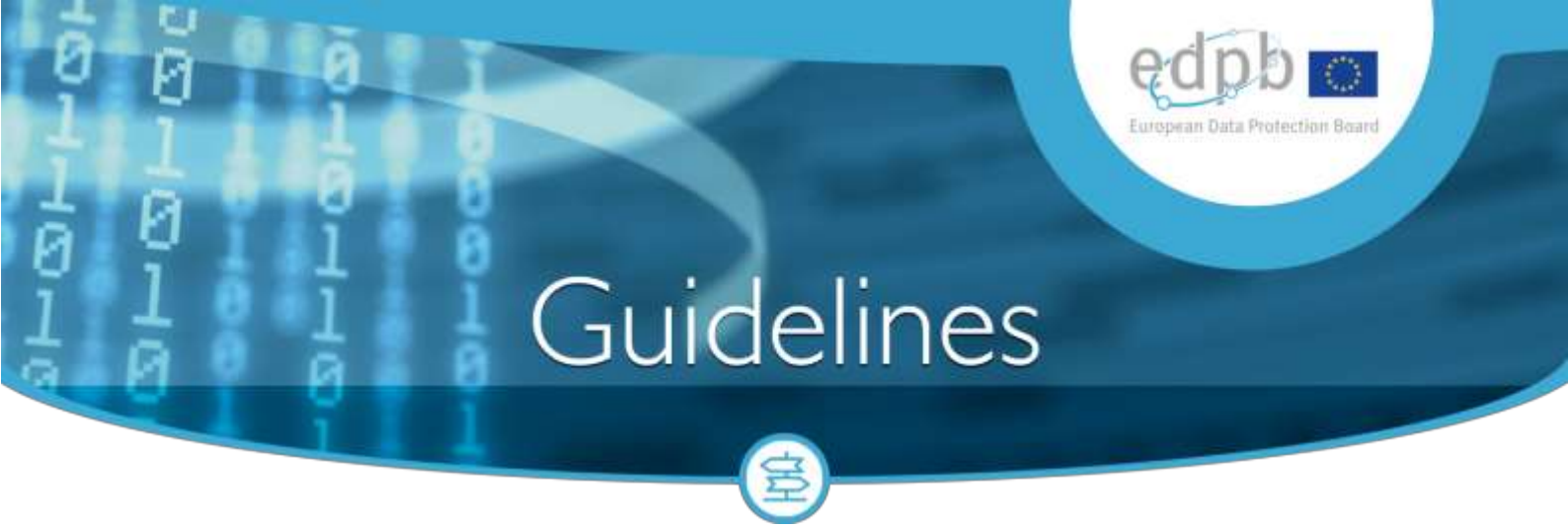


Guidelines 01/2022 on data subject rights - Right of access

Version 2.0

Adopted on 28 March 2023

Version history

Version 1.0	18 January 2022	Adoption of the Guidelines for public consultation
Version 2.0	28 March 2023	Adoption of the Guidelines after public consultation

EXECUTIVE SUMMARY

The right of access of data subjects is enshrined in Art. 8 of the EU Charter of Fundamental Rights. It has been a part of the European data protection legal framework since its beginning and is now further developed by more specified and precise rules in Art. 15 GDPR.

Aim and overall structure of the right of access

The overall aim of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data. This will make it easier - but is not a condition - for the individual to exercise other rights such as the right to erasure or rectification.

The right of access according to data protection law is to be distinguished from similar rights with other objectives, for example the right of access to public documents which aims at guaranteeing transparency in public authorities' decision-making and good administrative practice.

However, the data subject does not have to give reasons for the access request and it is not up to the controller to analyse whether the request will actually help the data subject to verify the lawfulness of the relevant processing or exercise other rights. The controller will have to deal with the request unless it is clear that the request is made under other rules than data protection rules.

The right of access includes three different components:

- Confirmation as to whether data about the person is processed or not,
- Access to this personal data and
- Access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers.

General considerations on the assessment of the data subject's request

When analysing the content of the request, the controller must assess whether the request concerns personal data of the individual making the request, whether the request falls within the scope of Art. 15 and whether there are other, more specific, provisions that regulate access in a certain sector. It must also assess whether the request refers to all or only parts of the data processed about the data subject.

There are no specific requirements on the format of a request. The controller should provide appropriate and user-friendly communication channels that can easily be used by the data subject. However, the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller. The controller is not obliged to act on requests that are sent to completely random, or apparently incorrect, addresses.

Where the controller is not able to identify data that refers to the data subject, it shall inform the data subject about this and may refuse to give access unless the data subject provides additional information that enables identification. Further more, if the controller has doubts about whether the data subject is who they claim to be, the controller may request additional information in order to confirm the identity of the data subject. The request for additional information must be proportionate

to the type of data processed, the damage that could occur etc. in order to avoid excessive data collection.

Scope of the right of access

The scope of the right of access is determined by the scope of the concept of personal data as defined in Art. 4(1) GDPR. Aside from basic personal data like name, address, phone number etc. a broad variety of data may fall within this definition like medical findings, history of purchases, creditworthiness indicators, activity logs, search activities etc. Personal data which have undergone pseudonymisation are still personal data as opposed to anonymised data. The right of access refers to personal data concerning the person making the request. This should not be interpreted overly restrictively and may include data that could concern other persons too, for example communication history involving incoming and outgoing messages.

In addition to providing access to the personal data, the controller has to provide additional information about the processing and on data subjects' rights. Such information can be based on what is already compiled in the controller's record of processing activities (Art. 30 GDPR) and the privacy notice (Art. 13 and 14 GDPR). However, this general information may have to be updated to the time of the request or tailored to reflect the processing operations that are carried out in relation to the specific person making the request.

How to provide access

The ways to provide access may vary depending on the amount of data and the complexity of the processing that is carried out. Unless explicitly stated otherwise, the request should be understood as referring to *all* personal data concerning the data subject and the controller may ask the data subject to specify the request if they process a large quantity of data.

The controller will have to search for personal data throughout all IT systems and non-IT filing systems based on search criteria that mirrors the way in which the information is structured, for example name and customer number. The communication of data and other information about the processing must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The more precise requirements in this regard depend on the circumstances of the data processing as well as the data subject's ability to grasp and comprehend the communication (for example taking into account that the data subject is a child or a person with special needs). If the data consists of codes or other "raw data", these may have to be explained in order to make sense to the data subject.

The main modality for providing access is to provide the data subject with a copy of their data but other modalities (such as oral information and on site access) can be foreseen if the data subject requests it. The data can be sent by e-mail, provided that all necessary safeguards are applied taken into consideration, for example, the nature of the data, or in other ways, for example a self-service tool.

Sometimes, when there is a large quantity of data and it would be difficult for the data subject to comprehend the information if given all in one bulk – especially in the online context - the most appropriate measure could be a layered approach. Providing information in different layers may facilitate the data subject's understanding of the data. The controller must be able to demonstrate that the layered approach has an added value for the data subject and all layers should be provided at the same time if the data subject chooses it.

The copy of the data and the additional information should be provided in a permanent form such as written text, which could be in a commonly used electronic form, so that the data subject can easily download it. The data can be given in a transcript or a compiled form as long as all the information is included and this does not alter or change the content of the information.

The request must be fulfilled as soon as possible and in any event within one month of receipt of the request. This can be extended by two further months where necessary, taking into account the complexity and number of the request. The data subject then has to be informed about the reason for the delay. The controller must implement necessary measures to deal with requests as soon as possible and adapt these measures to the circumstances of the processing. Where data is stored only for a very short period, there must be measures to guarantee that a request for access can be fulfilled without the data being erased while the request is being dealt with. Where a large quantityof data is processed, the controller will have to put in place routines and mechanisms that are adapted to the complexity of the processing.

The assessment of the request should reflect the situation at the moment when the request was received by the controller. Even data that may be incorrect or unlawfully processed will have to be provided. Data that has already been deleted, for example in accordance with a retention policy, and therefore is no longer available to the controller cannot be provided.

Limits and restrictions

The GDPR allows for certain limitations of the right of access. There are no further exemptions or derogations. 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 subject´s request.

According to Art. 15(4) the right to obtain a copy shall not adversely affect the rights and freedoms of others. The EDPB is of the opinion that these rights must be taken into consideration not only when granting access by providing a copy, but also, if access to data is provided by other means (on-site access for example). Art. 15(4) is not, however, applicable to the additional information on the processing as stated in Art. 15(1) lit. a.-h. The controller must be able to demonstrate that the rights or freedoms of others would be adversely affected in the concrete situation. Applying Art. 15(4) should not result in refusing the data subject's request altogether; it would only result in leaving out or rendering illegible those parts that may have negative effects for the rights and freedoms of others.

Art. 12(5) GDPR allows controllers to reject requests that are manifestly unfounded or excessive, or to charge a reasonable fee for such requests. These concepts have to be interpreted narrowly. Since there are very few prerequisites regarding access requests, the scope of considering a request as manifestly unfounded is rather limited. Excessive requests depend on the specifics of the sector in which the controller operates. The more often changes occur in the controller's data base, the more often the data subject may be permitted to request access without it being excessive. Instead of refusing access, the controller may decide to charge a fee from the data subject. This would only be relevant in the case of excessive requests in order to cover the administrative costs that such requests may cause. The controller must be able to demonstrate the manifestly unfounded or excessive character of a request.

Restrictions of the right of access may also exist in Member States' national law as per Art. 23 GDPR and the derogations therein. Controllers who intend to rely on such restrictions must carefully check the requirements of the national provisions and take note of any specific conditions that may apply. Such conditions may be that the right of access is only temporarily delayed or that the restriction only applies to certain categories of data.

Table of contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a dedicated stakeholders event on data subject rights, in order to identify the challenges and interpretation issues faced in the application of the relevant provisions of the GDPR;

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION - GENERAL OBSERVATIONS

1. In today´s society, personal data are processed by public and private entities, during many activities, for a wide array of purposes and in many different ways. Individuals may often be in a disadvantaged position in terms of understanding how their personal data are processed, including the technology used in the particular case, whether it is by a private or a public entity. In order to protect personal data of natural persons in these situations, the GDPR has created a coherent and robust legal framework, generally applicable with regard to different types of processing, including specific provisions relating to data subject rights.

2. The right of access to personal data is one of the data subjects' rights provided for in Chapter III of the GDPR among other rights, such as for instance the right to rectification and erasure, the right to restriction of processing, the right to portability, the right to object or the right of not being subject to automated individual decision making, including profiling[2]. The right of access by the data subject is enshrined both in the Charter of Fundamental Rights of the EU (the Charter)[3] and in Art. 15 GDPR, where it is precisely formulated as the right of access to personal data and to other related information.

3. Under the GDPR, the right of access consists of three components i.e. confirmation of whether or not personal data are processed, access to it, and information about the processing itself. The data subject can also obtain a copy of the processed personal data, whereas this possibility is not an additional data subject right but the modality of providing access to the data. Thus, the right of access can be understood both as the possibility of the data subject to ask the controller if personal data about him or her are processed and as the possibility to access and to verify these data. The controller shall

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] Art. 15 - 22 GDPR.
[3] Under Art. 8 para. 1 of the Charter of Fundamental Rights of the European Union Everyone has the right to the protection of personal data concerning him or her. Under Art. 8 para. 2 sentence 2 Everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified.

provide to the data subject, on the basis of his/her request, the information falling within the scope of Art. 15(1) and (2) GDPR.

4. The exercise of the right of access is realised both in the framework of data protection law, in accordance with the objectives of data protection law, and more specifically, in the framework of "*fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*", as put forward by Art. 1(2) GDPR. The right of access is an important element of the whole data protection system.

5. The practical aim of the right of access is to enable the natural persons to have the control over their own personal data[4]. In order to realise this goal effectively in practice, the GDPR is aiming to facilitate this exercise by number of guarantees enabling the data subject to exercise this right easily, without unnecessary constraints, at reasonable intervals and without excessive delay or expense. All this should lead to more effective enforcement of the right of access by data subject in the digital age, part of which in a broader sense is also the data subject's right to file a complaint to the supervisory authority and the right to effective judicial protection[5].

6. With regards to the development of the right of access, as part of the data protection legal framework, it should be stressed that it has been an element of the European data protection system from its beginning. In comparison with Directive 95/46/EC, the standard of the data subject rights set out in the GDPR has been both refined and strengthened; this also applies to the right of access. As the modalities of the right of access are now specified more precisely in the GDPR, this right is also more instructive from the point of legal certainty for both the data subject and the controller. Besides, the specific wording of Art. 15, and the precise deadline for the provision of data under Art. 12(3) GDPR, obliges the controller to be prepared for data subject inquiries by developing procedures for handling requests.

