraph 143 of these Guidelines). However, it remains uncertain how DC should provide a completeness of the information while simultaneously assessing the relevance of the data to the DS. The EDPB should further clarify how DC should do this, but also make sure that the clarification does not put an excessive burden on the DC. (**Magdalena Rangelova**)

111. In order to comply with Art. 15(1)(a) to (h) and 15(2), controllers may carefully use text modules of their privacy notice as long as they make sure that they are of adequate actuality and preciseness with regards to the request of the data subject. (…)

As explanation, even if empty or misleading, increases data subject's trust,[142] a user-friendly privacy policy might be used to misled data subjects into thinking that all the elements under Article 15 of the GDPR have been provided.[143] On the other hand, an (unnecessarily) lengthy privacy policy may lead to information overload – a form of a dark pattern known as *obstruction* – and consequently, data subjects may dismiss the information altogether.[144] Indeed, Reindenberg et al[145] shows that privacy policies are not only misleading but take too long to read and 'may be the least read items on most websites.'[146] Moreover, distributing information (privacy policy, copy of personal data) could also be seen as obstruction since a data subject needs to take multiple steps to obtain all the necessary information.[147] Therefore, the Guidelines should elaborate, considering the above-mentioned scenarios, on the standards for providing information in privacy policies. For instance, when providing a copy of personal data, the controller could be required to list the elements of Article 15 of the GDPR that can be found in the privacy policy and indicate where (e.g., under which section of the privacy policy). This would further develop the idea behind the obligation to indicate where information is provided in the context of the layered approach. (**Eva Opsenica**)

112. Information on the purposes according to Art. 15(1)(a) needs to be specific as to the precise purpose(s) in the actual case of the requesting data subject. It would not be enough to list the general purposes of the controller without clarifying which purpose(s) the controller pursues in the current case of the requesting data subject. (…)

Companies like Facebook refer to their privacy policy, even when explicitly asked to specify the legal basis for data processing and it has been expressed in the literature that this is problematic.[148] Firstly, such an approach is not transparent enough on which specific category of data is linked to which legal basis, leaving the data subject guessing.[149] The EDPB should suggest that provision of the specific legal basis used per purpose and data category is mandatory for data controllers and that such information cannot be provided only in the privacy policy but needs to be specifically addressed when providing access. **(Joanna Taneva)**

115. Concerning the question, if the controller is free to choose between information on recipients or on categories of recipients, it has to be recalled, that, as stated in the above-mentioned guidelines on transparency, already under

[141] René L. P. Mahieu, Hadi Asghari, Michel van Eeten, *Collectively exercising the right of access: individual effort, societal effect* Published on 13 Jul 2018 | DOI: 10.14763/2018.3.927
[142] Chromik, M., Eiband, M., Völkel, S. T., & Buschek, D. (2019). Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems. In *IUI 2019 Workshops, 2327,* 2. http://ceur-ws.org/Vol-2327/IUI19WS-ExSS2019-7.pdf
[143] Ausloos J., Dewitte P. (2018). Shattering one-way mirrors – data subject access rights in practice. *International Data Privacy Law, 8(1),* 1-25, 8.
[144] Ibidem
[145] Reidenberg J. R., Breaux T., Cranor L. F., French B. M., Grannies A., Graves, J. T., … Ramanath, R. (2015). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. *Fordham Law Archive of Scholarship & History*. *https://ir.lawnet.fordham.edu/faculty_scholarship/619/*
[146] Ibidem
[147] Chromik, M., Eiband, M., Völkel, S. T., & Buschek, D. (2019). Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems. In *IUI 2019 Workshops*, 2327, 3. http://ceur-ws.org/Vol-2327/IUI19WS-ExSS2019-7.pdf in connection to 'Nested Details'; 'Similarly, the information *detail* could be distributed, for example nested in many links […] they would have to take many steps to reach the level of detail that satisfies their information need.'
[148] Ausloos, J., Mahieu, R., & Veale, M. (2019). Getting Data Subject Rights Right. *JIPITEC, 10*, 283-309, 292, para 60.
[149] Ibidem.

Art. 13 and 14 GDPR information on the recipients or categories of recipients should be as concrete as possible in respect of the principles of transparency and fairness.

The paragraph is not clear about the criteria to determine when information about the recipients is required and when information about the categories of recipients is sufficient. It should be absolutely clear that, when personal data has been disclosed to a recipient, no matter how many or for what purposes, information should be provided of each recipient. Article 15(c) provides a distinction regarding actual transfers ("to whom the data have been disclosed") and future or eventual transfers ("to whom the data will be disclosed") as the criteria to determine if recipients or categories of recipients need to be informed. **(Phillipe Truan**)

5. HOW CAN A CONTROL PROVIDE ACCESS

120. Information 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.

The European Commission ensures that the rules that protect personal data "travel with the data".[150] In this regard, article 15.2 establishes that data subjects "shall have the right to be informed" where personal data is transferred to a third country. However, this intention or action may be indicated already in the privacy policy of controllers and therefore there would be no need to notify data subjects. Moreover, it is imprecise who shall be leading the notification process, if it is the data subject who needs to fill in a data access request in order to be notified about its data being transferred to a third country; or if this information should be provided by a controller independently of the request of subject access. So far, case law has ruled that no negative report is needed when transfer of data to third countries is not carried out[151], but still the question about this right of information is ambiguous. It would be interesting for these guidelines to clarify when this notification should be completed. (**Isabel Sierra Rubio**)

121. The GDPR is not very prescriptive as to how the controller has to provide access. The right of access may be easy and straight forward to apply in some situations, for example when a small organisation holds limited information about the data subject. (…)

It is worrying to see that compliance with the obligation placed on controllers to respond to access is low despite there being no prescriptive procedure put in place. Complaints relating to access requests not being fulfilled are the most common complaint for data protection authorities[152]. For example, in 2019 almost 40% of the complaints received by the UK ICO were about access requests[153] and almost 30% of the complaints received by the Dutch DPA were about data subject rights, with a substantial part concerning the right of access.[154] The EDPB is urged to investigate why the controller's obligations to respond is not being adhered to and to place stricter measures in place to ensure compliance by controllers of access requests. (R**oberto de Alcantara**)

Part 5: How can a controller provide access

123. The data subjects should have access to all the information that the controller processes regarding them. This means, for example, that the controller is obliged to search for personal data throughout its IT systems and non-IT filing systems. (…)

[150] European Comission (2021). What rules apply if my organisation transfers data outside the EU? Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en

[151] Hessel, S., & Potel, K. (2021). Recent case law on the right of access in accordance with Article 15 of the GDPR. Retrieved from Reuschlaw Legal Consultations: https://www.reuschlaw.de/en/news/recent-case-law-on-the-right-of-access-in-accordance-with-article-15-of-the-gdpr/

[152] Rene Mahieu, Jef Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' (2020)

[153] See Information Commissioner's Office (2019). Annual Report and Financial Statements 2018-2019, 32

[154] See Autoriteit Persoonsgegevens (2020) Klactenrapportage 2019. Retrieved April 1, 2020, <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/klachtenrapportage_ap_2019.pdf>

It is recommended that the Guidelines include factors for the data controller to consider when assessing the reasonability and proportionality of the search for personal data. These may include, but are not necessarily limited to:

- the circumstances of the request;
- any difficulties involved in finding the information; and
- the fundamental nature of the right of access.[155] **(Rijk Rouppe van der Voort)**

According to the paragraph in question, all the searches concerning the requested data take place based on their structure on the data controllers' systems. However, according to Article 25 of the GDPR, data controllers should take all the necessary technical and organizational measures to ensure that the data protection principles included in Article 5 of the GDPR are respected – and consequently the data subject's rights – during the processing of personal data.[156] Also, EDPB in its Guidelines 4/2019 on Article 25 - and more specifically in point 11 - has highlighted the importance of the principles' implementantion in every concrete data processing operation.[157] This applies also to the process needed for the disclosure of the relevant data and, therefore, it will be very hard for the searches under this paragraph to be conducted. (**Eleni Arampatzi**)

> 124. In line with Art. 25 GDPR on data protection by design and by default, the controller should also already have implemented functions enabling the compliance with data subject rights. This means, in this context, that there should be appropriate ways to find and retrieve information regarding a data subject when handling a request. However, it should be noted that an excessive interpretation in this regard could lead to functions for finding and retrieving information that in itself pose a risk for the privacy of data subjects. (...)

In the second sentence of this paragraph the syntagm "appropriate ways" is used. Following Recital (78), there are given several examples of how controller could stay compliant. In order to exclude the arbitrary from this assessment, there must be a list of minimum requirements in order to help the controllers to stay compliant. (**Marius Chirtoaca)**

> 126. Art. 12(1) of the GDPR states that the controller shall take appropriate measures to provide any communication under Art. 15 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Art. 12(2) provides that the controller shall facilitate the data subject's exercise of access right. The more precise requirements in this regard will have to be assessed case by case. When deciding which measures are appropriate, the controllers have to take into account all the relevant circumstances, including, but not limited to, the amount of data being processed, the complexity of their data processing and the knowledge they have about their data subjects, for example if the majority of the data subjects are children, elderly people or people with disabilites. In addition, in situations where the controller is made aware of any special needs for the data subject making the request, for example through additional information in the request made, the controller needs to take these circumstances into consideration. As a result the appropriate measures will vary.

As a controller needs to take into consideration the special needs of the data subject making a SAR based on the *knowledge* it possesses, the Guidelines should define the efforts that are expected from the controller in obtaining such knowledge. Namely, this obligation can be understood as taking appropriate measures to provide information under Article 15 in line with Article 12(1) of the GDPR *only* based on the data the controller already has on the data subject, which may not indicate that he or she has special needs. In order to comply with Article 12(1) of the GDPR, the Guidelines should encourage controllers to implement mechanisms that would help them to assess whether a data subject might have special needs. For instance, controllers could use on-site surveys[158] with questions such as *Rate how difficult was to find the download button from 1-5* or provide a sample of personal data and ask the data subject to rate the intelligibility of the sample before providing him or her with the information. Moreover, paragraph 9 of the

---

[155] Information Commissioner's Office. (2021, May 20). *Guidance on the right of access*, p. 28. ico.org.uk. Retrieved February 24, 2022, from https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf.

[156] Bygrave, L. A. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review, 4(2),* 114.

[157] Bincoletto, G. (2020). EDPB Guidelines 4/2019 on Data Protection by Design and by Default. *European Data Protection Law Review (EDPL), 6(4),* 575.