7. The right of access should not be seen in isolation as it is closely linked with other provisions of the GDPR, in particular with data protection principles including the fairness and lawfulness of processing, the controller´s transparency obligation and with other data subject rights provided for in Chapter III of the GDPR.

8. In the framework of data subject rights, it is also important both to stress the significance of Art. 12 GDPR, which lays down requirements for appropriate measures adopted by the controller in providing the information referred to in Art. 13 and 14 GDPR, and the communications referred to in Art. 15-22 and 34 GDPR; these requirements generally specify the form, manner and time limit for the responses to the data subject, and in particular for any information addressed to the child.

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. More particularly, the section hereafter is meant to give a general overview and explanation of the content of the Art. 15 itself whereas the subsequent sections provide deeper analysis of the most frequent practical questions and issues concerning the implementation of the right of access.

[4] See recitals 7, 68, 75 and 85 of the GDPR

[5] See Chapter VIII Articles 77, 78 and 79 of the GDPR

2 AIM OF THE RIGHT OF ACCESS, STRUCTURE OF ARTICLE 15 GDPR AND GENERAL PRINCIPLES

2.1 Aim of the right of access

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*"[6]. More specifically, the purpose of the right of access is to make it possible for the data subjects to understand how their personal data are 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. In other words, the purpose of the right of access is to provide individuals with sufficient, transparent and easily accessible information about data processing, regardless of the technologies used, and to enable them to verify different aspects of a particular processing activity under the GDPR (e.g. lawfulness, accuracy).

11. The interpretation of the GDPR provided in these guidelines is based on the CJEU case law which has been rendered so far. Taking into account the importance of the right of access, related case law can be expected to evolve significantly in future.

12. In accordance with CJEU decisions[7], the right of access serves the purpose of guaranteeing the protection of the data subjects' right to privacy and data protection with regard to the processing of data relating to them [8] and may facilitate the exercise of their rights flowing from, for example, Art. 16 to 19, 21 to 22 and 82 GDPR. However, the exercise of the right of access is an individual's right and not conditional upon the exercise of those other rights and the exercise of the other rights does not depend on the exercise of the right of access.

13. Given the broad aim of the right of access, the aim of the right of access is not suitable to be analysed as a precondition for the exercise of the right of access by the controller as part of its assessment of access requests. Thus, controllers should not assess "why" the data subject is requesting access, but only "what" the data subject is requesting (see section 3 on the analysis of the request) and whether they hold personal data relating to that individual (see section 4). Therefore, for example, the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller.[9] Regarding limits and restrictions of the right of access, please see section 6.

Example 1: An employer dismissed an individual. One week later, the individual decides to collect evidence to file an unfair dismissal lawsuit against this former employer. With that in mind, the individual writes to the former employer requesting access to all personal data relating to him or her, as data subject, that the former employer, as controller, processes.

The controller shall not assess the intention of the data subject, and the data subject does not need to provide the controller with the reason for the request. Therefore, if the request fulfils all other requirements (see section 3), the controller needs to comply with the request, unless the request

[6] Recital 63 GDPR.
[7] CJEU, C-434/16, Nowak, and joined cases C-141/12 and C-372/12, YS and Others.
[8] CJEU, C-434/16, Nowak, para. 56.
[9] Questions related to this topic are at issue in a case currently pending before the CJEU (C-307/22).

proves to be manifestly unfounded or excessive in accordance with Art. 12 (5) of the GDPR (see section 6.3), which the controller is required to demonstrate.

Variation: The data subject exercises the right of access with regard to the personal data relating to him or her during the course of the lawsuit. However, the national law of the Member State, which governs the employment relation between the controller and the data subject, contains certain provisions that limit the scope of information to be provided to or exchanged between parties to ongoing or prospective legal proceedings, which are applicable to the unfair dismissal lawsuit that the data subject filed. In this context and provided that, these national provisions comply with the requirements posed by Art. 23 GDPR[10], the data subject is not entitled to receive more information from the controller than is prescribed by the national law provisions of the Member State governing the information exchange between parties to legal disputes.

14. Although the aim of the right of access is broad, the CJEU illustrated also the limits of the remit of data protection law and the right of access. For instance, the CJEU found that the objective of the right of access guaranteed by EU data protection law is to be distinguished from that of the right of access to public documents established by EU and national legislation, the latter aiming at, "the greatest possible transparency of the decision-making process of the public authorities and to promote good administrative practices"[11], an objective not sought by data protection law. The CJEU concluded that the right of access to personal data applies irrespective of whether a different kind of right of access with a different aim applies, such as in the context of an examination procedure.

2.2 Structure of Article 15 GDPR

15. In order to reply to a request for access and to ensure that none of its aspects might be disregarded, it is necessary first to understand the structure of Art. 15 and the constituent components of the right of access stipulated in this Article.

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

1.	Confirmation as to whether or not the controller is processing personal data concerning the requesting person	Art. 15(1), first half of the sentence
2.	Access to the personal data concerning the requesting person	Art. 15(1), second half of the sentence (first part)
3.	Access to the following information on the processing: (a) the purposes of the processing; (b) the categories of personal data; (c) the recipients or categories of recipients; (d) the envisaged duration of the processing or the criteria for determining the duration; (e) the existence of the rights to rectification, erasure, restriction of processing and objection to processing; (f) the right to lodge a complaint with a supervisory authority; (g) any available information on the source of the data, if not collected from the data subject;	Art. 15(1), second half of the sentence (second part)

[10] EDPB Guidelines 10/2020 on restrictions under article 23 GDPR, version for public consultation, 18 December 2020.
[11] CJEU, Joined cases C-141/12 and C-372/12, YS and Others, para. 47.

	(h) the existence of automated decision-making, including profiling and other information relating thereto.	
4.	Information on safeguards pursuant to Art. 46 where the personal data are transferred to a third country or to an international organisation	Art. 15(2)
5.	The obligation of the controller to provide a copy of the personal data undergoing processing	Art. 15(3), first sentence
6.	Charging of a reasonable fee by the controller based on administrative costs for any further copies requested by the data subject	Art.15(3), second sentence
7.	Provision of information in electronic form	Art. 15(3), third sentence
8.	Taking into account the rights and freedoms of others	Art. 15(4)

While all elements of Art. 15(1) and (2) together define the content of the right of access, Art.15(3) deals with the modalities of access, in addition to the general requirements set out in Art. 12 GDPR. Art. 15(4) supplements the limits and restrictions that Art. 12(5) GDPR provides for all data subjects' rights with a specific focus on rights and freedoms of others in the context of access.

2.2.1 Defining the content of the right of access

17. Art. 15(1) and (2) contain the following three aspects: first, the confirmation whether personal data of the requesting person are being processed, if yes, second, access to those data, and, third, information on the processing. They can be regarded as three different components which together build the right of access.

2.2.1.1 Confirmation as to 'whether' or not personal data are being processed

18. When making a request for access to personal data, the first thing that the data subjects need to know is whether or not the controller processes data concerning them. Consequently, this information constitutes the first component of the right of access under Art. 15(1). Where the controller does not process personal data relating to the data subject requesting the access, the information to be provided would be limited to confirming that no personal data relating to the data subject are being processed. Where the controller does process data relating to the requesting person, the controller must confirm this fact to this person. This confirmation may be communicated separately, or it may be encompassed as part of the information on the personal data being processed (see below).

2.2.1.2 Access to the personal data being processed

19. Access to personal data is the second component of the right of access under Art. 15(1) and it constitutes the core of this right. It relates to the notion of personal data as defined by Art. 4(1) GDPR. Aside from basic personal data like name and address, an unlimited variety of data may fall within this definition, provided that they fall under the material scope of the GDPR, notably with regards to the way in which there are processed (Art. 2 GDPR). Access to personal data hereby means access to the actual personal data themselves, not only a general description of the data nor a mere reference to the categories of personal data processed by the controller. If no limits or restrictions apply[12], data subjects are entitled to have access to all data processed relating to them, or to parts of the data,

[12] See section 6 of these Guidelines.

depending on the scope of the request (see sec. 2.3.1). 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 scope of personal data under Art. 15 is explained in detail in sec. 4.1 and 4.2.

2.2.1.3 Information on the processing and on data subject rights

20. The third component of the right of access is the information on the processing and on data subjects' 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 controller[13] 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's request. The content and degree of specification of the information is further elaborated in section 4.3.

2.2.2 Provisions on Modalities

21. Art. 15(3) supplements the requirements for the modalities of the reply to access requests laid down in Art. 12 GDPR by some specifications in context of access requests.

2.2.2.1 Providing a copy

22. Under the first sentence of Art. 15(3) GDPR, the controller shall provide a free copy of the personal data which the processing relates to. The copy therefore refers only to the second component of the right of access («access to the personal data processed», see above). The controller must ensure that the first copy is free of charge, even where it considers the cost of reproduction to be high (example: the cost of providing a copy of the recording of a telephone conversation).

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 right of access to the data[14] 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. At the same time, the obligation to provide a copy is not designed to widen the scope of the right of access: it refers (only) to a copy of the personal data undergoing processing, not necessarily to a reproduction of the original documents (see section 5, para. 152). More generally speaking, there is no additional information to be given to the data subject upon providing a copy: the scope of the information to be contained in the copy is the scope of the access to the data under 15(1) (second component of the right of access as referred to above, see para. 19), which includes all information necessary to enable the data subject to understand and verify the lawfulness of the processing.[15]

24. In light of the above, if access to the data in the sense of Art. 15(1) is given by providing a copy, the obligation to provide a copy mentioned under 15(3) is complied with. The obligation to provide a copy serves the objectives of the right of access to allow the data subject to be aware of, and verify the lawfulness of the processing (Recital 63). To achieve these objectives, the data subject will in most

[13] See for information on this Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB").
[14] The obligation to provide a copy was not mentioned in the Data Protection Directive 95/46/EC.
[15] Questions related to the topic of this paragraph are at issue in a case currently pending before the CJEU (C-487/21

cases need to see the information not only temporarily. Therefore, the data subject will need to get access to the information by receiving a copy of the personal data.

25. In view of the above, the notion of a copy has to be interpreted in a broad sense and includes the different kinds of access to personal data as long as it is complete (i.e. it includes all personal data requested) and possible for the data subject to keep. Thus, the requirement to provide a copy means, that the information on the personal data concerning the person who makes the request is provided to the data subject in a way which allows the data subject to retain all of the information and to come back to it.

26. In spite of this broad understanding of a copy, and regarding that it is the main modality by which access should be provided, under some circumstances other modalities could be appropriate. Further explanations on copies and other modalities of providing access are given in section 5, in particular 5.2.2 - 5.2.5.

2.2.2.2 Providing further copies

27. Art. 15(3), second sentence concerns situations where the data subject asks the controller for more than one copy, for example in case the first copy was lost or damaged or the data subject wants to pass on a copy to another person or a Supervisory Authority. On the basis that further copies must be provided by the controller upon request of the data subject, Art. 15(3) rules, that for any further copy requested, the controller may charge a reasonable fee based on administrative costs (Art. 15(3) second sentence).

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) second sentence, in which case a fee for an additional copy may be charged. The response to these questions depends solely on the content of the request: the request should be interpreted as asking for an additional copy, insofar as, in terms of time and scope, it concerns the same processing of personal data as the former request. If, however, the data subject aims to get information on the data processed at a different point in time or relating to a different set of data from the one initially requested, the right to obtain a free copy according to Art. 15(3), applies once again. This also is valid in cases where the data subject has made a first request shortly beforehand. A data subject may exercise its right of access through a subsequent request and obtain a free copy, unless the request is regarded as excessive under Art. 12(5) with the possibility of charging a reasonable fee in accordance with Art. 12(5)(a) (on excessive character of repetitive requests, see section 6).

Example 2: A customer submits an access request to a trading company. One year after the reply of the company, the same customer makes a request for access under Art. 15 to the same company. Irrespective of whether there have been new business transactions or other contacts between the parties since the previous request, this second request is to be regarded as a new request. Even if no change in the data processing by the company occurred– which is not necessarily apparent to the data subject – the data subject has the right to get a free copy of the data.

Variation 1: Even if the customer in the above cases places the new request for example only one week after the first request, this may well be regarded as a new request under Art. 15(1) and (3), first sentence, if it is not to be interpreted as a mere reminder of the first request. Regarding the short interval and depending on the specific circumstances of the new request, its excessiveness according to Art. 12(5) is at issue (see section 6).

Variation 2: The request for a "new copy" of the information that had already been given in form of a copy in response to a previous request, for example in case that the customer lost the copy previously received, should, as a matter of course, be regarded as a request for an additional copy as it refers to the previous request in scope and time of the processing.

29. If the data subject repeats a first request for access on the grounds that the answer received was not complete or that no reasons had been given for the refusal, this request is not to be regarded as a new request, since it is merely a reminder of a first unsatisfied request.

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. This means, that the administrative costs are a relevant criterion for fixing the level of the fee. At the same time, the fee should be appropriate, taking into account the importance of the right of access as a fundamental right of the data subject. The controller should not pass on overhead costs or other general expenses to the data subject, but should focus on the specific costs that where caused by providing the additional copy. When organising this process the controller should deploy its human and material resources efficiently in order to keep the costs of the copy low, including if the controller involves external support.

31. In case the controller decides to charge a fee, the controller should indicate in advance that a fee will be charged and – as accurately as is possible - the amount of costs it is planning to charge to the data subject in order to give the data subject the possibility to determine whether to maintain or to withdraw the request.

2.2.2.3 Making the information available in a commonly used electronic form

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) GDPR). Art. 15(3), third sentence, complements this requirement in the context of access requests by stating, that the controller is in addition obliged to provide the answer in a commonly used electronic form, unless otherwise requested by the data subject. Art. 15(3) presupposes, that for controllers who are able to receive electronic requests it will be possible to provide the reply to the request in a commonly used electronic form (for details see sec. 5.2.5). This provision refers to all the information that needs to be provided in accordance with Art. 15(1) and (2). Therefore, if the data subject submits the request for access by electronic means, all information must be provided in a commonly used electronic form. Questions of format are further developed in section 5. The controller should, as always, deploy appropriate security measures, in particular when dealing with special category of personal data (see below, under 2.3.4).

2.2.3 Possible limitation of the right of access

33. Finally, in context of the right of access, a specific limitation is foreseen in Art. 15(4). It states, that possible adverse effects on the rights and freedoms of others have to be considered. Questions as to the scope and the consequences of this limitation as well as to additional limits and restrictions set forth in Art. 12(5) GDPR or under Art. 23 GDPR are explained in section 6.

2.3 General principles of the right of access

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. Accordingly, where the controller processes data relating to the data subject, the controller shall provide all the information referred to in Art. 15(1)

and, where applicable, the information referred to in Art. 15(2). The controller has to take the appropriate measures to ensure that the information is complete, correct and up-to-date, corresponding as close as possible to the state of data processing at the time of receiving the request[16]. Where two or more controllers process data jointly, the arrangement of the joint controllers regarding their respective responsibilities with regards to the exercise of data subject's rights, especially concerning the answer to access requests, does not affect the rights of the data subjects towards the controller to whom they address their request[17].

2.3.1 Completeness of the information

35. Data subjects have the right to obtain, with the exceptions mentioned below, full disclosure of all data relating to them (for details on the scope, see section 4.2). 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[18]. Limiting access to part of the information may be considered in the following cases:

a) The data subject has explicitly limited the request to a subset. In order to avoid providing incomplete information, the controller may consider this limitation of the data subject's request only if it can be certain that this interpretation corresponds to the wish of the data subject (for further details, see section 3.1.1, para. 51). In principle, the data subject shall not have to repeat the request for the transmission of all the data the data subject is entitled to obtain.

b) In situations where the controller processes a large quantity of data concerning the data subject, the controller may have doubts if a request of access, that is expressed in very general terms, really aims at receiving information on all kind of data being processed or on all branches of activity of the controller in detail. These may arise in particular in situations, where there was no possibility to provide the data subject with tools to specify their request from the beginning or where the data subject did not make use of them. The controller then faces problems of how to give a full answer while simultaneously avoiding the creation of an overflow of information for the data subject that the data subject is not interested in and cannot effectively handle. There may be ways to solve this problem, depending on the circumstances and the technical possibilities, for example by providing self-service tools in online contexts (see section 5 on the layered approach). If such solutions are not applicable, a controller who processes a large quantity of information relating to the data subject may request the data subject to specify the information or processing to which the request relates before the information is delivered (see Recital 63 GDPR). Examples of this may include a company with several fields of activity or a public authority with different administrative units, if the controller found that numerous data relating to the data subject are processed in those branches. In addition, a large quantity of data may be processed by controllers who collect data regarding frequent activities of the data subject over a prolonged time period.

Example 3: A public authority processes data on the data subject in a number of different departments concerning various contexts. File management and file keeping are partly processed by non-automated means and most of the data is only stored in paper files. Regarding the general wording of the request, the public authority doubts whether the data subject is aware of the extent

[16] For guidance on appropriate measures see sec. 5 para. 123 - 129

[17] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, par. 162f.. Processors have to assist the controller, ibd., para. 129.

[18] For details please see section 5.2.3 below on the topic of layered approach.

of the request, especially the variety of processing operations that it would encompass, the amount of information and the number of pages that the data subject would receive.

Example 4: A big insurance company receives a general access request by letter from a person who has been a customer for many years. Even though deletion periods are fully respected, the company actually processes a vast amount of data concerning the customer, because processing is still necessary to fulfil contractual obligations arising from the contractual relationship with the customer (including for example continuing obligations, communication on controversial issues with the customer and with third parties, …) or to comply with legal obligations (archived data that have to be stored for tax purposes, etc.). The insurance company may have doubts as to whether the request, that was made in very general terms, is really intended to encompass all kinds of those data. This may be especially problematic if the insurance company only has a postal address of the data subject and therefore has to send any information on paper. However, the same doubts may be relevant also when providing the information by other means.

If, in such cases, the controller decides to ask the data subject to specify the request, in order to fulfil its obligation to facilitate the exercise of the right of access (Art. 12(2) GDPR) the controller shall at the same time give meaningful information about its processing operations that could concern the data subject, by informing about relevant branches of its activities, databases etc.

Example 5: In an employment relationship, in case of a generally formulated request for access, it is not *per se* clear that the employee wants to receive all user-login data, data on access to a workplace, data on settlements in the canteen, data on salary payments, etc. A request for specification made by the employer could for example lead to the clarification, that the employee's interest is to understand or verify to whom his performance assessment has been passed on. Without request for specification, the employee would receive a large quantity of information, without having an interest in most of the data. At the same time, the employer would need to give information on the different contexts of processing which could concern the employee in order to allow the employee to specify the request sensibly.

It is important to underline that the request for specification shall not aim at a limitation of the reply to the access request and shall not be used to hide any information on the data or the processing concerning the data subject. If the data subject, who has been asked to specify the scope of its request, confirms to seek all personal data concerning him or her, the controller of course has to provide it in full.

In any case, the controller should always be able to demonstrate, that the way to handle the request aims to give the broadest effect to the right of access and that it is in line with its obligation to facilitate the exercise of data subjects rights (Art. 12(2) GDPR). Subject to these principles, the controller may await the answer of the data subject before providing additional data according to the data subject's wish, if the controller has provided the data subject with a clear overview of all processing operations that could concern the data subject, including especially those that the data subject might not have expected, if the controller has also given access to all data that the data subject clearly aimed for, and if, furthermore, this information has been combined with clear indication of how to get access to the remaining parts of the processed data.

c) Exceptions or restrictions to the right of access apply (see below in section 6). In such cases, the controller should carefully check to which parts of the information the exception relates to and provide all information that is not excluded by the exception. For example, confirmation of the processing of personal data itself (component 1) may not be affected by the exception. As a result, information has

to be provided about all the personal data and all the information referred to in Art. 15(1) and (2) that are not concerned by the exception or the restriction.

2.3.2 Correctness of the information

36. The information included in the copy of the personal data given to the data subject has to comprise the actual information or personal data held about the data subject. This includes the obligation to give information about data that are inaccurate or about data processing which is not or no longer lawful. The data subject may for example use the right of access to find out about the source of inaccurate data being circulated between different controllers. If the controller corrected inaccurate data before informing the data subject about it, the data subject would be deprived of this possibility. The same applies in case of unlawful processing. The possibility to know about unlawful processing concerning the data subject is one of the main purposes of the right of access. The obligation to inform about the unchanged state of processing is without prejudice to the obligation of the controller to end unlawful processing or to correct inaccurate data. Questions about the order in which those obligations should be fulfilled, are answered in the following.

2.3.3 Time reference point of the assessment

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. This means that the controller has to try to find out about all the data processing activities relating to the data subject without undue delay. Controllers are thus not required to provide personal data, which they processed in the past but which they no longer have at their disposal[19]. For instance, the controller may have deleted personal data in accordance with its data retention policy and/or statutory provisions and may thus no longer be able to provide the requested personal data. In this context, it should be recalled that the length of time for which the data are stored should be fixed in accordance with Art. 5(1)(e) GDPR, as any retention of data must be objectively justifiable.

38. At the same time, the controller shall implement in advance the necessary measures in order to facilitate the exercise of the right of access and to deal with such requests as soon as possible (see Art. 12(3)) and before the data will have to be deleted. Therefore, in the case of short retention periods, the measures taken to answer the request should be adapted to the appropriate retention period in order to facilitate the exercise of the right of access and to avoid the permanent impossibility of providing access to the data processed at the moment of the request[20]. In some cases it may nevertheless not be possible to reply to a request before the time the data are scheduled for deletion. For example, if in course of replying to a request as promptly as possible, a controller retrieves personal data that were scheduled to be deleted the following day, the controller may need some additional time to consider whether redactions need to be made to protect the freedoms of others before releasing a copy of the personal data to the requester. If the data have been retrieved within the

[19] See, to that effect, further clarifications in section 4 of these guidelines, as well as in Court of Justice of the European Union, C-553/07, 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* on a right of access to information on the recipients or categories of recipients in respect of the past.
[20] For example, the implementation of a self-service tool enabling the data subject to easily access the requested personal data and a notification system alerting the controller about a request that relates to personal data with short retention periods could be considered in order to facilitate prompt action.

scheduled retention period, the controller may continue to process those data for the purpose to fulfill its obligation to answer the request. Processing in such cases may be based on Art. 6(1)(c) in combination with Article 15 GDPR and its duration has to comply with the requirements of Art. 12(3) GDPR[21]. The application of this legal basis is limited to processing of the data identified to be necessary for answering the concrete request and is not to be used as a justification for general extentions of retention periods.

39. Furthermore, the controller shall not deliberately escape the obligation to provide the requested personal data by erasing or modifying personal data in response to a request for access (see 2.3.2). If, in the course of processing the access request, the controller discovers inaccurate data or unlawful processing, the controller has to assess the state of the processing and to inform the data subject accordingly before complying with its other obligations. In its own interest, to avoid the need of further communication on this as well as to be compliant with the transparency principle, the controller should add information about the subsequent rectifications or deletions.

> **Example 6**: On the occasion of replying to an access request a controller realises, that an application of the data subject for a vacancy in the company of the controller has been stored beyond the retention period. In this case the controller cannot delete first and then reply to the data subject that no data (concerning the application) is processed. It has to give access first and delete the data afterwards. In order to prevent a subsequent request for erasure it would then be recommended to add information about the fact and time of the deletion.

In order to comply with the principle of transparency, controllers should infom the data subject as of the specific point in time of the processing to which the response of the controller refers. In some cases, for example in contexts of frequent communication activities, additional processing or modifications of the data may occur between this time reference point, at which the processing was assessed, and the response of the controller. If the controller is aware of such changes, it is recommended to include information about those changes as well as information about additional processing necessary to reply to the request.

2.3.4 Compliance with data security requirements

40. Since communicating and making available personal data to the data subject is a processing operation, the controller is always obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing (see Art. 5(1)(f), 24 and 32 GDPR). This applies independently of the modality in which access is provided. In case of non-electronic transmission of the data to the data subject, depending on the risks that are presented by the processing, the controller may consider using registered mail or, alternatively, to offer, but not oblige, the data subject to collect the file against signature directly from one of the controller's establishments. If, in line with Art. 12(1) and (3), information is provided by electronic means, the controller shall choose electronic means that comply with data security requirements. Also in case of providing a copy of the data in a commonly used electronic form (see Art. 15(3)), the controller shall take into account data security requirements when choosing the means of how to transmit the electronic file to the data subject. This may include applying encryption, password protection etc. In order to facilitate access to the encrypted data, the controller should also ensure that appropriate information is made available so that the data subject can access the decrypted information. In cases

[21] This is without prejudice to subsequent processing of data for evidence purposes in connection with the handling of the access request for an appropriate period of time.

where data security requirements would necessitate end-to-end encryption of electronic mails but the controller would only be able to send a normal e-mail, the controller will have to use other means, such as sending a USB-stick by (registered) letter post to the data subject.