[158] Dossetto F. (2021, September 20). The easiest way to find out what people need, right on your website. *hotjar*. https://www.hotjar.com/blog/on-site-surveys/#2-understand-what-your-visitors-like-or-dont-like-and-why

Guidelines on transparency under Regulation 2016/679[159] lists examples of mechanisms that can be used to assess the level of intelligibility and transparency of information. One of the mentioned mechanisms, *readability testing*,[160] could be used by controllers to assess whether supplementary information found in their privacy policy is comprehensible to data subjects with special needs. (**Eva Opsenica**)

Read in conjunction with para 139, a data controller should take a data subject's special needs that he 'is made aware of' into account when delivering communication under article 15 GDPR. Logically, it follows that if a data controller is unaware of a data subject's special needs, he does not need to take them into account. This may lead to problematic situations where (automated) self-service tools are used, as the result of such tool could be unsatisfactory for specific data subjects with special needs, and leave them in a vulnerable position, unable to effectively exercise their rights. The guidelines could specify in which way data controllers should be made aware of special needs of certain data subjects. (**Jasper Hille**)

127. It is important to keep in mind when making the assessment that the term "appropriate" should never be understood as a way of limiting the scope of the data covered by the right of access. The term "appropriate" **does not mean that the efforts to provide the information can be balanced against, for example, any interest the data subject may have** in obtaining the personal data. Instead the assessment should aim at choosing the most appropriate method for providing all information covered by this right, depending on the specific circumstances in each case. As a consequence, a controller who processes a vast amount of data on a large scale must accept to undertake great efforts to ensure the right of access to the data subjects in a concise, transparent, intelligible and easily accessible form, by using plain and clear language.

It can be hard for data controllers to comply with DSARs to this extent, for example in an electronic unstructured format such as email. Due to factors like size, different data formats (eg. live data, back-ups or archives), issues in identifying an individual in the database (eg. mentioning mr. Johnson vs David Johnson) and a mixture of personal information (eg. a file containing personal data about David Johnson but also about Anna Smith), situations may arise where full compliance with the DSAR is realistically impossible.[161] Therefore, a proportionality test should be included for the data controller to limit the search to personal data.
Interestingly, the UK has responded more adequately to this issue. Firstly, the ICO Guidance states that controllers "*are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information*."[162] Secondly, UK courts have recognized that the "*the implied obligation to search is limited to a reasonable and proportionate search,"* and is therefore "*not an obligation to leave no stone unturned*."[163] Thirdly, a current proposal for law reforms (*Data: A new direction*) introduces a cost ceiling to unburden controllers from wide-ranging, speculative DSARs.[164] The UK progressive approach truly seems to be aimed at practical reality. Therefore, it is urged that the EDPB Guidelines take a similar approach. **(Rijk Rouppe van der Voort)**

128. It needs to be avoided to direct the data subject to different sources in response to a data access request. As previously stated in the WP29 Guidelines on Transparency (with regard to the notion of "provide" in Art. 13 and 14), the notion of "provide" entails that "the data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app" (…)

While this paragraph makes it clear that data subjects should not have to collect their personal data from different sources, after using their Subject Acces Rights, the last sentence does appear to leave some room for the data controller

[159] Article 29 Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679* (WP260rev.01). https://ec.europa.eu/newsroom/article29/items/622227/en
[160] Ibidem.
[161] Van Overstraeten, T., Couneson, G., & Church, P. (2022, February 2). *EU: EDPB Guidelines on subject access requests – Intentionally disproportionate?* linklaters.com. Retrieved February 26, 2022, from https://www.linklaters.com/en/insights/blogs/digilinks/2022/february/eu-edpb-guidelines-on-subject-access-requests-intentionally-disproportionate.
[162] Information Commissioner's Office. (2021, May 20). *Guidance on the right of access*, p. 28. ico.org.uk. Retrieved February 24, 2022, from https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf.
[163] [2017] EWCA Civ 121 (Royal Courts of Justice March 3, 2017), para 103.
[164] Department for Digital, Culture Media & Sport (2021). *Data: a new direction*, para 189. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf.

to refer the data subject to the location of some of the data, rather than provide it themselves. In certain cases, such as online web shops where some of the personal data may consist of details pertaining a data subject's order history, it may make sense to refer a data subject to the order history in their website account, without it detracting from a data subject's right to access. The guidelines should provide more clarity on the situations in which it is acceptable to refer to different sources. (**Jasper Hille)**

131. However, under some circumstances it could be appropriate for the controller to provide access through other ways than providing a copy. 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. (…)

It would be helpful if the EDPB clarifies what the controllers should do when they provide information via non-permanent matters. For example, controllers should be able to provide oral information or inspection of files under certain conditions: to keep a record of the date of response, the information that was provided to the data subject, who provided the information, which files were inspected.[165] If there is no record like this, the data controller will not be able to prove that they responded in a timely manner to the request nor that they provided all the information that they are obliged to provide. This is confirmed by the Italian DPA which specified that a verbal response (even if the company has no personal data to provide) is not adequate if there is no record of it.[166] (**Stamatia Beligianni**)

For oral information, there should be a limitation to it as it cannot be saved and check whether it is actual and comprehensive. Art 12(1) GDPR requests that: When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. Therefore, the provision of oral information should be premised on the requirements of the data subject for that approach. Controllers cannot choose this means to provide access for their own convenience. Even though this paragraph tries to have a broad range of examples of non-permanent modalities of access, in its second part it states that " A controller is not obliged to provide the information through other ways than providing a copy ... '' It should be stated expressis verbis, following the assessment in para. 129, that if a copy is not the appropriate solution, then the application of a non-permanent modality is mandatory. I consider it particularly important because a copy might be usually a more convenient method for the controller and therefore it might lead to a discretionary power. **(Marius Chirtoaca)**

132. The controller may choose, depending on the situation at hand, to provide the copy of the data undergoing processing, together with the supplementary information, indifferent ways, e.g. by e-mail, physical mail or by the use of a self-service tool. In any case, the controller has to consider appropriate technical and organizational measures, including **adequate encryption** when providing information via e-mail or online-self-service tools.

It would be beneficial if the EDPB clearly stated the encryption standards to which the data requested by the data subject should be encrypted with, or at least the best practices that the data controllers could follow, as to both better protect the data subject's data and the organizations involved. A collaboration with Europol and Eurojust, which has examined and assessed the efficacy of the various typologies of encryption,[167] could render this possible. This is even more necessary seeing as cybercrime is on the rise during the pandemic,[168] which is a fact that could be taken into consideration in these guidelines. It also has to be underlined that the subject of encryption, pseudonymization, anonymization, and making data safe as a whole, in the context of the GDPR, has mainly been tackled from the perspective of data storage, and not when it comes to sending the data itself to the data subject, as it can be seen by the work done by ENISA[169] and the WP29.[170] (**Antonio Cannavacciuolo**)

---

[165] Information Commission's Office. (2020). Right of access. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/

[166] Garante per la protezione dei dati personali. (2021, May 6). Garante per la protezione dei dati personali – 9445710. GDPRhub. https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_-_9445710

[167] Europol, Eurojust. (2019). First report Observatory Function on Encryption. Luxembourg: Publications Office of the European Union. https://www.eurojust.europa.eu/first-europoleurojust-report-encryption-observatory-function

[168] EUROPOL. (2021). Internet Organised Crime Threat Assessment. Luxembourg: Publications Office of the European Union. , pp. 8-9. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime

[169] European Union Agency for Cybersecurity (ENISA). (2019). Pseudonymisation techniques and best practices, https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

[170] Article 29 Data Protection Working Party (WP29). (2014). Opinion 05/2014 on Anonymisation Techniques. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

In a 2020 empirical study, out of 195 responses to a SAR request, 82 of these responses shared the personal data in plain text or unencrypted zip file over email.[171] While the GDPR does not mandate encryption, mentioning instead that 'appropriate safeguards' should be taken (for example in recital 83 and articles 6 and 32), encrypting personal data sent over (unsecure) email should be standard practice, considering most email is not encrypted itself. Where information is shared in plaintext or through unencrypted means, anyone could gain access to the information.
While some DPA's (such as the ICO) have taken the stance that encryption is (strongly) suggested, the Danish DPA has made it mandatory for businesses in Denmark to encrypt 'confidential and sensitive' personal data sent over email.[172] Furthermore, the Data Protection Authority of the state of Brandenburg has imposed a fine on a company for violating art. 32 GDPR because although the personal data was shared through a password-protected document, the password was sent to the same email address minutes later, in plain text.[173]
The guidelines should stress the importance of encryption of personal data (when transmitting it in response to a SAR request) as a standard practice, especially when responding to the request over email. (**Jasper Hille**)

In the study of Bufalerie et al. argued that sending personal information through electronic means such as emails carries privacy risks when there are no security measures in place such as encryption.[174] It is reasonable to require data controllers who provide information under Article 15 to the data subject to take reasonable steps to protect the data subject's privacy when utilizing electronic means, such as adopting encryption mechanisms when the access information is sent to an email address. The ICO has provided in their guideline on encryption of personal data various types of encryptions that can be used by data controllers and different ways that encryption methods should be implemented. [175] For this reason, this guideline should highlight the criteria catalogue set under article 32 (1) for data controllers to understand which method is best and state of the art in sending personal information through emails. (**Thalis Cabral**)

The wording "… depending on the situation at hand …" is a very vague discretionary power left in favor of the controller. **(Marius Chirtoaca)**

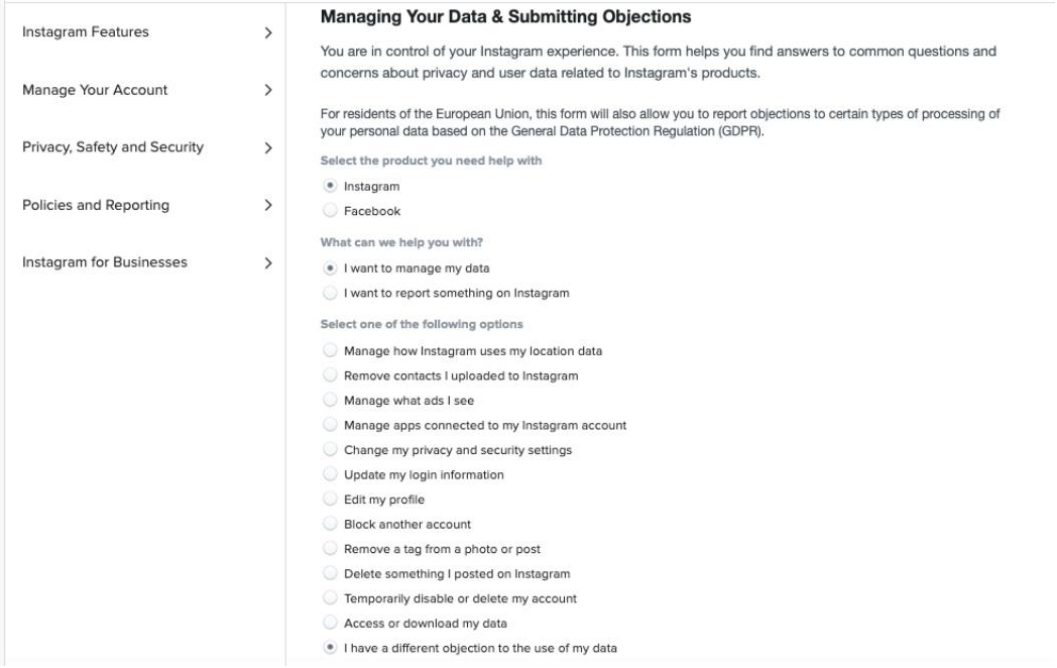
135. Although manual processes for handling access requests could be regarded as appropriate, some controllers may benefit from using automated processes to handle data subject requests. This could for example be the case for controllers that receive a large number of requests. One way to provide the information under Art. 15 is by providing the data subject with self-service tools. This could facilitate an efficient and timely handling of data subjects' requests of access and will also enable the controller to include the verification mechanism in the self-service tool.

This download tool conforms one of the most direct ways of exercising data access rights, as the subject would just need to login into the account (if possible) and download the data.[176] Moreover, it automatises requests, and complies with regulation in a fast and accurate way. However, these download tools often need to cluster information for subjects to download their data. This situation puts data subjects in a position of having to decide which types of data they want to download (see Annex 1). The self-service tool should take into account that the subject might not know which exact data is looking for, as he might not be aware of which data is owned by the controller. It would be interesting for the EDPB to identify threats of self-service tools, in order to prevent them and help balance the relationship between data subjects and controllers. (**Isabel Sierra Rubio 5**)

---

[171] L. Bufalieri, M. L. Morgia, A. Mei and J. Stefa, "GDPR: When the Right to Access Personal Data Becomes a Threat," *2020 IEEE International Conference on Web Services (ICWS)*, 2020, p. 79, doi: 10.1109/ICWS49710.2020.00017.
47 Datatilsynet. (2018, July 23). Stricter practice in relation to encrypted e-mail. Datatilsynet.Dk. Retrieved February 24, 2022, from https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/jul/skaerpet-praksis-ift-krypteret-e-mail/
[173] Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg. (2021). Tätigkeitsbericht 2020 Datenschutz. Retrieved February 28, 2022, from https://www.lda.brandenburg.de/sixcms/media.php/9/TB_2020_web.pdf.
174 Bufalerie et al. 'GDPR: When the Right to Access Personal Data Becomes a Threat' (International Conference on Web Services (ICWS), Beijing, October 2020)
[175] Informantion Commissioner's Office, 'Encryption' (ICO) < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/#types> accessible 26 February 2022
[176] Coline Boniface et al. Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data. APF 2019 - Annual Privacy Forum, Jun 2019, Rome, Italy. pp.1-20. ffhal-02072302

Annex **1**



Nowadays there are a wide variety of automation platforms that can help companies to facilitate subject access request.[177] It is important to emphasize the fact that the self-service tools need to be easily accessible by the average Internet user. (**Marius Chirtoaca)**

136. The use of self-service tools should never limit the scope of personal data received. If not possible to give all the information under Art. 15 through the self-service tool, the remaining information needs to be provided in a different manner. (…)

It could be clarified if data controllers that use this kind of tool must mention and inform the data subjects that not all the personal data will be sent after the request on the download tool and more personal data will be sent via e-mail (or other means). The time that the two files must be sent is also to be clarified, as it is not clear if they must be sent at the same time or if they can be sent at different points. (**Stamatia Beligianni**)

137. According to Art. 12(1) the controller shall take appropriate measures to provide access under Art. 15 in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

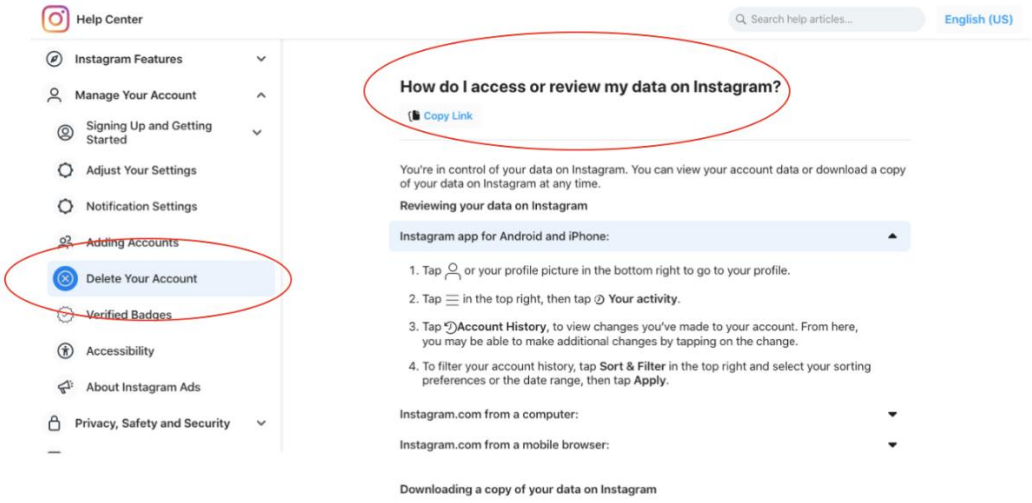
The requirement that Information is 'intelligible' means that it is understood by an average member of the intended audience. Intelligibility is linked to the requirement to use clear and plain language. However, the EDPB in its guidelines can propose that controllers who are uncertain about the level of intelligibility and transparency of the information or the effectiveness of user interfaces/notices/policies could test these through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory groups.[178]
(Roberto de Alcantara)

The EDPB could also provide guidance on how controllers present data download tools or procedures to request data access. More concretely, there is not a specific way of informing data subjects about the possibility of accessing their

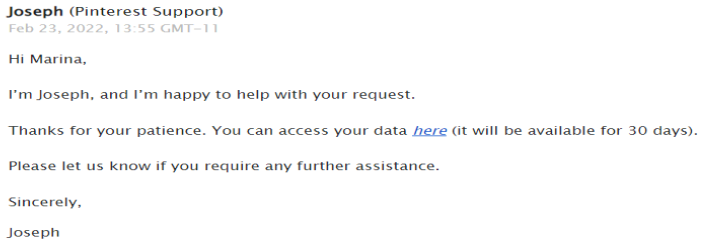
[177] Truyo. (2021). *Data Subject Access Requests: How Automation Can Help Make Compliance Easier*, insights.truyo.com. Accessed March 1, 2022, from https://insights.truyo.com/data-subject-access-requests-automation
[178] Article 29 Data Protection Working Party: Guidelines on transparency under Regulation 2016/679 (2017) 7

data, and in some cases, it may not be "easily accessible"[179]. Guidelines on transparency underline that for information to be easily accessible the data subject should not be in need of seeking out the information. Therefore, the way controllers present the options to download data or to create a SAR may not need to be "easily accessible", but it should at least not me misleading. In a recent data subject request, the option to download the information could only be found under the "Delete Your Account" section. This creates a lot of confusion, as article 15 does not entail the delete of data stored or processed by controllers. The way controllers offer the possibility to practice data subject requests may alter the main purpose of article 15: to grant access to data and information on how it is processed. It would be very encouraging to see best practices on how to present download tools and data access requests procedures in a user-friendly manner.
(**Isabel Sierra Rubio**)

Annex 2



Expiring links[180] are commonly used and readily available. For example, as an answer to uploaded SAR to the Pinterest website[181], it has provided link that last 30 days.


Joseph (Pinterest Support)
Feb 23, 2022, 13:55 GMT-11

Hi Marina,

I'm Joseph, and I'm happy to help with your request.

Thanks for your patience. You can access your data *here* (it will be available for 30 days).

Please let us know if you require any further assistance.

Sincerely,

Joseph

Despite the fact that data is available on the link and can be downloaded, access to personal data itself is limited to a period of 30 days. Therefore, Guidelines should provide additional information regarding usage of exact or similar means that can limit the right of access and define such as good or unfavorable practice. **(Marina Mijuskovic)**

138. The requirement that providing access to the data subject has to be done in a concise and transparent form means, that controllers should present the information efficiently and succinctly in order to be easily understood and captured by the data subject, especially if it is a child. The controller needs to take into account the quantity and complexity of the data when choosing means for providing access under Art. 15.

Should different quantities of data be provided to a 11 and 15 years old? If yes, is the data controller qualified to make this assessment? Moreover, not all 15 year old have the same level of knowledge. The safest bet for the data controller

[179] Ibidem, page 8
[180] Introducing share links with time expirations, Koofr Blog, available on https://koofr.eu/blog/posts/introducing-share-links-with-time-expiration , accessed on 25.02.2022.
[181] Pinterest available on https://www.pinterest.com/ , accessed on 28.02.2022.

would be to provide 2 versions of information: one as if the data subject was an adult and the other one in a simplified format. This measure would guarantee data the data subject right to access her personal data was not infringed. **(Marius Chirtoaca)**

> 140. (…) The information should always be given in a plain and clear language. A controller that offers a service in a country should also offer answers in the **language that is understood by the data subjects in that country.** (…) The controller should take special care to ensure that people with special needs, such as elderly people, children, visually impaired persons or persons with **cognitive disabilities** can exercise their rights, for instance by proactively providing easily accessible elements to facilitate exercise of these rights.

Whereas para.140 states that the language in which the controller offers the service should be offered in relation to SARs, it is not clear whether for controllers that provide their services in a specific country in *multiple languages*, there is the obligation to also offer access in those languages (other than the language of that country). An example of this is the Dutch website of Amazon,[182] where one can choose both Dutch (default language) and English. Would I, as a user using the English version of the website, be entitled to access my data formatted in the English language? Clarification on this point may further the ability of data subjects to fully utilize their art.15. In fact, language is an essential element to be taken into consideration in the field of privacy, as it is pivotal in relaying clear information that is understandable to the user, such as through data policies, both in written language and programming language.[183] When this is not provided to the users, the users will not use their privacy rights, which in turn may cause unwanted legal consequences for companies.[184] (**Antonio Cannavacciuolo**)

More attention should be paid to how the persons with disabilities can exercise their rights. Some examples of these elements could be i) the presentation of elderly people data in a short video to be more understandable to them and less time-consuming concerning the difficulty they often have regarding the use the new technologies, ii) voice assistance messages presenting the data for visually impaired people or people with cognitive disabilities. (**Evangelia Cheiladak**i).