3 GENERAL CONSIDERATIONS REGARDING THE ASSESSMENT OF ACCESS REQUESTS

3.1 Introduction

41. When receiving requests for access to personal data, the controller must assess each request individually. The controller shall take into consideration, *inter alia*, the following issues, further developed in the following paragraphs: whether the request concerns personal data linked to the requesting person and who the requesting person is. This section aims to clarify what elements of the request for access the controller should take into account when carrying out its assessment and to discuss possible scenarios for such an assessment as well as its consequences. The controller, when assessing a request for access to personal data, shall also take into account, pursuant to Art. 12(2) GDPR, the obligation to facilitate the exercise of the data subject rights, while keeping in mind the appropriate security of the personal data[22].

42. Therefore, the controllers should be proactively ready to handle the requests for access to personal data. This means that the controller should be prepared to receive the request, assess it properly (this assessment is the subject of this section of the guidelines) and provide an appropriate reply without undue delay to the requesting person. The way the controllers will prepare themselves for the exercise of access requests should be adequate and proportionate and depend on the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons, in accordance with Art. 24 GDPR. Depending on the particular circumstances, the controllers may, for example, be required to implement an appropriate procedure, the implementation of which should guarantee the security of the data without hindering the exercise of the data subject's rights.

3.1.1 Analysis of the content of the request

43. This issue can be more specifically assessed by asking the following questions.

a) <u>Does the request concern personal data?</u>

44. Under the GDPR, the scope of the request shall only cover personal data[23]. 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. Additionally, a request for information about anonymous data or data that

[22] The controller shall ensure appropriate security of the personal data, in accordance with the integrity and confidentiality principle (Art. 5(1)(f) GDPR), by implementing appropriate technical and organisational measures, as referred to in Art. 32 GDPR and elaborated in Art. 24 GDPR. The controller shall be able to demonstrate that it ensures an adequate level of data protection, in line with the accountability principle (see also: Art. 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 00062/10/EN WP 173 and EDPB Guidelines nr 07/2020 on the concepts of controller and processor in the GDPR).

[23] Unless the request covers also non-personal data inextricably linked to the personal data of the data subject. For further explanations see para 100.

does not concern the requesting person or the person on whose behalf the authorised person made the request, will not be within the scope of the right of access. This question will be analysed more in detail in section 4.

45. Unlike anonymous data (which are not personal data), pseudonymised data, which could be attributed to a natural person by the use of additional information, are personal data[24]. Thus, pseudonymised data that can be linked to a data subject - e.g. when the data subject provides the respective identifier allowing their identification, or when the controller is able to connect the data to the requesting person by its own means - are to be considered within the scope of the request[25].

b) Does the request relate to the requesting person (or the person on whose behalf the authorised person makes the request)?

46. As a general rule, a request may only concern the data of the person making the request. Access to other people's data can only be requested subject to appropriate authorisation[26].

Example 7: Data subject X works as a department manager for a company that provides parking spaces for its managers at a company car park. Although data subject X has a permanent parking space, when the data subject arrives at the office for their second shift, this space is often already occupied by another car. Since this situation is repetitive, in order to identify the driver who unauthorised occupies its slot, the data subject asks the controller of the video surveillance system covering the office's parking lot area, for access to the personal data of this driver. In such a case, data subject X's request will not be a request for access to their personal data, as the request does not concern the requesting person'sdata, but the data of another person - and therefore it should not be considered a request under Art. 15 GDPR.

c) Do provisions, other than the GDPR, regulating access to a certain category of data apply?

47. Data subjects are not required to specify the legal basis in their request. However, if the data subjects clarify that their request is based on sectoral legislation or on national legislation regulating the specific issue of access to certain categories of data, and not on the GDPR, such a request shall be examined by the controller in accordance with such sectoral or national rules, where applicable. Often, depending on the relevant national legislation, controllers may be required to provide separate replies, each dealing with the specific requirements set out by the different legislative acts. This is not to be confused with national or EU legislation setting out restrictions on the right of access which needs to be complied with when answering access requests.

48. If the controller has doubts as to which right the data subject wishes to exercise, it is recommended to ask the data subject making the request to explain the subject matter of the request. Such correspondence with the data subject shall not affect the duty of the controller to act without undue delay[27]. However, in case of doubts, if the controller asks the data subject for further explanation and receives no response, bearing in mind the obligation to facilitate the exercise of the person's right of access, the controller should interpret the information contained in the first request and act on this basis. In accordance with the accountability principle, the controller may determine an appropriate

[24] See Recital 26 GDPR. Further explanations on the concepts of anonymous data and pseudonymised data can be found in WP29 Opinion 4/2007 on the concept of personal data, p. 18-21.
[25] Art. 29 Working Party, WP242 rev.01, 5 April 2017, Guidelines on the right to data portability - endorsed by the EDPB (hereinafter "WP29 Guidelines on the right to data portability - endorsed by the EDPB"), p. 9.
[26] See section 3.4 ("Requests made via third parties/proxies").
[27] See further guidance on the timing in section 5.3.

timeframe during which the data subject may provide further explanation. When fixing such timeframe, the controller should leave enough time to comply with the request after it elapsed and therefore consider how much time is objectively necessary to compile and provide the requested data once the specification was provided (or not) by the data subject.

49. If the request is in the scope of the GDPR, the existence of such specific legislation does not override the general application of the right of access, as provided by the GDPR. There might be restrictions set out by EU or national law, when allowed by Art. 23 GDPR (see section 6.4).

d) Does the request fall within the scope of Article 15?

50. It should be noted that the GDPR does not introduce any formal requirements for persons requesting access to data. In order to make the access request, it is sufficient for the requesting persons to specify that they want to know what personal data concerning them the controller processes. Therefore, the controller cannot refuse to provide the data by referring to the lack of indication of the legal basis of the request, especially to the lack of a specific reference to the right of access or to the GDPR.

For example, in order to make a request, it would be sufficient for the requesting person to indicate that:

- they wish to obtain access to the personal data concerning them;
- they are exercising their right of access; or
- they wish to know the information concerning them that the controller processes.

It should be borne in mind that applicants may not be familiar with the intricacies of the GDPR and that it is advisable to be lenient towards persons exercising their right of access, in particular when it is exercised by minors. As indicated above, 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.

e) Do the data subjects want to access all or parts of the information processed about them?

51. Additionally, the controller needs to assess whether the requests made by the requesting persons refer to all or parts of the information processed about them. Any limitation of the scope of a request to a specific provision of Art. 15 GDPR, made by the data subjects, must be clear and unambiguous. For example, if the data subjects require verbatim "information about the data processed in relation to them", the controller should assume that the data subjects intend to exercise their full right under Art. 15(1) – (2) GDPR. Such a request should not be interpreted as meaning that the data subjects wish to receive only the categories of personal data that are being processed and to waive their right to receive the information listed in Art. 15(1)(a) to (h). This would be different, for example, where the data subjects wish, with regard to data which they specify, to have access to the source or origin of the personal data or to the specified period of storage. In such a case the controller may limit its reply to the specific information requested.

3.1.2 Form of the request

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. Therefore, there are, in principle, no requirements under the GDPR that the data subjects must observe when choosing a communication channel through which they enter into contact with the controller.

53. The EDPB encourages controllers to provide the most appropriate and user-friendly communication channels, in line with Art. 12(2) and Art. 25 GDPR, to enable the data subject to make an effective request. Nevertheless, if a data subject makes a request using a communication channel provided by the controller[28], which is different from the one indicated as the preferable one, such request shall be, in general, considered effective and the controller should handle such a request accordingly (see the examples below). The controllers should undertake all reasonable efforts to make sure that the exercise of data subject rights is facilitated (for example, when a data subject sends an access request to an employee who is on leave, an automatic message informing the data subject about an alternative communication channel for this request could be a reasonable effort).

54. It should be noted that the controller is not obliged to act on a request sent to a random or incorrect e-mail (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.

55. The controller is also not obliged to act on a request sent to the e-mail address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights (e.g. drivers, cleaning staff, etc.). Such requests shall not be considered effective, if the controller has clearly provided the data subject with appropriate communication channel. However, if the data subject sends a request to the controller's employee who has been assigned to them as their regular contact person (such as e.g. a personal account manager at a bank or a regular consultant at a mobile phone operator), such contact should not to be considered as a random one and the controller should make all reasonable efforts, to handle such a request so that it can be redirected to the contact point and answered within the time limits provided for by the GDPR.

56. Nevertheless, the EDPB recommends, as good practice, that controllers introduce appropriate mechanisms to facilitate the exercise of data subjects' rights, including autoresponder systems to inform of staff absences and appropriate alternate contact and, where possible, mechanisms to improve internal communication between employees on requests received by those who may not be competent to deal with such requests.

Example 8: Controller X provides, both on its website and in the privacy notice, two e-mail addresses - the general e-mail address of the controller: CONTACT@X.COM and the e-mail address of the controller's data protection contact point: QUERIES@X.COM. Additionally, controller X indicates on its website that in order to submit any inquiries or to make a request with regard to the processing of personal data, individuals should contact the data protection contact point by way of the e-mail address provided. However, the data subject sends a request to the controller's general e-mail address: CONTACT@X.COM.

In such a case, the controller should make all reasonable efforts, to make its services aware of the request, which was made through the general e-mail, so that it can be redirected to the data protection contact point and answered within the time limits provided for by the GDPR. Moreover, the controller is not entitled to extend the period for responding to a request, merely because the data subject has

[28] This may include, for example, communication data of the controller provided in its communications addressed directly to data subjects or contact data provided by the controller publicly, such as in the controller's privacy policy or other mandatory legal notices of the controller (e.g. owner or business contact information on a website).

sent a request to the controller's general e-mail address, not the controller's data protection contact point e-mail address.

Example 9: Controller Y runs a network of fitness clubs. Controller Y indicates on its website and in the privacy notice for clients of the fitness club that in order to submit any inquiries or to make a request with regard to the processing of personal data, individuals should contact the controller under the e-mail address: QUERIES@Y.COM. Nevertheless, the data subject sends a request to an e-mail address found in the changing room, where he found a notice that reads "If you are not satisfied with the cleanliness of the room, please contact us at: CLEANERS@Y.COM", which is the e-mail address of the cleaning staff employed by Y. The cleaning staff are obviously not involved in handling matters concerning the exercise of the rights of data subjects - customers of the fitness club. Although the e-mail address was available on the premises of the fitness club, the data subject could not reasonably expect that this was an appropriate contact address for such requests, since the website and the privacy notice clearly informed about the communication channel to be used for the exercise of data subjects' rights.

57. Date of receipt of the request by the controller triggers, as a rule, the one month period for the controller to provide information on action taken on a request, in accordance with Art. 12(3) GDPR (further guidance on timing is provided in section 5.3). The EDPB considers as good practice for the controllers to confirm receipt of requests in writing, for example by sending e-mails (or information by post, if applicable) to the requesting persons confirming that their requests have been received and that the one month period runs from day X to day Y.

3.2 Identification and authentication

58. In order to ensure the security of processing and minimise the risk of unauthorised disclosure of personal data, the controller must be able to find out which data refer to the data subject (identification) and confirm the identity of that person (authentication).

59. It may be recalled that in situations in which the purpose for which the personal data are processed do not or no longer require the identification of a data subject, the controller does not need to maintain identification for the sole purpose of complying with data subjects' rights, also in light of the principle of data minimisation. These situations are dealt with in Art. 11(1) GDPR.

60. Art. 12(2) GDPR 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 processes personal data for a purpose that does not require the identification of the data subject and it demonstrates that it is not in a position to identify the data subject. In such circumstances, the data subject may, however, decide to provide additional information enabling this identification (Art. 11(2) GDPR)[29].

61. The controller is not obliged to acquire such additional information in order to identify the data subject for the sole purpose of complying with the data subject's request, also in light of the principle of data minimisation. However, it should not refuse to take such additional information provided by the data subject in order to support the exercise of his or her rights (Recital 57 GDPR).

Example 10: X is the controller of the data processed in connection with the video surveillance of a building. In accordance with Art. 11(1) GDPR, the controller is not obliged to identify all persons who

[29] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 13.

have been registered by a security camera as a part of the monitoring (purpose not requiring identification). The controller receives a request for access to the personal data from the person who claims that to have been recorded by the controller's video surveillance. The controller's actions will depend on the additional information provided. If the requesting person indicates a particular day and time when the cameras may have recorded the event in question, it is likely that the controller will be able to provide such data (Art. 11(2) GDPR). However, if the controller is not in a position to identify the data subject (e.g. if it is impossible for the controller to be certain that a requesting person is in fact the data subject or if the request concerns e.g. a long period of recordings and a controller is unable to process such a large quantity of data), the controller may refuse to take action if it demonstrates that it is not in the position to identify the data subject (Art. 12(2) GDPR).