There are several cases where the data subjects – after the submission of data requests – have been confronted with inaccurate personal data.[185] Therefore, it would be useful if Guidelines contained advice regarding how data controllers should respond to data requests in a more specific manner. (**Eleni Arampatzi**)

> 143. When deciding what information should be given in the different layers the controller should consider what information the data subject in general would consider as most relevant. In line with the fairness principle, the first layer should also contain information on the processing which has the most impact on the data subject and processing which could surprise them. The controllers need to be able to demonstrate accountability as to their reasoning of the above.

According to the paragraph, the data controller should take into account what information the data subject would consider as most relevant. However, we could argue that the data controllers proceed to a normative yardstick, rather than a statistical one, because every data subject could consider as "most relevant" a different category of data. Therefore, the EDPB could give further clarifications. (**Eleni Arampatzi)**

> 144. For the use of layered approach to be considered as an appropriate measure it is necessary that the data subject is informed at the outset that the information under Art. 15 is structured into different layers and provided with a description of what personal data and information that will be contained in the different layers (…)

[182] Amazon.nl

[183] Kumaraguru, P. et al. (2007). A Survey on Privacy Policy Languages, p.1 https://precog.iiitd.edu.in/Publications_files/Privacy_Policy_Languages.pdf

[184] Ibidem.

[185] Thomas van Biemen (2018) "Personal Privacy in Practice: Putting the GDPR to test in a collective exercise of data subjects' right of access", Technical University of Delft, pp. 31.

A layered approach can constitute a means of data provision which could easily be exploited by data controllers. Users can be unlawfully steered when technical language is used.[186] It has been argued that numerous of users do not even proceed to the second layer of consent requests.[187] Similarly, in the layered approach scenario, the data subjects – and especially those who do not have any relevant knowledge or appear to be easily convinced – could decide to limit their request to the first layer due to the technical wording used by the data controllers. Therefore, we should consider that the description that will reflect the categories of the data processed by the data controller which correspond to different layers should be clear and detailed. Data controllers must always be precise and transparent while applying this specific form.[188] (**Eleni Arampatzi**)

146. According to Art. 12(1), information under Art.15 shall be provided in writing, or by other means including, where appropriate, by electronic means. (…)

The term "by other means including, where appropriate, electronic means" does not specifically state if that means are accessible to data subjects with disabilities. More precise wording could make clear that these people can access their right too as it is stated in Guideline No. 140. "Other means" which let e.g., blind people have access can be: the use of voice assistance messages, tools that include options to magnify, keyboard control and verbal descriptions to describe what is happening on screen[189],or where electronic tools are not available a hard copy of the data (typed in Braille system) delivered to the data subject (**Evangelia Cheiladaki**).

147. What could be considered as commonly used electronic form should be based upon the reasonable expectations of the data subject and not upon what format the controller uses in its daily operations. The data subject should not be obliged to buy specific software in order to get access to the information.

To suggest that information be sent in a format to the data subject which is based on his or her reasonable expectations is impractical as the majority of data subjects requesting information do so for the first time[190] and have no expectation as to the form of data. The EDPB could be encouraged to undertake user studies to determine user expectations on the preferred form of data. **(Roberto de Alcantara)**

Whereas the machine-readable format will comprehend all the data, the PDF is designed for printing, rather than for analysis.[191] Furthermore, PDF has been found insufficient to provide the data subject access to all the information.[192] Therefore, the use of PDF to comply with the subject access request mainly disadvantages the data subject and expels the possibility to analyze the data.[193] Moreover, the provision of machine-readable data is crucial for research purposes.[194] The use of PDF is therefore inadequate in complying with the subject access request when this concerns a machine-readable format. This has also been underlined by the *Guidelines on the Right to Data Portability* with regard to the conversion of emails.[195] Thus, it is urged that the EDPB amends the Draft Guidelines to specify that machine-readable formats should be provided to the data subject in its original form, rather than converting such to a PDF. However, data controllers could be obliged to provide the information in PDF *besides* the machine-readable format when the latter is inaccessible for the data subject. Furthermore, the data controller may have to provide guidance to allow the data subject to understand the machine-readable format. **(Rijk Rouppe van der Voort**)

---

[186] Utz, Christine & Degeling, Martin & Fahl, Sascha & Schaub, Florian & Holz, Thorsten. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.*

[187] McDonald, A. M., & Cranor, L. (2008). The Cost of Reading Privacy Policies. I/S: Journal of Law and Policy for the Information Society, 4(3), 543-568;

Santos, C., Rossi, A., Sanchez Chamorro, L., Bongard-Blanchy, K., & Abu-Salma, R. (2021). What Is the Purpose of Cookie Banners? Analyzing Cookie Banner Text through a Legal Lens. In *Workshop on Privacy in the Electronic Society (WPES)* ACM.

[188] Guidelines on Transparency under Regulation 2016/679 - endorsed by the EDPB, pp.19-21.

[189] <https://usabilitygeek.com/10-free-screen-reader-blind-visually-impaired-users/> Accessed 28 February 2022

[190]Rene Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively exercising the right of access: individual effort, societal effect" (2018) 15

[191] Ausloos, J., Mahieu, R., & Veale, M. (2019). Getting data subject rights right. *JIPITEC*, *10*, 283–309, para 23. https://doi.org/10.31228/osf.io/e2thg.

[192] I bidem

[193] Ibidem

[194] Ibidem

[195] Article 29 Data Protection Working Party (2016). Guidelines on the Right to Data Portability (WP 242), p. 14. https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

If the data is delivered in PDF format, the data subject should have the possibility to ask for the data to be delivered in a machine-readable format such as JSON or CSV, especially when there are vast amounts of information, as it is notoriously difficult to extract data from[196]. **(Phillipe Truan)**

It will be a better practice if the above paragraph suggests the controllers to provide data subjects with the possibility to select 'their preferred format, prior to fulfilling their request'.[197] Moreover, direct access to their data will be achieved more efficiently if information will be sent to data subjects 'in an encrypted format', providing them separately with a secure code in order to access the encrypted data.[198] (**Olga Lampousi**)

> 148. When deciding upon the format in which the copy of the personal data and the information under Art. 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. It is important that the data subject is provided with information in an embodied, permanent form (text, electronic). (…)

According to paragraph 131 of the Guidelines, access without the possibility of downloading the information is a non-permanent modality of access. Conversely, paragraph 148 seems to suggest that a 'permanent form' does not require that the data subject is able to download the information. Accordingly, there seems to be two definitions of what is *permanent* and using both might prevent controllers from being certain on what is expected of them. Namely, if not providing the possibility of downloading the information is considered as non-permanent,[199] the requirement of providing information in a 'permanent form (text, electronic)' could be interpreted as an obligation to provide the information either in a physical document ('text') or in a way that allows the information to be downloaded ('electronic'). This might be due to the blurry distinction between a modality of access and a form. For instance, paragraph 149, under the section *Format*, discusses what the Guidelines introduced as a modality of access,[200] seemingly contradicting paragraph 131[201] by stating that 'For the requirement to provide a copy of personal data to be fulfilled [...] data subjects need to be able to download their data in a commonly used electronic form.' This considered, the Guidelines should clearly establish the difference between a modality of access and a form such as by explaining the obligations in connection to each only under separate sections and use the term *permanent* uniformly (or avoid using it). (**Eva Opsenica**)

> 151. **Making some kind of compilation and extraction** of the data that makes the information easy to comprehend is also a way of complying with the requirements to provide the information in a way that is both intelligible and easily accessible.

Whereas initially it is argued that the data provided for must be fully comprehensive (see for instance paras 35 and 123), para 151 states that the data controller can suffice by "making some kind of compilation". The noun 'compilation' is defined in the Oxford Dictionary as: "*a collection of items (…) taken from different places and put together*". This stands opposite to the principle that all personal data must be provided (which is also underlined in the ICO Guidance: "*The UK GDPR places a high expectation on you to provide information in response to a SAR*").[202] At the same time, however, the comprehensiveness of the requested information creates an inherent tension with the principle of

---

[196] Ausloos, J., Mahieu, R., & Veale, M. (2019). Getting data subject rights right. *JIPITEC, 10*, 283–309, para 23. https://doi.org/10.31228/osf.io/e2thg.

[197] Information Commissioner's Office Guidelines. (2020). Right of access. Retrieved from https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf. p 35.

[198] Ibidem.

[199] European Data Protection Board. (2022). *Guidelines 01/2022 on data subject rights – Right of access* (version 1.0), para. 131. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

[200] European Data Protection Board. (2022). *Guidelines 01/2022 on data subject rights –Right of access* (version 1.0), para. 148. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en p. 3, stating that 'The main modality for providing access is to provide the data subject with a copy of their data [...]'; *see* also paras. 130, 131.

[201] Para. 131 states that non-permanent modalities of access such as access without the possibility of downloading information may be appropriate ways of granting access where 'It is in the interest of the data subject or the data subject asks for it.'

[202] Information Commissioner's Office. (2021, May 20). *Guidance on the right of access*, p. 28. ico.org.uk. Retrieved February 24, 2022, from https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf.

intelligibility (the provided information must be understandable and clear, para 139 Draft Guidelines).[203] But making a compilation of the data is not the solution to solve this tension. Instead, as provided for in para 139 of the Draft Guidelines, "*the controller might need to supply the data subject with additional information that explains the data provided."* Furthermore, the recommendation of making a compilation seems to be at odds with the previously advocated layered approach (see 142-145 Draft Guidelines). Therefore, it is urged that paragraph 151 be amended as to exclude the wording "making some kind of compilation" and to add that data controllers must be comprehensive when providing the requested information. **(Rijk Rouppe van der Voort)**

The syntagm "some kind of compilation" is vague and leaves a big margin of decision to the data controller. In accordance with the other paragraphs referring to the information that need to be provided to the data subjects, the compilation needs to have a thorough overview over the most important aspects. (**Marius Chirtoaca)**

> 153. In some cases, the personal data itself sets the requirements in what format the personal data should be provided. When the personal data for example constitutes handwritten information by the data subject, the data subject needs in some cases to be provided with a photocopy of that handwritten information since the handwriting itself is personal data. (…)

The EDPB accepts transcripts of audio recordings instead of the actual recordings to be sufficient for access "in some cases". The example named is if the data subject agrees with this. However, this implies that there are also cases where a transcript would be sufficient where the data subject does not agree with receiving a transcript instead of the recording. The guidance does not clarify under what conditions this would be acceptable. It would be a good idea to add more examples or criteria, otherwise this part of the guidance could be abused by data controllers claiming that they do not have to supply the data subject with their audio recording. **(Tomas Baçe)**

There is no example of format that disable people can use (neither the handwritten information nor the audio recording can help them). (**Evangelia Cheiladaki**).

> 155. Art. 12(3) requires that the controller provides information on action taken on a request under Art. 15 to the data subject without undue delay and in any event within one month of receipt of the request. (…)

The determination of a specific deadline for the controller's reply to the data subject's request is a necessary requirement, since, on one hand, a one-month time limit is enough for controllers to process the data and, on the other hand, time restrictions are crucial, in order for the controller to not exploit specific situations, such as the hypothesis that the type or category of the requested data is difficult to process, even though this may not correspond to reality. The appropriate time limit should be approached using a case-by-case assessment, since there are cases when the requested data require less than a one-month period to process. According to ICO guidelines, 'whether a request is complex depends upon the specific circumstances of each case'.[204] Moreover, it should be added in the paragraph that the same time limit is also valid for cases where controllers will not provide any data, because for instance these data is no longer processed. This was the case with the French DPA (CNIL) who found that a French mobile telephone operator company neither replied to SARs within the time limit nor informed the complainants 'within one month when they will not provide any data'.[205] (**Olga Lampousi**)

It could be clarified that a delay could trigger the right to compensation. More specifically, in that regard, the Higher Regional Court of Vienna ruled that a delayed answer could lead to material damages[206] and thus it arms the data subject with the right to claim compensation.[207] On the other hand, the District Court of Bonn ruled that data subjects are entitled to compensation only when there is a violation in processing[208] and argues that a delay in answering is not

---

[203] See para 141 of the Draft Guidelines.

[204] Information Commissioner's Office Guidelines. (2020). Right of access. Retrieved from https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf. p 17.

[205] GDPRhub. CNIL (France) - SAN-2021-021. Retrieved from https://gdprhub.eu/index.php?title=CNIL_(France)_-_SAN-2021-021&mtc=today.

[206] REPUBLIK ÖSTERREICH Oberlandesgericht Wien. (2020). 11 R 153/20f, 154/20b. https://noyb.eu/sites/default/files/2020-12/BVI-209_geschw%C3%A4rzt.pdf

[207] Hessel S., Potel K. (2021). Recent case law on the right of access in accordance with Article 15 of the GDPR. https://www.reuschlaw.de/en/news/recent-case-law-on-the-right-of-access-in-accordance-with-article-15-of-the-gdpr/

[208] District Court of Bonn. (2020). Cases 15 O 372/20 and 15 O 355/20.

such a case.[209] In that regard, the EDPB could clarify whether delayed answers to SARs trigger (or may potentially trigger) under article 82 GDPR. **(Stamatia Beligianni)**.

157. The time limit starts when the controller has received an Art. 15 request, meaning when the request reaches the controller through one of its official channels. It is not necessary that the controller in fact has taken notice of it.

It would be beneficial to both parties if a reasonable time frame was established for the data subject to submit the essential information to the controller to guarantee that there is no additional delay in fulfilling the access request. This suspension in time can be calculated based on article 3 of the 1182/71 Regulation on determining the rules applicable to periods, dates and time limits.[210] In considering the time limit for the suspension, it needs to be proportional to allow the data subject enough time to provide the necessary additional information needed to the data controller, provided that the additional information was requested without undue delay. (**Thalis Cabral)**

A reasonable period of time before considering the request closed[211] should be stated in the Guidelines. It should also not be assumed that the data subject simply does not wish to respond as he or she may struggle with specifying the request.[212] In the context of a vague SAR, it is also important to highlight that the Guidelines do not explain the consequences of a data subject's vague or modified reply to the controller's request for specification. For instance, it is possible to envision a situation where the data subject additionally clarifies/modifies the request in a way that would imply additional time and costs for the controller.[213] Would, in that case, the controller have three months in total to provide access due to the complexity of the request? If that is so, the Guidelines should list this under the factors that are considered relevant for establishing a complex request in paragraph 161. (**Eva Opsenic**a)

6. LIMITS AND RESTRICTIONS OF THE RIGHT OF ACCESS

164. It is important to note that, apart from the above-mentioned limits, derogations and possible restrictions, the GDPR does not allow any further exemptions or derogations to the right of access. That means inter alia that 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 under Art. 15 GDPR79.

Proportionality always plays a significant role about individuals rights under the GDPR[214]. In the case Rotterdam v Rijkeboer (Case C-553/07), the CJEU considered a controller's duty to store certain information in order to respond to a DSAR and held that this duty may represent an excessive and *disproportionate* burden[215], recognizing the necessity to establish a fair balance between the rights of individuals and the burden placed on controllers[216]. Additionally, it is important to mention that paragraph 171 expressly mentioned that the exercise of the right of *access has to be balanced against other fundamental rights in accordance with the principle of proportionality*. Paragraph 69 also mentions that the *controller shall carry out a proportionality assessment when reasonable grounds* for doubting the identity of the requesting person exists. Thus, it is necessary to clarify this contradiction in the sense that the principle of proportionality should be applied even with some limitations. (Q**uezia Amaral Sayão)**

---

[209] Hessel S., Potel K. (2021). Recent case law on the right of access in accordance with Article 15 of the GDPR. https://www.reuschlaw.de/en/news/recent-case-law-on-the-right-of-access-in-accordance-with-article-15-of-the-gdpr/

210 Regulation (EU) 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits [1971] OJ L 124 art 3

[211] Information Commissioner's Office. *What should we consider when responding to a request?* ico. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-should-we-consider-when-responding-to-a-request/#clarify stating that 'Where you seek clarification, but do not receive a response, you should wait for a reasonable period of time before considering the request 'closed'. While one month is generally reasonable, you should adopt a proportionate and reasoned approach.'

[212] Ibidem

[213] Society for Computers and Law (communication to ICO, p. 4) https://ico.org.uk/media/about-the-ico/consultations/sars/4018247/society-of-computers-and-laws-privacy-committee.pdf

[214] Lawne R. (2020, February 26). *Subject Access Requests and the Search for Proportionality*. Fieldfisher. Retrieved February 25, 2022, from https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/subject-access-requests-and-the-search-for-proport

[215] ibid

[216] Rotterdam v M. E. E. Rijkeboer, Case C-553/07, (Raad van State – Netherlands) OJ C 153 from 04.07.2009, p.10

By adopting this paragraph, the EDPB Draft Guidelines strongly advocate a wide reach of the data subject access request. Namely, this right may not be restricted by the data controller who claims to be disproportionately burdened to provide the requested information. Therefore, this then excludes the possibility for the data controller to either (i) charge a reasonable fee or (ii) refuse the data subject access request (according to Article 12(5) GDPR). From the perspective of the data controller, this stance is highly undesirable and can cause problems in practice. Although the right of the data subject to make an access request should generally prevail over the difficulty of the data controller to provide the requested information, a safety net in the form of a proportionality test could filter out frivolous requests that put a disproportionate burden on the data controller (ie. where compliance can reasonably not be expected). This interpretation is in line with the general case-by-case approach of subject access requests (see in that respect para 174 of the Guidelines). Furthermore, case-law has allowed for an exception based on a disproportionate burden on the data controller before (see Regional Court of Heidelberg, February 21, 2020, O 6/19, paras 35-37 ("*einen unverhältnismäßigen Aufwand*")).[217] Naturally, this proportionality exception must be interpreted narrowly. Consider, for example, a small voluntary organization that provides second-hand clothes to relatively poor countries within the EU. Through local municipalities, it has obtained personal data about the people they are sending the clothes to. But the organization only consists of a few members, mostly elderly people that store the personal data non-electronically (though in a filing system). If one of the data subjects files a subject access request (which, moreover, will be in a foreign language to the organization), the burden to provide the requested information seems disproportionate for the organization (that, according to the "easily accessible" requirement must provide the information in a language understood by the data subject, see para 140 of the Draft Guidelines). Therefore, it is urged that the EDPB amends the current approach. If the concerned paragraph of the Draft Guidelines is enacted, further reasons of why this approach was taken and how this affects current practice are required. (**Rijk Rouppe van der Voort**)

The concept of proportionality has been a long-standing general principle of EU law and is explicitly established in article 5(4) TEU.[218] The paragraph seems to indicate the above-mentioned limits, derogations and restrictions is exhaustive, and that the right of access is without any general reservation to proportionality. The summary specifies a controller will have to look 'for personal data throughout all IT systems and non-IT filing systems' but it appears this may constitute a disproportional ask. (**Jasper Hille**)

166. According to Art. 15(4) GDPR, the right to obtain a copy shall not adversely affect the rights and freedoms of others. (…)

The EDPB could take into consideration mentioning that the evolving state of technology can impact whether a controller can provide information that also concerns other people, while also considering the availability of current technologies, and that thus due care must be taken by the controller to offer the requested data by taking all the measures possible. For instance, the Spanish DPA ruled that videos taken by security cameras could be given to the requesting data subject, seeing as existing technology is able to obfuscate the faces of other people on camera, consequently protecting their right to privacy, and thus rejecting the reasoning brought by the controller that they couldn't give the video due to other people appearing in it.[219] (**Antonio Cannavacciuolo)**

Regarding the rights and freedom of others, it should be made clearer that the data regarding a DS that is coming from exchanges between persons who are not the DS are regarded as being out of the scope of data request. Indeed, as it is reminded in Recital 63, the rights and freedoms of others should not be infringed upon by the right to access. The secrecy of correspondence is protected by article 8 ECHR as well as by Directive 2002/58/EC ("ePrivacy Directive). Hence, when information about the data subject can be found in correspondence between two people, and where neither

[217] Case derived from: Feldman, R. J., Hickman, T., Lamm, J., Luo, H., & Sloane, C. T. (2022, February 16). *EDPB issues guidelines on right of access under Art. 15 GDPR*. whitecase.com. Retrieved February 23, 2022, from whitecase.com/publications/alert/edpb-issues-guidelines-right-access-under-art-15-gdpr.
[218] CJEU Case 11/70 Internationale Handelsgesellschaft, bH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel [1970] ECR 1125 [12].
[219] Agencia Española Protección Datos, RESOLUCIÓN Nº: R/00634/2021. https://www.aepd.es/es/documento/td-00183-2021.pdf

the sender or the receiver of this correspondence are the data subject themselves[220] -[221], it is justified that this information net be shared with the data subject issuing a request for access, at least not without the prior authorization of the sender and receiver of the correspondence. A brief note on this topic would be welcomed. (**Solène Tobler**)

> 168. According to Recital 63, conflicting rights and freedoms include trade secrets or intellectual property and in particular the copyright protecting the software. These explicitly mentioned rights and freedoms should be regarded as examples, as in principle any right or freedom based on Union or Member State law may be considered to invoke the limitation of Art. 15(4) GDPR82. (…)