Example 11: A controller C processes personal data for the purpose of addressing behavioral advertising to its web users. Personal data collected for behavioral advertising are usually collected by means of cookies and associated with pseudonymous random identifiers. A data subject Mr. X exercises his right of access with C via C's website. C is able to precisely identify Mr. X to show the data subject's behavioral advertising, by linking the terminal equipment of Mr. X to its advertising profile with the cookies dropped in the terminal. C should then also be able to precisely identify Mr. X to grant him access to his personal data, as a link between the data processed and the data subject can be found. Therefore, and taking into account the principles of the GDPR, the above example would not fall within the scope of Art. 11 GDPR. More precisely, in the above example, the purposes of C require the identification of the data subjects while Art. 11 GDPR addresses the situation of processing which does not require identification where a controller shall not be obliged to process additional data within the meaning of Art. 11(1) GDPR for the sole purpose of being able to comply with the GDPR. Consequently, in some cases, no additional data should be requested in order to exercise the rights of the data subject.

However, if Mr. X tries to exercise his access right by e-mail or by regular mail, then, in this context, C will have no other choice but to ask Mr. X to provide "additional information" (Art. 12(6) GDPR) in order to be able to identify the advertising profile associated with Mr. X. In this case, the additional information will be the cookie identifier stored in the terminal equipment of Mr. X.

62. In case of demonstrated impossibility to identify the data subject (Art. 11 GDPR), the controller needs to inform the data subject accordingly, if possible, since the controller shall respond to requests from the data subject without undue delay and give reasons where it does not intend to comply with such requests . This information needs to be provided only "if possible", as the controller may not be in a position to inform the data subjects if their identification is impossible.

63. Both where the processing does not require identification and where it requires it, 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) GDPR).

64. The GDPR does not impose any requirements on how to authenticate the data subject. However, Art. 11 and 12 GDPR indicate the conditions for the exercise of all the data subject rights, including the right of access to personal data.

65. It should be remembered that, as a rule, the controller cannot request more personal data than is necessary to enable this authentication, and that the use of such information should be strictly limited to fulfilling the data subjects' request.

66. Authentication procedures often already exist between the data subjects and the controllers. The controllers may use these authentication procedures in order to ascertain the identity of the data subjects requesting their personal data or exercising the rights granted by the GDPR[30]. Otherwise, controllers should implement an authentication procedure to do so[31].

67. In cases where the controller requests or is provided by the data subject with 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 (see section 3.3).

68. In order to allow the data subject to provide the additional information required to identify his or her data, the controller should inform the data subject of the nature of the additional information required to allow identification. Such additional information should not be more than the information initially needed for the authentication of the data subject. In general, the fact that the controller may request additional information to assess the data subject's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested[32].

69. 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[33].

Example 12: The data subject Ms. X requests access to her data while speaking to a helpline consultant of an electricity company with which she has concluded a contract. The consultant, having doubts as to the identity of the person making the request, generates in the company's system a one-time unique code sent to the user's mobile phone number, provided when the account was set up, as part of the double verification system, which action should be considered proportionate in this case.

3.3 Proportionality assessment regarding authentication of the requesting person

70. 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 authentication of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.

71. The controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data[34], and ensure security of the processing throughout the

[30] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.
[31] See further guidance regarding authentication in section 3.3.
[32] Ibid, p. 14.
[33] Ibid, p. 13-14.
[34] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.

process of handling an access requests in accordance with Art. 32 GDPR, including for instance a secure channel for the data subjects to provide additional information. The method used for authentication should be relevant, appropriate, proportionate and respect the data minimisation principle. If the controller imposes measures aimed at authentifying the data subject which are burdensome, it needs to adequately justify this and ensure compliance with all fundamental principles, including data minimisation and the obligation to facilitate the exercise of data subjects' rights (Art. 12(2) GDPR).

72. In an online context, the authentication mechanism may include the same credentials, used by the data subject to log-in to the online service offered by the controller (Recital 57 GDPR)[35].

73. 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, which in such cases should be sufficient to authenticate a data subject[36]. Furthermore, the data subjects are often already authenticated by the controller before entering into a contract or collecting their consent to the processing and, as a result, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate the data subject for access purposes[37]. Consequently, it is disproportionate to require a copy of an identity document in the event where the data subject making a request is already authenticated by the controller.

74. It should be emphasised that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and, as such, it should be considered inappropriate, unless it is necessary, suitable, and in line with national law. In such cases, the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that authentication by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.

75. Taking into account the fact, that many organisations (e.g. hotels, banks, car rentals) request copies of their clients' ID card, it should generally not be considered an appropriate way of authentication. Alternatively, the controller may implement a quick and effective security measure to identify a data subject based on the authentication it has previously carried out, e.g. via e-mail or text message containing confirmation links, security questions or confirmation codes[38].

76. Information on the ID that is not necessary for confirming the identity of the data subject, such as the access and serial-number, nationality, size, eye colour, photo and machine-readable zone, depending on a case by case assessment, may be redacted or hidden by the data subject before submitting it to the controller, except where national legislation requires a full unredacted copy of the identity card (see para. 78 below). Generally, the date of issue or expiry date, the issuing authority and the full name matching with the online account are sufficient for the controller to verify the identity, always provided

[35] See further guidance regarding authentication methods in the EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification, adopted on 14 January 2021, p. 30-31., and in the EDPBGuidelines 02/2021 on virtual voice assistants , Version 2.0, Adopted on 7 July 2021, section 3.7.

[36] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.

[37] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.

[38] See also Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC that has put forth different services that allow secure remote identification.

that the authenticity of the copy and the relation to the applicant are ensured. Additional information such as the birth date of the data subject may only be required in case the risk of mistaken identity persists, if the controller is able to compare it with the information it already processes.

77. 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 redact or hide those parts of the ID document. In such a case, if the data subject does not know how or is not able to redact such information, it is good practice for the controller to redact it upon receipt of the document, if this is possible for the controller, taking into account the means available to the controller in the given circumstances.

Example 13: The user Ms. Y has created a password protected account in the online store, providing her e-mail and/or username. Subsequently, the account owner asks the controller for information whether it processes their personal data, and if so, asks for access to them within the scope indicated in Art. 15. The controller requests the ID of the person making request to confirm her identity. The controller's action in this case is disproportionate and leads to unnecessary data collection.

However, in order to confirm the identity of the requesting person while preventing unnecessary data collection, the controller could require her to authenticate via logging into the account or ask her (non-intrusive) security questions, the answer to which only the data subject should know, or use multifactor authentication that were configured when the data subject registered their account, or use other existing means of communication known as to belong to the data subject, such as the e-mail address or a phone number, in order to send an access password.

Example 14: A bank customer, Mr. Y, plans to get a consumer credit. For this purpose, Mr. Y goes to a bank branch to obtain information, including his personal data, necessary for the assessment of his creditworthiness. To verify the data subject's identity, the consultant asks for a notarised certification of his identity to be able to provide him with the required information.

The controller should not require notarised confirmation of identity, unless it is necessary, suitable and in line with the national law (for example, where a person is temporarily not in possession of any identity document and proof of the data subject's identity is required by the national law for the performance of a legal act). Such practice exposes the requesting persons to additional costs and imposes an excessive burden on the data subjects, hampering the exercise of their right of access.

78. Without prejudice to the above general principles, under certain circumstances, authentication on the basis of an ID may be a justified and proportionate measure, in particular for entities processing special categories of personal data or undertaking data processing which may pose a risk for data subject (e.g. medical or health information). However, at the same time, it should be borne in mind that certain national provisions provide for restrictions on the processing of data contained in public documents, including documents confirming the identity of a person (also on the basis of Art. 87 GDPR). Restrictions on the processing of data from these documents may relate in particular to the scanning or photocopying of ID cards or processing of official personal identification numbers[39].

79. 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

[39] Several member states introduced such restriction in their national provisions in this regard stating, for example, that making copies of ID cards is lawful only if it results directly from the provisions of a legal act.

unlawful processing of the ID. Notwithstanding any applicable national provisions regarding ID authentication, this may include refraining from making a copy or deleting a copy of an ID immediately after the successful authentication of the identity of the data subject. This is because further storage of a copy of an ID is likely to amount to an infringement of the principles of purpose limitation and storage limitation (Art. 5(1)(b) and (e) GDPR) and, in addition, national legislation regarding the processing of the national identification number (Art. 87 GDPR). The EDPB recommends, as good practice, that the controller, after checking the ID card, makes a note e.g. " ID card was checked " to avoid unnecessary copying or storage of copies of ID cards.

3.4 Requests made via third parties / proxies

80. 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 some circumstances, the identity of the person authorised to exercise the right of access as well as authorisation to act on behalf of the data subject may require verification, where it is suitable and proportionate (see section 3.3 above)[40]. It should be recalled that making personal data available to someone who is not entitled to access it can amount to a personal data breach[41].

81. In doing so, national laws governing legal representation (e.g. powers of attorney), which may impose specific requirements for demonstrating authorisation to make a request on behalf of the data subject, should be taken into account, since the GDPR does not regulate this issue. In accordance with the principle of accountability, as well as of the other data protection principles, controllers shall be able to demonstrate the existence of the relevant authorisation to make a request on behalf of the data subject, and to receive the requested information, except if national law differs (e.g. national law contains specific rules regarding the trustworthiness of lawyers) leaving the controller to verify the identity of the proxy (e.g. in the case of lawyers checking enrolment at the bar). Therefore, it is recommended to collect appropriate documentation in this respect, in relation to the previously indicated general rules regarding confirmation of identity of a natural person making a request and, if the controller has reasonable doubts concerning the identity of a person acting on behalf of data subject, it shall request additional information to confirm the identity of this person.

82. 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. The matter is therefore dealt with by national law and Member States may provide for rules regarding the processing of personal data of deceased persons. However, it should be borne in mind that the data may, in addition, relate to living third persons, e.g. in the context of requested access to a deceased person's correspondence. The confidentiality of such data still needs to be protected.

[40] Regarding the time limits for exercising the right of access when the controller needs to obtain additional information, see para. 157.
[41] Art. 4(12) GDPR.

3.4.1 Exercise of the right of access on behalf of children

83. 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[42]. Any information and communication to a child, where personal data of a child are processed, should be in clear and plain language so that the child can easily understand[43].

84. 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, the child may need a third party to act on it's behalf e.g. the holder of parental responsibility.

85. The best interests of the child should be a 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.

86. 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 (in this respect see also section 3.4 above).

87. Finally, the right of the holder of parental responsibility to act on behalf of the child should not be confused with instances, outside of data protection law, where national legislation may provide the right of the holder of parental responsibility to ask and receive information on the child (e.g. performance of the child at school).

3.4.2 Exercising the right of access through portals / channels provided by a third party

88. There are companies that provide services which enable data subjects to make access requests through a portal. The data subject signs in and gets access to a portal through which they can submit for example an access request, request data rectification or data erasure from different controllers. Different questions arise from the use of portals provided for by a third party.

89. The first issue controllers need to deal with when facing these circumstances is to ensure 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.

90. Additionally, a controller that receives a request made through such a portal needs, invariably, to handle that request in a timely manner[44]. There is, however, no obligation for the controller to provide the data under Art. 15 GDPR directly to the portal, if the controller, for example, establishes that the security measures are insufficient or it would be deemed appropriate to use another way for the disclosure of data to the data subject. Under such circumstances, when the controller has other procedures in place to deal with access requests in an efficient and secure way, the controller can provide the requested information through these procedures.

[42] Recital 38 GDPR. As provided in the work programme of the EDPB, it is its intent to provide guidance on children's data. Such a document is expected to provide more guidance on the conditions under which a child may exercise their own right of access, and the holder of parental responsibility can exercise the right of access on behalf of the child.

[43] Recital 58 GDPR. EDPB Guidelines 05/2020 on consent under Regulation 2016/679, section 7.

[44] Regarding the time limits for exercising the right of access when the controller needs to obtain additional information, see para. 157

4 SCOPE OF THE RIGHT OF ACCESS AND THE PERSONAL DATA AND INFORMATION TO WHICH IT REFERS

91. The present section aims at shedding light on the definition of personal data (4.1) and clarifying the scope of the information covered by the right of access in general (4.2 and 4.3). Of note is that the scope of the concept of personal data and thus, the differentiation between personal data and other data, is an integral part of the assessment carried out by the controller to identify the scope of the data that the data subject is entitled to obtain access to[45].

92. As a preliminary consideration it should be recalled that the right of access can only be exercised with regard to processing of personal data falling within the material and territorial scope of the GDPR. Therefore, personal data that are not processed by automated means or that are not part of or intended to become part of a filing system as per Art. 2(1) GDPR or processed by a natural person in the course of a purely personal or household activity as per Art. 2 (2) GDPR, are not covered by the right of access.

4.1 Definition of personal data

93. Art. 15(1) and (3) GDPR refer to "*personal data*", and "*personal data undergoing processing*", respectively. Therefore, the scope of the right of access is first and foremost determined by the scope of the concept of personal data, defined in Art. 4(1) GDPR[46]. The concept of personal data has already been the subject of several Art. 29 Working Party[47] documents[48] and has been interpreted by the CJEU, including in the context of the right of access under Art. 12 of the Directive 95/46/CE.

94. The WP29 considered that the definition of personal data in the Directive 95/46/EC "*reflects the intention of the European lawmaker for a wide notion of 'personal data'*"[49]. Under the GDPR, the definition still refers to "*any information relating to an identified or identifiable natural person*". Aside from basic personal data like name and address, telephone number etc., unlimited broad variety of data may fall within this definition, including medical findings, history of purchases, creditworthiness indicators, communication contents, etc. In light of the broad scope of the definition of personal data,

[45] In accordance with the principle of privacy by design, such analysis is part of the assessment of appropriate measures and safeguards to protect data protection principles and data subject rights, which is carried out "*at the time of the determination of the means for processing and at the time of the processing itself*", *e.g.* reducing the response time when data subjects exercise their rights may be one of the metrics. For further explanations, see guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

[46] As per Art. 4(1) GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

[47] The Art. 29 Working Party (Art. 29 WP) is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR), the predecessor of the EDPB.

[48] e.g. WP251 rev01 Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679 i.e., p.19; WP29 Guidelines on the right to data portability - endorsed by the EDPB,p. 9.

[49] WP29 Opinion 4/2007 on the concept of personal data, p. 4.

a restrictive assessment of that definition by the controller would lead to an erroneous classification of personal data[50] and ultimately to a violation of the right of access.

95. In joint cases C-141/12 and C-372/12[51] the CJEU ruled that the right of access covered personal data contained in minutes, namely the "*name, date of birth, nationality, gender, ethnicity, religion and language of the applicant*" "*and, "where relevant, the data in the legal analysis contained in the minute*", but not the legal analysis itself[52]. The legal analysis was in this context not liable in itself to be the subject of a check of its accuracy by the data subject nor of rectification. Furthermore, providing access to the legal analysis does not fulfil the purpose of guaranteeing privacy but access to administrative documents.

96. In Nowak[53], 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. More precisely, such subjective information are personal data "*in the form of opinions and assessments, provided that it 'relates' to the data subject*"[54] as opposed to the examination questions, which are not considered personal data[55]. Thus, a contextual assessment should shed light on the effect or result an information may have on an individual and thus the scope of the right of access.

Example 15: An individual has a job interview with a company. In this context, the job applicant hands over a CV and an application letter. During the interview, the HR officer takes notes on a computer to document the interview. Afterwards, the job applicant, as data subject requests access to personal data relating to him or her that the company, as controller, collected in the course of the recruitment procedure.

The controller is obliged to provide the data subject with personal data actively communicated by them in their CV and letter of application. Moreover, the controller needs to provide the data subject with the summary of the interview, including the subjective comments on the behaviour of the data subject the HR officer wrote during the job interview, subject to any exemptions under national law and in compliance with Art. 23 GDPR.

97. 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:

- Special categories of personal data as per Art. 9 GDPR;
- Personal data relating to criminal convictions and offences as per Art. 10 GDPR;
- Data knowingly and actively provided by the data subject (e.g. account data submitted via forms, answers to a questionnaire)[56];
- Observed data or raw data provided by the data subject by virtue of the use of the service or the device (e.g. data processed by connected objects, transaction history, activity logs such as

[50] as information not relating to an identified or identifiable natural person.
[51] CJEU, joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, 17 July 2014.
[52] CJEU, joined Cases C-141/12 and C-372/12, YS and Others, paras. 38 and 48.
[53] CJEU, C-434/16, Peter Nowak v Data Protection Commissioner, 20 December 2017.
[54] CJEU, C 434/16, Nowak, paras. 34- 35.
[55] CJEU, C-434/16, Nowak, para. 58.
[56] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9.

access logs, history of website usage, search activities, location data, clicking activity, unique aspects of a person's behaviour such as handwriting, keystrokes, particular way of walking or speaking) [57];

- Data derived from other data, rather than directly provided by the data subject (e.g. credit ratio, classification based on common attributes of data subjects, country of residence derived from postcode)[58];
- Data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment or a personalization or recommendation process)[59];
- Pseudonymised data as opposed to anonymized data (see also section 3 of these guidelines).

Example 16: Elements that have been used to reach a decision about e.g. employee's promotion, pay rise or new job assignment (e.g. annual performance reviews, training requests, disciplinary records, ranking, career potential) are personal data relating to that employee. Thus such elements can be accessed by the data subject on request and respecting Art. 15(4) GDPR in case personal data for example, also relate to another individual (e.g. the identity or elements revealing the identity of another employee whose testimony about the professional performance is included in an annual performance review may be subject to limitations under Art. 15(4) GDPR and hence it is possible that they cannot be communicated to the data subject in order to protect the rights and freedoms of said employee). Nevertheless, national labour law provisions may apply for instance regarding the access to personnel files by employees or other national provisions such as those concerning professional secrecy. Under all circumstances, such restrictions to the exercise of the right of access of the data subject (or other rights) provided in a national law must respect the conditions of Art. 23 GDPR (see section 6.4).

98. Several considerations may be drawn from the above non-exhaustive list of personal data which may be provided to the data subject in the context of an access request. It is apparent from the above, that the controller may not operate a distinction when providing access to personal data between those data contained in paper files and those stored electronically as long as they fall within the scope of the GDPR. In other words, personal data which are contained in paper files as part of a filing system, or which are intended to form part of a filing system, are covered by the right of access in the same way as personal data stored in a computer memory by means of, for example, binary code or videotape.

99. Moreover, like most data subject rights, the right of access includes both inferred and derived data, including personal data created by a service provider, whereas the right to data portability only includes data provided by the data subject[60]. Therefore, in case of an access request and unlike a data portability request, the data subject should be provided not only with personal data provided to the

[57] WP29 Opinion 4/2007 on the concept of personal data, p. 8

[58] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 10-11

[59] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p.10-11; Art. 29 Working Party, WP 251 rev.01, 6 February 2018, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on Automated individual decision-making and profiling - endorsed by the EDPB"), p. 9-10.

[60] As previously stated in WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 10 and reiterated in WP29 Guidelines on Automated individual decision-making and profiling - endorsed by the EDPB, p. 17.

controller in order to make a subsequent analysis or assessment about these data but also with the result of any such subsequent analysis or assessment.

100. It also is important to recall that there is information, such as anonymous data[61], which is data that do not relate directly or indirectly to an identifiable person, and that are hence excluded from the scope of the GDPR. For example, the location of the server on which the personal data of the data subject processed is not personal data. The distinction can be challenging and controllers may wonder how to draw a clear line between personal and non-personal data in particular in the case of mixed datasets. In such case it may be useful to differentiate between mixed datasets in which personal and non-personal data are inextricably linked and those in which this is not the case. Personal and non-personal data may be inextricably linked in mixed datasets and fall altogether under the scope of the right of access of the data subject to which the personal data relates[62]. In other cases personal and non-personal data in mixed datasets may not be inextricably linked rendering only the personal data in the set accessible to the data subject. For example, a company might need to provide a data subject with the individual IT incident reports it triggered, but not with the company's knowledge database of IT problems. However, which security measures the controller has put in place is generally not to be understood as being personal data, provided that these are not inextricably linked with personal data, and therefore not covered by the right of access.

101. Before concluding the section, the EDPB recalls in this context that the protection of natural persons with regard to the processing of personal data encompasses all the types of personal data listed above and that a restrictive interpretation of the definition contravenes the provisions of the GDPR and ultimately violates Art. 8 of the Charter of Fundamental Rights. The application of a differing regime for the exercise of a right in relation to some types of personal data, which has not been foreseen by the GDPR can be introduced exclusively by law, in accordance with Art. 23 GDPR (as further explained in section 6.4). Thus, controllers cannot limit the exercise of the right of access by unduly restricting the scope of personal data.

4.2 The personal data the right of access refers to

102. According to Art. 15(1) GDPR, "*the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information*"(emphasis added).

103. Several elements emerge from paragraph (1) of Art. 15 GDPR. The paragraph refers *expressis verbis* to "*personal data concerning him or her*"(4.2.1) , which "*are being processed*"(4.2.2) by the controller:

4.2.1 "personal data concerning him or her"

104. The right of access can be exercised exclusively with regard to personal data relating to the data subject requesting access or, where applicable, by an authorised person or proxy (see section 3.4). There are also situations in which data do not have a link to the person exercising the right of access but to

[61] Further explanations on the concept of anonymization can be found in Art. 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, 10 April 2014, p. 5-19.
[62] Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, 29.05.2019, COM/2019/250 final.

another individual. The data subject is however, only entitled to personal data relating to themselves excluding data which exclusively concern someone else[63].

105. 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[64]. 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.

106. The words "*personal data concerning him or her*" should not be interpreted in an "*overly restrictive*" way by controllers, as the Art. 29 Working Party already stated with regard to the right to data portability[65]. Applied to the right of access, the EDPB considers for example that recordings of telephone conversations (and their transcription) between the data subject that requests access and the controller, may fall under the right of access provided that the latter are personal data[66]. Provided that the GDPR applies and that the processing is not covered by the household exemption as per Art. 2(2)(c) GDPR, if the data subject uses the obtained record which includes personal data of the interlocutor for other purposes by, for instance, publishing the record, the data subject will become a controller for this processing of personal data relating to the other person whose voice was recorded. Although this will not exempt the controller from its data protection obligations when duly analysing whether access to the full record may be given, the controller is encouraged to inform the data subject about the fact that they may become controller in such case. This is without prejudice to any further assessment under Art. 15(4) GDPR detailed in section 6. In the same vein, messages that data subjects have sent to others in the form of interpersonal messages and deleted themselves from their device, that are still avaible to the service provider, may fall under the right of access.

107. 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. In this context it is important to recall that the victim should be provided with information on all personal data the controller stores in connection with their identity, including those that have been collected on the basis of the fraudster's actions. In other words, even after the controller learned about the identity theft, personal data which are associated with or related to the identity of the victim constitute personal data of the data subject.

---

[63] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9: "*Only personal data is in scope of a data portability request. Therefore, any data that is anonymous or does not concern the data subject, will not be in scope. However, pseudonymous data that can be clearly linked to a data subject (e.g. by them providing the respective identifier, cf. Article 11 (2)) is within the scope."*

[64] CJEU, judgment in case C-434/16 Peter Nowak v. Data Protection Commissioner, 2017, para. 44.

[65] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9: *In many circumstances, controllers will process information that contains the personal data of several data subjects. Where this is the case, controllers should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an example, telephone, interpersonal messaging or VoIP records may include (in the subscriber's account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests, because the records are (also) concerning the data subject. However, where such records are then transmitted to a new controller, this new controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties (see below: third condition).*"

[66] See example 34 in section 6.2.

Example 17: An individual fraudulently uses the identity of someone else in order to play poker online. The perpetrator pays the online casino using the credit card they stole from the victim. When the victim finds out about the identity theft, the victim asks the provider of the online casino to provide him or her with access to his or her personal data and more specifically, to the online games played and information about the credit card used by the perpetrator.

There is a link between the collected data and the victim as the latter's identity has been used. After the detection of the fraud, the personal data mentioned above still has a link by reason of their content (the victim's credit card is clearly about the victim), purpose and effect (the information about the online games played by the perpetrator may for instance be used to issue invoices to the victim). Therefore, the online casino shall grant the victim access to the aforementioned personal data.

108. If appropriate, internal connection logs can be used to hold record about accesses to a file and to trace back which actions were performed in connection with accesses to a record, such as printing, copying, or deleting personal data. These logs may include the time of logging, the reason for the access to file as well as information identifying the person having had access. Questions related to this topic are at issue in a case currently pending before the CJEU (C-579/21). The putting in place and the supervision and revision of connection logs fall within the controller's responsibility and are liable to be checked by the supervisory authorities. The controller should thus make sure that the persons acting under its authority who have access to personal data do not process personal data except on instructions from the controller, as per Art. 29 GDPR. If the person nevertheless processes the personal data for other purposes than fulfilling the controller's instructions, it may become controller for that processing and subject to disciplinary or criminal proceedings or administrative sanctions issued by supervisory authorities. The EDPB notes that it is part of the employer's responsibility under Art. 24 GDPR to make use of appropriate measures, extending from education to disciplinary procedures, to ensure that processing is in compliance with the GDPR and that no infringement occurs.

4.2.2 Personal data which "are being processed"

109. Paragraph (1) of Art. 15 GDPR moreover refers to personal data, which "are being processed". The time reference point for determining the range of personal data falling within the access request has already been elaborated in section 2.3.3. The wording however also suggests that the right of access does not distinguish between the purposes of the processing operations.