The EDPB mentions in paragraph 168 that the right to privacy in Art.8 ECHR can be considered an affected right in light of Art.15(4). However, this brings some confusion because the ECtHR has expressed in *Gaskin*[222] that the lack of consent of the third party data subject whose data may be present in the requested data is not always a justification for a refusal to disclose, but rather there was a need for an independent authority, which has to make the final call. Therefore, more guidance is needed on this topic because the Guidelines do not state what the procedure here would be for data controllers. If this situation is left without clarification, this leaves EU controllers in a Catch-22 scenario where they might be violating their obligations whichever route they take. Therefore, a good solution could be to provide controllers with a list of steps they should take. For example, the ICO Guidance[223] on subject access requests provide the following steps when a data disclosure involves third party personal data: step 1) try to find a way to disclose the data by omitting the third-party personal data. In fact, it can be argued controllers are obliged to take this step, because recently the Romanian DPA fined Kaufland for a violation of Art.15(3) GDPR because it refused to provide data subjects with copies of video surveillance, due to the fact it would infringe third parties' rights to privacy.[224] The Romanian DPA held that the data could be provided if the faces of the persons were obscured.[225] Step 2) if step 1) is impossible, ask for consent. Step 3) if consent cannot be obtained, it should be considered if it would be reasonable to provide information without asking for consent. I would further suggest that the EDPB adds a step 4) if all other steps are impossible, and data disclosure would inevitably violate a third party's right to privacy, the controller should provide data to the data subject, which requested it, but explain that some (and, if possible, which) data has been omitted due to interference with third party rights or that data cannot be disclosed due to the same reason. **(Joanna Taneva)**

The Guideline excluded economic interests of a company as an exception when applying Art. 15(4), with the disclaimer they are related with trade secrets, intellectual property, or other protected rights. Nevertheless, it remains unclear the reason because other fundamental rights, such as "the freedom to run a business" established by Article 16 of the EU Charter should not be applicable more broadly to require a fair balance and proportional response to eventual request under the terms of Article 15(4) of the GDPR[226].**(Quezia Amaral Sayão)**

Though this article discusses personal data, in particular that of emails, we see that there is a mention of the limitation that exists for the right to obtain a copy. We can clearly see that the limitation has indeed been discussed with regard to emails. We see that in Germany, the case of the Federal Labor Court in its Judgement on 27 April 2021 (Case No.2 AZR 342/20)[227]. Here, a motion demanding that the defendant be forced to provide his emails that have been subject

---

[220] CNIL. (2022). *Le droit d'accès des salariés à leurs données et aux courriels professionnels*. CNIL. URL: https://www.cnil.fr/fr/le-droit-dacces-des-salaries-leurs-donnees-et-aux-courriels-professionnels#:~:text=Le%20droit%20d'accès%20porte,fondement%20du%20droit%20d'accès.

[221] GDPRHub. (2021). *Persónuvernd (Iceland) - 2020031242*. Category: Article 15 GDPR. URL: https://gdprhub.eu/index.php?title=Persónuvernd_(Iceland)_-_2020031242

[222] *Gaskin v United Kingdom* [1990] EHRR 36.; Ausloos, J., Mahieu, R., & Veale, M. (2019). Getting Data Subject Rights Right. *JIPITEC, 10*, 292. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544173

[223] ICO Guidance on Subject Access Requests, 21 October 2020, pp. 42-43 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

[224] ANSPDCP (Romania) - Fine against Kaufland Romania SCS. (2022, January 20). GDPRhub. Retrieved February 26, 2022, from https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_Kaufland_Romania_SCS

[225] Ibidem.

[226] Tanguy Van Overstraeten, Guillaume Couneson and Peter Church (2 February 2022), *EU: EDPB Guidelines on subject access requests – Intentionally disproportionate?* Linklaters. Retrieved February 24, 2022, from https://www.linklaters.com/en/insights/blogs/digilinks/2022/february/eu-edpb-guidelines-on-subject-access-requests-intentionally-disproportionate

[227] 2 AZR 42/20 (Federal Labor Court April 27, 2021

to processing and had also been sent to the work based email address of the defendant or those emails that had included his name. The ruling was the motion was not specific enough. This particular case limits the right of access and more employees that are leaving their work have chosen to use this method, this procedure has been efficient in preventing abuse. When applied to the article, we see that the right to confidentiality is still maintained in a strong manner, the right to obtain a copy is limited, with the requirement being that of specificity. Clearly, the protection of the rights of citizens and protection of personal data in this case is viewed, therefore both the GDPR and European Charter are valued. (**Arystan Jazin**)

"In terms of copyright protection, in case of pictures or videos of data subjects, data controllers have to determine whether the copyright holder is data subject or someone else.".[228] She explains that if the picture was provided to the DC by the DS (who is also the author of the picture) then the access right to the picture has to be provided. However, she further elaborates that in case the author is not a data subject (e.g. the picture was uploaded on the social network by third person and data subject was tagged on the picture), it is not acknowledged by the GDPR if data controllers have obligation to acquire IP rights from third parties in order to provide right of access to data subjects.[229] Thus, the EDPB could clarify the current uncertainty as mentioned by Angela Sobolciakova.[230] (**Magdalena Rangelova**)

168. According to Recital 63, conflicting rights and freedoms include trade secrets or intellectual property and in particular the copyright protecting the software. (…)

In connection to
195. Controllers, who plan to rely on a restriction based on national law must carefully check the requirements of the provision of the respective national legislation. (…)

In relation to limitation and restriction of the right of access, Guidelines differ bases of limitation into rights and freedoms of others (Art.15(4)), manifestly unfounded or excessive requests (Art. 12 (5)) followed with state ability to restrict the right of access based on Art 23 of the GDPR. Although further guidance is given in paragraphs from 168 to 195 with reference to Guidelines on restrictions[231], Guidelines do not provide any information regarding automated decision making and access to personal data encompassed in algorithmic processing, nor do they refer to Guidelines on Automated individual decision-making and Profiling, which concern this matter in more detail.[232] Furthermore, the use of algorithms has already provoked issues regarding access to personal data, e.g., French algorithm Parcoursup manages admissions of students to higher education based on algorithmic decision making.[233] Students have already initiated lawsuits[234] to access the data in order to protect their rights (e.g., non-discrimination)[235] as the primary and practical aim of right of access. In addition, the Guidelines on transparency under Regulation 2016/679[236]also do not elaborate on the rights of access in more detail. Thus, Guidelines should directly assess the right of access to personal data regarding circumstances of automated decision making and refer to good practice. **(Marina Mijuskovic)**

170. The general concern that rights and freedoms of others might be affected by complying with the request for access, is not enough to rely on Art. 15 (4) GDPR. In fact the controller must be able to demonstrate that in the concrete situation rights or freedoms of others would factually be impacted.

---

[228] A Sobolčiaková, *Right of Access under GDPR and Copyright*, (Masaryk University Journal of Law and Technology, 2018) <https://scholar.google.nl/scholar?start=10&q=right+to+access+data+GDPR&hl=en&as_sdt=0,5&inst=7240083048524121927> accessed 28 February 2022.

[229] Ibidem.

[230] Ibidem.

[231] Guidelines 10/2020 on restrictions under Article 23 GDPR, 13 October 2021.

[232] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 , Article 29 Data Protection Working Party 17/EN WP251rev.01, 6 February 2018.

[233] Restrepo-Amariles, David, Algorithmic Decision Systems: Automation and Machine Learning in the Public Administration (30 November 2020). The Cambridge Handbook of the Law of Algorithms (2020), available at SSRN: https://ssrn.com/abstract=, page 284.

[234] Décision n° 2020-834 QPC du 3 avril 2020, available on, <Décision n° 2020-834 QPC du 3 avril 2020 | Conseil constitutionnel (conseil-constitutionnel.fr)>.

[235] Decision 2019-021 Of 18 January 2019 On The Operation Of The National Platform For Pre-Registration In The First Year Of Higher Education (Parcoursup).

[236] Guidelines on transparency under Regulation 2016/679, Article 29 Working Party 17/EN WP260 rev.01, 11 April 2018.

The EDPB should add an example to this paragraph, noting that "Depending on the interests in question and their relative weight, providing [...] specific information may be rejected. Therefore, it seems like under such circumstances, the EDPB allows data controllers to make the situation less concrete. This however, does not answer the question what should be done in a case where providing any kind of concrete information infringes rights or freedoms of others. In order to prevent abuse, the DPA should be notified when this happens and possibly be granted the right to investigate those cases. (**Tomas Baçe**)

171. With regard to Recital 4 GDPR and the rational behind Art. 52(1) of the European Charter of Fundamental Rights, the right to protection of personal data is not an absolute right (…)

The EDPB formulates a three-step balancing test that the data controller shall consider when personal data of third parties are at stake. The EDPB does not mention that consent as formulated in the GDPR could also serve as a legal basis for providing the requested copy that contains personal data of other people to the requesting data subject. If consent is provided, no further need for the balancing test is required. If consent is not provided, then the controller shall not assume that they no longer have the obligation to answer the SAR.[237] On the contrary, if consent is either denied or not obtained the data controller shall proceed and try to balance in case of conflicting rights and freedoms, which of them will prevail after considering the severity and the risks of the disclosure of third parties' information. The EDPB could also add more circumstances that could be taken into consideration during the balancing test like for example the type of data to be disclosed, any duty of confidentiality owed to the other individual, whether that individual is capable of providing consent, any steps taken by the controller to seek that consent,[238] or any refusal of consent of the other individual.[239] **(Stamatia Beligianni)**

The paragraph adopts a 3 step assessment test for balancing the right of access against other fundamental rights of third persons as an ex-post measure to limit the scope of the SAR . This is especially relevant in the case of 'entangled personal data' as defined by Andrew Cormack[240][1]. Conflicting rights should be proactively avoided (ex-ante) by data controllers considering the article 5 principles and accountability. Cormack provides that "Art.5(1)(b) requirement for purposes to be explicit means those who provide information must know who else it may be linked to and, because Art.5(1)(a) requires fairness to both, that knowledge must not distort the providers' own behaviour or relationship with the processes through which data are collected". The controller thus, can require consent when data subjects are sharing data that relates to third parties. The principle of data protection by design (recital 73) and transparency (recital 39) require that data controllers adopt the appropriate technical and organizational measures to facilitate the exercise of data subjects' rights, and that data subjects are aware of the risks, rules, safeguards and rights in relation to the processing of personal data. (**Phillipe Truan)**.

In the ICO guidelines[241], we see that children are offered protection, as the authorities are aware of the vulnerabilities borne by children. Simply asking for consent may be considered insufficient, and alternative methods of requesting lawful processing is needed. The UK offers clear rules that indicate an emphasis on ensuring that children are adequately protected, though not necessarily given a higher protection of personal data. It would be highly useful if the EDPB Guidelines offered a more direct reference to state whether children enjoy a higher standard of protection of personal data or a similar one to adults. (**Arystan Jazin**)

173. Art. 12(5)GDPR enables controllers to override requests for the right of access that are manifestly unfounded or excessive. These concepts have to be interpreted narrowly, as the principles of transparency and cost free data subjects rights must not be undermined.
174. Controllers must be able to demonstrate to the individual why they consider that the request is manifestly unfounded or excessive and, if asked, explain the reasons to the competent supervisory authority. Each request

[237] Nissim, J. (2020, April 28). The perils of third-party data in data subject access requests. HelloDPO. https://hellodpo.com/blog/the-perils-of-third-party-data-in-data-subject-access-requests/

[238] Ibidem.