Example 18: A company processed personal data relating to a data subject in order to process their purchase order and arrange shipping to data subject's home address. After these initial purposes for which the personal data were collected no longer exist, the controller keeps some of the personal data solely to comply with its legal obligations relating to the keeping of records.

The data subject requests access to personal data relating to them. To comply with its obligation under article 15 (1) GDPR, the controller needs to provide the data subject with the requested personal data which are stored to comply with its legal obligations.

110. 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. It should be pointed out, that in respect of the principles of data protection by design and data minimisation, the back-up data is in principle similar to the data in the live system. Where there are slight differences between personal data in the back-up and the live production system, these are generally linked to the collection of additional data since the last back-up. A decrease in data in the live system (e.g. erasure after the

retention period of some data came to an end or following an erasure request) will in some cases only be overwritten in the back-up data at the time of the subsequent back-up. In case there is an access request at the moment where there are more personal data relating to the data subject in the back-up than in the live system or different personal data (noticeable for example via log of deletions in the live production system implemented in full compliance with the principle of data minimisation), the controller needs to be transparent about this situation and where technically feasible provide access as requested by the data subject, including to personal data stored in the back-up. For instance, with the aim of being transparent to data subjects who exercise their right, a log of deletions in the live production system may enable the controller to see that there are data in the back-up which are not in the live system anymore as they have been recently deleted has and have not yet been overwritten in the back-up.

4.2.3 The scope of a new request to access

111. What remains to say is that data subjects are 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). As a consequence, where a controller already complied with a request for access in the past and provided that the request is not excessive, the controller cannot narrow the scope of this new request. This means that in relation to any further access request of the same data subject, the controller should not inform the data subject only about the mere changes in the personal data processed or the processing itself since the last request, unless the data subject expressly agrees to this. Otherwise, data subjects would be obliged to compile their personal data provided in order to a complete set of personal data concerning their information on the processing and on data subjects rights.

4.3 Information on the processing and on data subject rights

112. In addition to the access to the personal data themselves, the controller has to provide information on the processing and on data subject rights according to Art. 15(1)(a) to (h) and 15(2) GDPR. Most of the information on those specific points is already compiled, at least in general form, in the controller's record of processing activities referred to in Art. 30 GDPR and/or in its privacy notice elaborated in accordance with Art.s 12 to 14 GDPR. Therefore, it might be helpful as a first step to consult the "Guidelines on transparency under Regulation 2016/679" [67] of the Art. 29 Working Party, on the content of the information to be given under Art. 13 and 14 GDPR.

113. 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 up-to-date and precise with regards to the request of the data subject. Before or at the beginning of the data processing, some information, such as the identification of specific recipients or the specific duration of the data processing, can often not yet be provided. Some information, like for example the right to complain to a supervisory authority (see Art. 15(1)(f)), does not change depending on the person making the access request.Therefore, it may be communicated in general terms as it is also done in the privacy notice. Other types of information, such as the information on recipients, on categories and on the source of the data may vary depending on who makes the request and what the scope of the request is. In the context of an access request under Art. 15, any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with

[67] Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB").

regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the « tailored and updated » information is the same as the information provided at the beginning of the processing. In explaining which information relates to the requesting person, the controller could, where appropriate, refer to certain activities (such as "if you have used this service …", "if you have payed by invoice") as long as it is obvious for the data subjects if they are concerned. In the following, the degree of specification required is explained in relation to the individual types of information.

114. 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. If the processing is carried out for several purposes, the controller has to clarify which data or which categories of data are processed for which purpose(s). Unlike Art. 13(1)(c) and Art. 14(1)(c) GDPR, the information on the processing referred to in Art. 15(1)(a) does not contain information on the legal basis for the processing. However, as some data subjects' rights depend on the applicable legal basis, this information is important for the data subjects to verify the lawfulness of the data processing and to determine which data subject's rights are applicable in the specific situation. Therefore, in order to facilitate the exercise of data subjects' rights in line with Art. 12(2) GDPR, the controller is recommended to also inform the data subject as to the applicable legal basis for each processing operation or to indicate where they can find this information. In any event, the principle of transparent processing requires that the information on the legal bases of the processing be made available to the data subject in an accessible way (e.g. in a privacy notice).

115. Information on categories of data (Art. 15(1)(b)) may also have to be tailored to the data subject's situation such that categories which have turned out not to be relevant in case of the requester should be eliminated.

Example 19: In the context of the information referred to in Art. 13/14 GDPR, a hotel states that they process a number of categories of customer data (identification data, contact data, bank data, and number of credit card etc.). If a request of access is made on the basis of Art. 15, the data subject who makes the request must, in addition to the access to the actual data being processed (component 2), in line with Art. 15(1)(b) also be informed as to the specific categories of data which are being processed in the specific case (e.g. not including bank data or credit card data in the event payment was made in cash).

116. Information on "recipients or categories of recipients" (Art. 15(1)(c)) has firstly to take into account the definition of recipients given in Art. 4(9) GDPR. The definition of recipients is based on the disclosure of personal data to a natural or legal person, public authority, agency or other body[68]. From Art. 4(9) GDPR follows, that public authorities acting in the framework of a particular enquiry subject to specific national provisions are not to be considered as recipients.

117. Concerning the question, if the controller is free to choose between information on recipients or on categories of recipients, it has to be noted that "unlike Art. 13 and 14 of the GDPR, which lay down an obligation on the part of the controller (…), Article 15 of the GDPR lays down a genuine right of access

[68] It should further be noted, that different controllers as defined by Art. 4(7) GDPR may exist within the same company. In this constellation a disclosure of data from one recipient to another within one company is possible.

for the data subject, with the result that the data subject must have the option of obtaining either information about the specific recipients to whom the data have been or will be disclosed, where possible, or information about the categories of recipients."[69] It has also to be recalled, that, as stated in the above-mentioned guidelines on transparency[70], already under 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. Under Article 15, if the data subject has not chosen otherwise, the controller is obliged to name the actual recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) GDPR[71] [72]. The EDPB recalls in this regard, that storing information relating to the actual recipients is necessary *inter alia* to be able to comply with the controller's obligations under Art. 5(2) and 19 GDPR.

Example 20: In its privacy notice an employer gives information about which categories of data are passed on to "travel agencies" or "hotels" in case of business trips, in accordance with Art. 13(1)(e) and 14(1)(e) GDPR. If an employee makes a request for access to the personal data after business trips have taken place, the employer should then, concerning the recipients of the personal data pursuant to Art. 15(1)(c), indicate in its reply the travel agency(ies) and hotel(s) that received the data. While the employer legitimately referred to categories of recipients in its privacy notice pursuant to Art. 13 and 14, because at this stage, it was not yet possible to name the recipients, it should, unless the employee has chosen otherwise, provide information as to the specific recipients (name of travel agencies, hotels etc.) when the employee is making an access request.

Where, respecting the conditions mentioned above, a controller may only provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients[73].

118. According to Art. 15(1)(d), information has to be given on the envisaged period for which the personal data will be stored, where possible. Otherwise, the criteria used to determine that period have to be provided. The information given by the controller has to be precise enough for the data subject to know how long the data relating to the data subject will continue to be stored. If it is not possible to specify the time of deletion, the duration of storage periods and the beginning of this period or the triggering event (e.g. termination of a contract, expiration of a warranty period, etc.) shall be specified. The mere reference, for example to "deletion after expiry of the statutory storage periods" is not sufficient. Indications concerning data storage periods will have to focus on the specific data relating to the data subject. If the personal data of the data subject is subject to different deletion periods (e.g. because not all data is subject to legal storage obligations), the deletion periods shall be stated in relation to the respective processing operations and categories of data.

119. Whereas information on the right to lodge a complaint with a supervisory authority (Art. 15(1)(f)) is not dependant on the specific circumstances, the data subjects rights mentioned in Art. 15(1)(e) vary depending on the legal basis underlying the processing. With regard to its obligation to facilitate the

[69] CJEU, C-154/21 (Österreichische Post AG), para. 36.
[70] Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB"), p. 37 (Annex)
[71] CJEU, C-154/21 (Österreichische Post AG)
[72] The mere fact, that the data have been disclosed to a large number of recipients would not *per se* render the request excessive,see section 6, para 188.
[73] WP29 Guidelines on transparency - endorsed by the EDPB, p. 37 (Annex)

exercise of data subject rights pursuant to Art. 12(2) GDPR, the response by the controller on those rights shall be individually tailored to the case of the data subject and relate to the processing operations concerned. Information on rights that are not applicable for the data subject in the specific situation should be avoided.

120. According to Art. 15(1)(g), "any available information" as to the source of the data has to be provided, where the personal data are not collected from the data subject. The degree of available information may change over time.

Example 21: The privacy policy of a large company states:

"Credit checks help us to prevent problems in payment transactions. They guarantee the protection of our company against financial risks, which can also affect sales prices in the medium to long term. A credit check is necessarily carried out when we are going to ship goods without receiving the respective purchase price at the same time, e.g. in the case of a purchase on account. Without carrying out the credit check, only a prepayment payment option (immediate bank transfer, online payment provider, credit card) is possible.

For the purpose of credit checking, we will send your name, address and date of birth to the following service providers, for example: (1) Financial Information Agency X (2) Business Information Provider Y, (3) Commercial Credit Reference Agency Z.

The data are passed on to the above-mentioned credit institutions only within the scope of what is legally permissible and only for the purposes of the analysis of your past payment behaviour as well as for the assessment of the risk of default on the basis of mathematical-statistical procedures using address data as well as for verification of your address (examination of delivery). Depending on the result of the credit check, we may no longer be able to offer you individual payment methods, such as the purchase of invoices."

The privacy notice thus contains general information on the possibility of obtaining information from the listed Economic Information Offices in accordance with Art. 13 and 14 GDPR. If it is not clear ex ante, which of the companies will get involved in the processing, it is sufficient to mention the names of the eligible companies in the privacy policy. In the context of a request based on Art. 15, in addition to the information that a creditworthiness information has been obtained, it would then (ex post) be necessary to disclose, which of the companies mentioned has been involved exactly. It is clearly expressed by Art. 15(1)(g), that information on the processing of the data comprise "any available information as to their source" where the personal data are not collected from the data subject.

121. Art. 15(1)(h) provides that every data subject should have the right to be informed, in a meaningful way, *inter alia*, about the existence and underlying logic of automated decision-making including profiling concerning the data subject and about the significance and the envisaged consequences that such processing could have[74]. If possible, information under Art. 15(1)(h) has to be more specific in relation to the reasoning that lead to specific decisions concerning the data subject who asked for access.

[74] See on this behalf Guidelines on transparency under Regulation 2016/679 (WP 260), para. 41, with reference to Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP 251).

122. 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) GDPR. In the context of a request for access under Art. 15, Art. 15(2) requires information on the appropriate safeguards pursuant to Art. 46 GDPR only in cases where transfer to a third country or an international organisation is actually taking place.

5 HOW CAN A CONTROLLER PROVIDE ACCESS?

123. 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. In other situations, the right of access is more complicated because the data processing is more complex; with regard to the number of data subjects, the categories of processed data as well as the flow of data within and between different organisations. Considering the differences in personal data processing, the appropriate way to provide access may vary accordingly.

124. This section aims at giving some guidance and practical examples on different ways for controllers to comply with an access request as well as to the meaning of Art. 12(1) GDPR in relation to the right of access. This section will also give some guidance about what is considered to be a commonly used electronic form as well as the timing for the provision of access under Art. 12(3) GDPR.

5.1 How can the controller retrieve the requested data?

125. 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. When carrying out such search, the controller should use available information in the organisation regarding the data subject that likely will result in matches in the systems depending on how the information is structured[75]. For example, if the information is sorted in files depending on name or a reference number, the search could be limited to these factors. But if the structure of the data depends on other factors, such as family relations or professional titles or any kind of direct or indirect identifiers (e.g. customer number, user name or IP-addresses), the search needs to be extended to include these, provided that the controller also holds this information related to the data subject, or is provided with that information by the data subject. The same applies when records regarding third persons are likely to contain personal data regarding the data subject. The controller may, however, not require the data subject to provide more information than necessary to identify the data subject. If a controller uses a processor for its data processing activities the search naturally has to be extended to also include personal data processed by the processor.

126. In line with Art. 25 GDPR on data protection by design and by default, the controller (and any processors it uses) 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. It is therefore important to keep in mind that

[75] Such a search should naturally also include information that is held by a processor, see. Article 28(3)(e) GDPR.

the process to retrieve data should also be designed in a data protection friendly way, so that it doesn't compromise the privacy of others, for example the employees of the controller.