[239] English and Wales Court of Appeal. (2018, June 28). [2018] EWCA Civ 1497 Case number: A2/2016/3903. https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWCA/Civ/2018/1497.html&query=(general)+AND+(medical)

[240] Andrew Cormack, 'Entangled personal data: what if it's not only mine?' available at «https://regulatorydevelopments.jiscinvolve.org/wp/2022/01/17/entangled-personal-data-what-if-its-not-only-mine/» last accessed 26 February 2022.

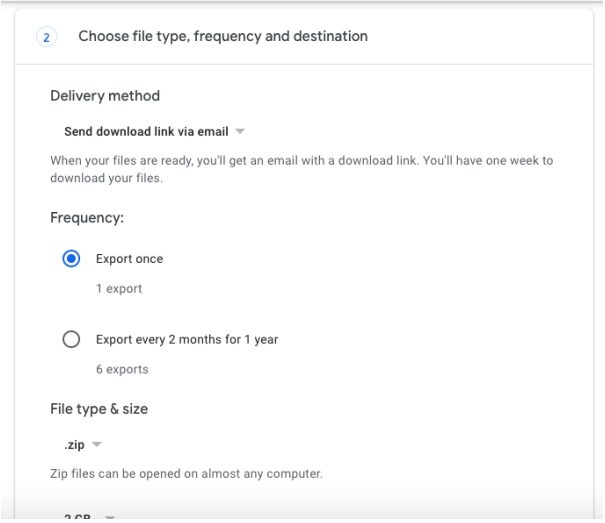
[241] Information Commissioners Office, I. C. O. (n.d.). Guide to the General Data Protection Regulation (GDPR) UK.

should be considered on a case by case basis in the context in which it is made in order to decide if it is manifestly unfounded or excessive.

After having submitted by data access requests, I noticed that on certain websites, such as Reddit, I could exercise my right only once every 30 days and that their email address dedicated to data requests should be contacted only for questions or issues relating to the download of the personal data.[242] In fact, as can be seen from the screenshot, I was completely locked out from taking any action. The guideline doesn't go into detail whether the reasons for denying a data subject their right to access data (under a valid, legal pretext) can be done through an internet interface (without direct contact), instead it simply says that they must "*... demonstrate to the individual why they consider that the request is manifestly unfounded or excessive*"; therefore, it would be useful to shed light on whether the EDPB considers internet interfaces imposing hard locks such as this one to be usable or not. (**Antonio Cannavacciuolo**)

The guidelines address the importance of assessing excessive and unfounded decisions in a **case-by-case** scenario. In this regard, it is worth to mention that some download tools acting as self-service tool of requesting data access, set a specific frequency to get data downloaded (see Annex 3). This strategy is basically preventing users from requesting data continuously, avoiding the situation of excessive and unfounded requests by establishing their own timelines. Moreover, from the subject perspective, companies such as "Mine"[243] identify an email address and send an automatic subject access request to all websites in which the address is found. Taking into account the number of requests that a controller may receive, and considering the completeness of information duty as well, it may be undoable to do a case-by-case analysis, so in the example given, the controller has already found a way of avoiding particular situations and keep using an automated system for data access requests. (**Isabel Sierra Rubio**)

Annex 3



175. A request for the right of access is manifestly unfounded, if the requirements of Art. 15 GDPR are clearly and obviously not met when applying an objective approach. However, as explained especially in section 3 above, there are only very few prerequisites for requests for the right of access. Therefore, the EDPB emphasises that there is only very limited scope for relying on the « manifestly unfounded » alternative of Art. 12(5) in terms of requests for the right of access.

The EDPB mentions that a request is manifestly unfounded when the requirements of article 15 of the GDPR are not met, when applying an objective approach. This seems like a vague sentence that does not explain exactly what constitutes a manifestly unfounded request. Article 15 does not set any formal requirements regarding the SARs, so it is not exactly clear what the EDPB means when it states that "*the requirements of article 15 are clearly and obviously not met".* A practical example of a manifestly unfounded SAR would help to set clearer boundaries. Moreover, the ICO guidelines seem to approach this issue totally differently. ICO suggests that a request may be manifestly

[242] Screenshot made by me with redacted user credentials, available at https://imgur.com/a/sRDcmUy
[243] Mine. (2022). Retrieved from Welcome to The Future of Data Ownership: https://saymine.com/

unfounded when the individual has no intention of exercising their right or when the request is malicious in intent.[244] ICO provides the example that when an individual asks for benefits from a company to withdraw their access request, then the request is manifestly unfounded.[245] On the other hand, the EDPB argues that this is a case of a manifestly excessive request (in paragraph 187). Obviously, the lines around what constitutes a manifestly unfounded request are blurred, and it would be helpful if the EDPB could clarify what exactly is perceived to be unfounded. (**Stamatia Beligianni**)

179. There is no definition of the term "excessive" in the GDPR. On the one hand, the wording "in particular because of their repetitive character" in Art. 12(5) GDPR allows for the conclusion that the main scenario for application of this limb with regard to Art. 15 GDPR is linked to the quantity of requests of a data subject for the right of access. On the other hand, the aforementioned phrasing shows that other reasons that might cause excessiveness are not excluded a priori.

Since there is no definition of the term 'excessive' in the GDPR and considering that the concept needs to be interpreted narrowly [as mentioned in paragraph 173], it would be beneficial for both the data subject and data controllers to understand this concept through an example, especially since it is not as straightforward and that other reasons, besides the repetitive character, can cause excessiveness that are not excluded a *priori.* The ICO provides that a request may be found to be excessive if it is clearly or obviously unreasonable. It is argued that to determine whether a request is excessive, the data controller must consider that the request is proportionate when balanced with the burden or costs involved in dealing with the request.[246] This guideline could follow in similar steps of the ICO to provide elements that need to be considered when determining whether a request is excessive. **(Thalis Cabral)**

Since there is no established minimum that defines a request to be excessive, this might result in abusive requests by data subjects. In a white paper by the Centre for Information Policy Leadership, it was argued that DSR requests are sometimes used for unrelated purposes and/or with the sole intent of disrupting business operations, congesting systems, and increasing costs for organizations, based on the assumption that organizations will face potentially large financial penalties if they do not respond satisfactorily to the DSR request.[247] Furthermore, a Dutch court ruled that there was a violation of rights since the individual submitted an access request solely to utilize the information in another legal proceeding rather than to verify the legality of the data processing.[248] For this reason, the Guideline could provide a specific amount that determines the extent to which the number of requests might be considered as excessive, since it is now entirely up to the controller to evaluate based on an analysis and sector operation. **(Thalis Cabral)**

180. Certainly, according to Art. 15(3) GDPR regarding the right to obtain a copy, a data subject may submit more than one request to a controller87 . In the event of requests that could potentially be regarded as excessive, the assessment of "excessiveness" depends on the analysis carried out by the controller and the specifics of the sector in which it operates.

This paragraph leaves it up to the controller to define excessiveness by conducting an analysis. However, no guidance is given on the structure or factors to be taken into account when conducting such an analysis. It is detrimental enough that the GDPR does not define this term but having no guidance from the EDPB leaves data subjects at risk, because controllers may interpret the term "excessive" in their favour. The ICO Guidance has given some useful examples of factors to be taken into account in order to determine whether a request is manifestly excessive. Firstly, they suggest that excessiveness can be interpreted as whether the request is "clearly or obviously unreasonable."[249] Secondly, the

[244]Information Commission's Office. (2020, October 21). Right of access. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/
[245] Ibidem.
[246] Information Commissioner's Office, 'When Can We Refuse to Comply with a Request' (ICO) < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/when-can-we-refuse-to-comply-with-a-request/> accessible, February 27 2022
[247]Centre for Information Policy Leadership, 'Data Subject Rights under the GDPR in a Global Data Driven and Connected World' (2020) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_data_subject_rights_under_the_gdpr_in_a_global_data_driven_and_connected_world__8_july_2020_.pdf > accessible, 27 February 2022 18
[248] Ibidem
[249] ICO Guidance on Subject Access Requests, 21 October 2020, p. 40 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

controller should conduct a proportionality analysis between the request and the costs to comply with it. When conducting such an analysis, the ICO suggest that controllers should assess the nature and context of the request, the relationship between controller and data subject, what the consequences for the individual would be if the request is not complied with, the controller's resources and whether the request overlaps with other requests. Therefore, the EDPB should consider including more information on how excessiveness should be assessed by taking into account the aforementioned considerations. **(Joanna Taneva)**

184. When 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.

This paragraph seems to be about whether the controller is objectively speaking strained or not and does not take in mind how the average data subject perceives this. This leads to a potential problematic situation where a data subject cannot know whether a data controller will be strained by an electronic request. If the data subject wants to assess whether their electronic data request is likely or unlikely to be regarded as excessive, knowledge about the factual situation is necessary. The problem is that the data subject does not have the knowledge about the objective situation, which is either that the electronic request does strain the controller, or that it does not. In some cases, the objective situation in a company could even vary by the day, which means subsequent data access requests would strain a company today but it might not be strained tomorrow. For the data subject there is no way to know what the objective situation is, and therefore it is difficult to assess whether a subsequent data access request would be likely to be regarded as excessive or not. It is important for the data subject to be able to assess this in advance, since excessive requests may lead to fees. Therefore, if the data subject knows the controller is not strained by the subsequent request, the data subject also knows it is probably not excessive and won't lead to a fee. (**Tomas Baçe**)

186. The fact that it would take the controller a vast amount of time and effort to provide the information or the copy to the data subject cannot on its own render a request excessive89. A large number of processing activities typically implicates bigger efforts when complying with access requests. However, as stated above, under certain circumstances requests can be regarded as excessive due to other reasons than their repetitive character. In the view of the EDPB this encompasses particularly cases of abusively relying on Art. 15 GDPR, which means cases in which data subjects make an excessive use of the right of access with the only intent of causing damage or harm to the controller.

As outlined in my comment under paragraph 164, the EDPB Draft Guidelines adopt a narrow approach with regard to the restrictions that can be made to the subject access request. Namely, it explicitly excludes the possibility for a data controller to limit the request based on reasons of proportionality; excessiveness cannot be established based on excessive time and effort for the controller. From the perspective of the data controller, this interpretation is undesirable. It is diametrically opposed to the case-by-case approach that is generally adopted for assessing a subject access request. Moreover, it rules out the possibility for data controllers to limit the access request in the most exceptional cases where a disproportionate burden is put on their shoulders. Furthermore, proportionality has been used by courts before to establish excessiveness of the data subject access request ((see Regional Court of Heidelberg, February 21, 2020, O 6/19, paras 35-37 ("*einen unverhältnismäßigen Aufwand*")).[250] The adoption of a safety net in the form of a proportionality test is strongly recommended. (**Rijk Rouppe van der Voort**)

The wording of this paragraph might lead to some confusion. It is our recommendation that this paragraph focuses exclusively on reminding data controllers that the amount of data requested, however imposing it might be, does not qualify the request as excessive. Indeed, if there is a vast amount of data being processed, within a complex network of data repositories, it is all the more important that the data subject may have access to a clear and understandable overview of it.[251] Therefore, we recommend that the following sentences be put in a separate paragraph: "However, as stated above, under certain circumstances requests can be regarded as excessive due to other reasons than their repetitive character. In the view of the EDPB this encompasses particularly cases of abusively relying on Art. 15

[250] Case derived from: Feldman et al. 'EDPB issues guidelines on right of access under Art. 15 GDPR' 16 February 2022 < https://www.whitecase.com/publications/alert/edpb-issues-guidelines-right-access-under-art-15-gdpr> Accessed on 23 February 2022.

[251] Ausloos, J., Veale, M., and Mahieu, R.. (2019), *Getting Data Subject Rights Right*, (2019) 10 JIPITEC 283, URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544173

GDPR, which means cases in which data subjects make an excessive use of the right of access with the only intent of causing damage or harm to the controller." (**Solène Tobler**)

The ICO guidelines on right of access clarifies that data controllers need to conduct *reasonable* searches. "You should make reasonable efforts to find and retrieve the requested information. However, you are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information." This information is missing in the current guideline, and I believe that it would be helpful for data controllers to know to what extent they are required to conduct searches to comply with the right of access. (**Elena Sheikhbahaei**)

189. In case of a manifestly unfounded or excessive request for the right of access controllers may, according to Art. 12(5) GDPR, either charge a reasonable fee (taking into account the administrative costs of providing information or communication or taking the action requested) or refuse to comply with the request.

The Guideline does not give any further details on what administrative costs might be counted into a reasonable fee if the data controller decides to charge a fee in case of a manifestly unfounded or excessive request. It must be noted that, for example, the ICO Guideline on the Right of access states that the data controller can consider the administrative costs of (i) assessing, whether or not it is processing the information; (ii) locating, retrieving, and extracting the information; (iii) providing a copy of the information and (iv) communicating the response to the individual, when it charges a reasonable fee.[252] Furthermore, the Finnish DPA stated in its decision concerning Article 15(3) of GDPR that the fee for more than one copy of the data subject's personal data can be based on the costs of mailing, floppy disk, invoicing, and secretarial work, but not on the costs of work, materials or postage related to the execution of the data subject's request.[253] Therefore, some clarification is needed concerning what expenses might be counted into a reasonable fee. (**Patrik Kovács**)

190. The EDPB points out that controllers are - on the one hand - not generally obliged to charge a reasonable fee primary before refusing to act on a request. (…)

This guideline mentions potential compensation for administrative costs of the data controllers, however, there is no mention of compensation for data subjects in case the data controller fails to comply with the right of access of data subjects. The ICO states that individuals have the right to claim compensation if they have suffered damages due to non-compliance with their right to access. This is also elaborated in the ICO guidance on right of access. However, this important information is missing in this guideline. (**Elena Sheikhbahaei**)

191. Controllers must be able to demonstrate the manifestly unfounded or excessive character of a request (Art. 12(5) third sentence GDPR). Hence, it is recommended to ensure a proper documentation of the underlying facts. (…)

In 2018, Max Schrems expressed the initiative of creating a NGO hub to help data subjects exercising their right, supporting them especially in a financial way.[254] Overall, The EDPB guidelines lack information on enforcement, and more concretely about the article 80 GDPR, on representation of data subjects and their possibility of mandating a non-for-profit body to "lodge the complaint on his or her behalf". Raising awareness for enacting data subject rights should also entail subject's possibilities to be financially supported. The financial resource may be an important roadblock for subjects pursuing legal actions against violations of their data. For this reason, I believe it is important for these Guidelines to address the options provided in the Regulation itself to smooth the process of legal actions in case of violation of data subject rights. (**Isabel Sierra Rubio**)

192. Before charging a reasonable fee based on Art. 12(5) GDPR, controllers should provide an indication of their plan to do so to the data subjects. The latter have to be enabled to decide whether they will withdraw the request to avoid being charged.

[252] Information Commissioner's Office (2020) *Right of Access* https://ico.org.uk/media/for-organisations/documents/2619803/right-of-access-1-0-20210520.pdf accessed 21 February 2022.
[253] Tietosuojavaltuutetun toimisto, Finland (2021). Case: 6132/151/19. https://finlex.fi/fi/viranomaiset/tsv/2021/20211083 (in Finnish) accessed 28 February 2022.
[254] Max Schrems Launches a New NGO That is None of Your Business. (2018, January 25). https://gdprinformer.com/news/max-schrems-launches-new-ngo-none-business

The possibility to withdraw the request without incurring a fee may be desirable from a data subject perspective. However, Art. 12(5) GDPR does not describe an obligation for the data controller to indicate the plan to charge a fee to the data subject. Obliging data controllers to give data subjects who lodge a manifestly unfounded or excessive requests an opportunity to not have to pay a reasonable fee and cancel the request, introduces a serious obligation. In fact, by the time a data controller communicates the possibility to withdraw to the data subject, the data controller may already have spent time and resources on the request. Adding this obligation goes further than simply interpreting Art. 12(5) GDPR, as it does not speak of the requirement of such choice for the data subject at all. **(Tomas Baçe)**

194. The scope of the obligations and rights provided for in Art. 15 GDPR may be restricted by way of legislative measures in Union or Member States law. Several Member States have made use of this option.

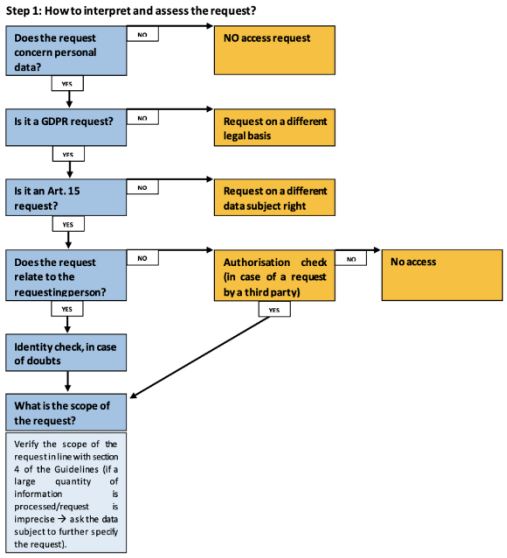
The Guideline completely lacks provisions on cross-border data requests when a data subject sends a SAR to a data controller established in a different Member State. However, such recommendations would be essential in relation to Article 23 GDPR since Member State law under Article 23 GDPR creates fragmentation that might mean (legal) uncertainty for data subjects concerning how they can practice their right of access.[255] As professor González Fuster and her colleagues wrote in their response to the public consultation on Guidelines 10/2020 on restrictions under Article 23 GDPR, data subjects are probably not aware of such restrictions implemented by Member State law. If the processing involves more Member States, then probably the situation is worse because, in lack of a common database about the Member States' restrictions, it is questioned how data subjects can get the necessary information about such restrictions, especially if the data controller's Member State allows a restriction whereas the data subject's Member State does not allow such a restriction.[256] **(Patrik Kovács**)

196. Legislative measures laying down the provisions for the application of restrictions under Art. 23 GDPR may also foresee that the exercise of a right is delayed in time, that a right is exercised partially or circumscribed to certain categories of data or that a right can be exercised indirectly through an independent supervisory authority

The EDPB clearly states throughout section 5.3 that for delays there is a duty for the controller to inform the data subject. However, in the specific section regarding art.23 GDPR, there is no mention of informing the data subject of delays due to restrictions imposed by Member States under art.23 GDPR. I believe that it would be opportune to specify in this section whether a duty to inform exists or not, or if it is dependent on the legislative measure of the specific Member State. Without clear instructions on how a controller should behave about the right of access in case of a restriction applied under article 23, would lead to a more fragmentated European standard, entailing a lack of legal certainty, with greater consequences in cases where data processing happens in a cross-border environment.[257] Furthermore, additional help by the EDPB in instructing controllers on how to behave in such situations could be by adding links on their website that redirects to the approach by the Supervisor Authority of specific Member States.[258] (A**ntonio Cannavacciuolo**)

[255] González Fuster, G., Drechsler, L., Mahieu, R. & Peeters, M.N. (2021). Feedback for the European Data Protection Board (EDPB) in response tot he public consultation on 'Guidelines 10/2020 on restrictions under Article 23 GDPR Version 1.0 Adopted on 15 December 2020' https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb_feedback_art23_ggf_ld_rm_mnp.pdf accessed 23 February 2022.
[256] Ibidem
[257] Prof. Dr. Gloria González Fuster et al. (2021). Feedback for the European Data Protection Board (EDPB) in response to the public consultation on 'Guidelines 10/2020 on restrictions under Article 23 GDPR Version 1.0 Adopted on 15 December 2020', p.1 https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb_feedback_art23_ggf_ld_rm_mnp.pdf
[258] Ibidem

Annex.



Considering that the aim of the step 1 flowchart in the Annex of this Guideline (figure above) is to provide a clear understanding of the interpretation and assessment of a request, it would be beneficial to include in this flowchart the other essential elements that have been mentioned in section 3 of this Guideline. One element that is essential, that is difficult to identify is the verification of identification. For example, a chart with 'Have all reasonable measures been taken to verify the identity of the DS?'. This way, if there are doubts, the data controller can do an identity check by requesting additional information from the data subject to confirm identity [as is shown in the chart]. In di Martino et al. it is argued that this step is critical not only for the organisation to respond appropriately, but also to prevent data from being disclosed to an unauthorized third party. [259]
Furthermore, the chart must state that with each denial or refusal of a request, the data controller is required to inform the requester of its decision and provide the relevant rationale. This can be done by including in the flowchart a 'bubble' stating "inform requester of decision and rationale". **(Thalis Cabral)**

259 di Martino et al., 'Revisiting Identification Issues in GDPR 'Right of Access' Policies: A Technical and Longitudinal Analysis' (PoPETS, July 2022) <https://www.marianodimartino.com/dimartino2021_gdpr.pdf> accessible, 28 February 2022 2.