5.2 Appropriate measures for providing access

5.2.1 Taking "appropriate measures"

127. Art. 12 GDPR lays down the requirements for providing access, i.e. for providing the confirmation, the personal data and the supplementary information under Art. 15, and also specifies the form, manner and time limit in relation to the right of access. Art. 29 Working Party's "Guidelines on transparency under Regulation 2016/679"[76] provides further guidance as regards Art. 12, mostly in relation to Art. 13 and 14 GDPR but also in relation to Art. 15 and on transparency in general. Thus, what is defined in those guidelines can often equally apply with regards to providing access under Article 15.

128. 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 disabilities. In addition, in situations where the controller is made aware of any particular needs of 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.

129. 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 large quantity of data on a large scale must accept to undertake great efforts to ensure the right of access to the data subjects in a consice, transparent, intelligible and easily accessible form, by using plain and clear language.

130. 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 GDPR), 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"*[77]. Therefore, and in respect of the transparency principle, data subjects must obtain from the controller the information and personal data required by Art. 15(1), 15(2) and 15(3) in a way that enables complete access to the requested information. In special circumstances, it would be inappropriate or even unlawful to share the information within the controller, for example due to the sensitive nature of the information (such as information relating to

[76] Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB").
[77] WP29 Guidelines on transparency - endorsed by the EDPB, para. 33.

whistleblowing). In these cases, it would be deemed appropriate to split the information into several replies as a response to the data subjects access request. The method chosen by the controller must actually provide the data subject with the requested data and information, hence it would not be appropriate to solely refer the data subject to check the requested data stored on their own device including, for example, to check clickstream history and IP addresses on their mobile phone.

131. In accordance with the accountability principle, a controller must document their approach to be able to demonstrate how the means chosen to provide the necessary information under Art. 15 are appropriate in the circumstances at hand.

5.2.2 Different means to provide access

132. As already explained in section 2.2.2 above, when making an access request the data subjects are entitled to receive a copy of their data undergoing processing pursuant to Art. 15(3) together with the supplementary information, which is considered as the main modality for providing access to the personal data.

133. However, in 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. These modalities may be appropriate ways of granting access for example in cases where it is in the interest of the data subject or the data subject asks for it. Onsite access could also be appropriate, as an initial measure, when a controller handles a large quantity of non-digitalized data to allow the data subject to be made aware of what personal data are undergoing processing and to be able to make an informed decision about what personal data he or she wants to be provided through a copy. Non-permanent ways of access can be sufficient and adequate in certain situations; for example, it can satisfy the need of the data subjects to verify that the data processed by the controller are correct by giving data subjects a chance to view the original data. A controller is not obliged to provide the information through other ways than providing a copy but should take a reasonable approach when considering such a request. Giving access through other ways than providing a copy does not preclude the data subjects from the right to also have a copy, unless they choose not to.

134. The controller may choose, depending on the situation at hand, to provide the copy of the data undergoing processing, together with the supplementary information, in different ways, e.g. by e-mail, physical mail or by the use of a self-service tool. If the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form as stated in Art. 15(3). 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.

135. In the situation, where the controller is processing personal data regarding the person making the request only in a small scale, the copy of the personal data and the supplementary information can and should be provided through a simple procedure.

Example 22: A local bookstore keeps a record of name and addresses of their customers that have ordered home delivery. A customer visits the bookstore and makes a request for access. In this situation it would be sufficient to print out the personal data concerning the customer directly from the business system, while also supplying the supplementary information in Art. 15(1) and (2).

Example 23: A monthly donor to a charity organisation makes an access request through e-mail. The charity organisation holds information about donations made in the past twelve months, as well as names and e-mail addresses of the donors. The controller could provide the copy of the personal data and the supplementary information by responding to the e-mail, provided that all necessary safeguards are applied, taking into consideration for example the nature of the data.

136. Even controllers that process a large quantity of data can choose to rely on manual routines for handling access requests. If the controller processes data in several different departments, the controller needs to collect the personal data from each department to be able to respond to the data subject request.

Example 24: An administrator is appointed by the controller to handle the practical issues regarding access requests. When receiving a request the administrator sends an enquiry by e-mail to the different departments of the organisation asking them to collect personal data regarding the data subject. Representatives of each department give the administrator the personal data processed by their department. The administrator then sends all the personal data to the data subject together with the necessary supplementary information, for example and when appropriate, by e-mail.

137. 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.

Example 25: A social media service has an automated process for handling access requests in place that enables the data subject to access their personal data from their user account. To retrieve the personal data the social media users can choose the option to "Download your personal data" when logged into their user account. This self-service option allows the users to download a file containing their personal data directly from the user account to their own computer.

138. 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. The controller may indeed encourage the data subject to use a self-service tool that the controller has set in place for handling access requests. However, it should be noted that the controller must also handle access requests that are not sent through the established channel of communication[78].

5.2.3 Providing access in a "concise, transparent, intelligible and easily accessible form using clear and plain language"

139. According to Art. 12(1) GDPR 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.

140. 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

[78] See section 3.1.2.

easily understood 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 the means for providing access under Art. 15.

Example 26: A social media provider processes a large quantity of information about a data subject. A large part of this personal data is information contained in hundreds of pages of log files where the data subject's activities on the website are registered. If data subjects request access to their personal data, the personal data in these log files are indeed covered by the right of access. The right of access may therefore be formally fulfilled if these hundreds of pages of log files were to be provided to the data subject. However, without measures taken to facilitate the understanding of the information in the log files, the data subject's right of access might not be met in practice, because no knowledge can easily be drawn from the log files, therefore not fulfilling the requirement of Art. 12(1) GDPR. The controller must therefore be careful and thorough when choosing the way the information and personal data is presented to the data subject.

141. Under the circumstances in the example above, the use of a layered approach, similar to the layered approach advocated in the Guidelines on transparency with regard to privacy notices[79], could be an appropriate measure to fulfil both the requirements in Art. 15 and 12(1) GDPR. This will be further developed under section 5.2.4. below. The requirement that the information is "intelligible" means that it should be understood by the intended audience[80], whilst keeping in mind any particular needs that the data subject might have that is known to the controller[81]. Since the right of access often enables the exercise of other data subject rights, it is crucial that the information provided is made understandable and clear. This is because data subjects will only be able to consider whether to invoke their right to, for example, rectification under Art. 16 GDPR once they know what personal data are being processed, for what purposes etc. As a result, the controller might need to supply the data subject with additional information that explains the data provided. It should be emphasised that the complexity of data processing obliges the controller to provide the means to make the data understandable and could not be used as an argument to limit the access to all data. Similarly, the controller's obligation to provide data in a concise manner cannot be used as an argument to limit access to all data.

Example 27: An ecommerce website collects data about items viewed or purchased on its website for marketing purposes. A part of this data will consist of data in a raw format[82], which has not been analysed and may not be directly meaningful to the reader (codes, activity history etc.). Such data related to the data subjects activities is also covered by the right of access and should, as a consequence, be provided to the data subject in response to an access request. When providing data in a raw format it is important that the controller takes the necessary measures to ensure that the data subject understands the data, for example, by providing an explanatory document that translates the raw format into a user friendly form. Also, such a document could explain that abbreviations and other acronyms for example "A" means that the purchase has been interrupted and "B" means that the purchase has gone through.

[79] WP29 Guidelines on transparency - endorsed by the EDPB, para. 35.

[80] Intelligibility is closely linked to the requirement to use a plain and clear language (WP29 Guidelines on transparency - endorsed by the EDPB, para. 9). What is said about a plain and clear language in para. 12-16 with regards to information referred to in Articles 13 and 14 GDPR, equally applies to communication under Article 15.

[81] See para. 128.

[82] The raw format in the example is to be understood as unanalysed data underlying a processing, and not the lowest level of raw data that may only be machine-readable (such as "bits").

142. The "easily accessible" element means that the information under Art. 15 should be presented in a way that is easy for the data subject to access. This applies for example, to the layout, appropriate headings and paragraphing. The information should always be provided in 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 use of standardised icons is also encouraged when it facilitates the intelligibility and accessibility of the information. When the request for information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information, the controller is expected to take measures facilitating the understanding of the information provided, including oral information, when adequate[83]. The controller should take special care to ensure that elderly people, children, visually impaired persons or persons with cognitive or other disabilities can exercise their rights, for instance, by proactively providing easily accessible elements to facilitate exercise of these rights.

5.2.4 A large quantity of information necessitates specific requirements on how the information is provided

143. Regardless of the means used to provide access there may be a tension between the amount of information the controller needs to provide data subjects with and the requirement that it must be concise. One way of achieving both, and an example of an appropriate measure for certain controllers, when a large quantity of data is to be provided, is to use a layered approach. This approach can facilitate the data subjects' understanding of the data. It should nevertheless be stressed that this approach can only be used under certain circumstances and needs to be carried out in a way that does not limit the right of access, as explained below. Furthermore, the use of a layered approach should not create an extra burden for the data subject. Hence, it would be best suited when access is provided in an online context. A layered approach is merely a way to present the information under Art. 15 in a manner which is also compliant with the requirements in Art. 12(1) GDPR and should not be confused with the possibility for the controllers to request that the data subject specifies the information or processing activities to which the request relates, as prescribed in Recital 63 of the GDPR[84].

144. A layered approach in relation to the right of access means that a controller, under certain circumstances, can provide the personal data and the supplementary information required under Art. 15 in different layers. The first layer should include information about the processing and data subject's rights according to Art. 15(1)(a)-(h) and 15(2) as well as a first part of the processed personal data. In a second layer, more personal data should be provided.

145. 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[85]. The controllers need to be able to demonstrate accountability as to their reasoning of the above.

Example 28: A controller analyses big data sets to place customers in different segments depending on their online behaviour. In this situation, it can be assumed that the information that is the most

[83] See WP29 Guidelines on transparency - endorsed by the EDPB, para. 21.
[84] See also section 2.3.1.
[85] See WP29 Guidelines on transparency - endorsed by the EDPB, para. 36.

important for the data subjects to obtain is information about what segment they have been put in. As a result, this information should be included in the first layer. The data in a raw format[86] that has not yet been analysed or further processed, such as user activity on a website, is also personal data covered by the right of access, however, it could in some cases be sufficient to provide this information in another layer.

146. 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. In this way it will be easier for the data subject to decide what layers they want to access. The description should objectively reflect all the categories of personal data that are actually processed by the controller. It also needs to be clear how the data subject can get access to the different layers. Access to the different layers shall not entail any disproportionate effort for the data subject and shall not be made conditional on the formulation of a new data subject request. This means that the data subjects must have the possibility to choose whether to access all layers at once or to access one or two of the layers, if they are satisfied with this.

Example 29: A data subject makes an access request to a video streaming service. The request is made through an option that is available when data subjects have logged into their account. The data subject is presented with two options which appear as buttons on the webpage. Option one is to download part 1 of the personal data and the supplementary information. This contains, for example, recent streaming history, account information and payment information. Option two is to download part 2 of the personal data that contains technical log files about the data subjects activities and historical information on the account. In this case, the controller has made it possible for data subjects to exercise their right in a way that does not create an extra burden for the data subject.

Variation 1: In cases where the data subject only chooses the button to download part 1 of the personal data, the controller is obliged only to provide part 1 of the data.

Variation 2: In cases where the data subject chooses the buttons for both part 1 and part 2 of the data, the controller cannot communicate only part 1 of the data and ask for a new confirmation before communication of part 2 of the data. Instead both parts of the data must be provided to the data subject, as it follows from the request made.

147. The use of a layered approach will not be considered appropriate for all controllers or in all situations. It should only be used when it would be difficult for the data subject to comprehend the information if given in its entirety. In other words, the controller needs to be able to demonstrate that the use of layered approach adds value for the data subject in helping them understand the information provided. A layered approach would therefore only be considered appropriate when a controller processes a large quantity of personal data about the data subject making a request and where there would be apparent difficulties for the data subject to grasp or comprehend the information if it were to be provided all at once. The fact that it would require great effort and resources from the controller to provide the information under Art. 15 is not in itself an argument for using a layered approach.

5.2.5 Format

148. According to Art. 12(1) GDPR, information under Art.15 shall be provided in writing or by other means including, where appropriate, by electronic means. As regards access to the personal data undergoing

[86] See footnote 82.

processing, Art. 15(3) states that where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The GDPR does not specify what a commonly used electronic form is. Thus there are several conceivable formats that can be used. What is considered to be a commonly used electronic form will also vary over time.

149. What could be considered as a commonly used electronic form should be based on an objective assessment and not on what format the controller uses in its daily operations. In order to determine what format is to be considered as a commonly used format in the situation at hand, the controller will have to assess if there are specific formats generally used in the controller's area of operation or in the given context. When there are no such formats generally used, open formats set in an international standard, such as ISO, should, in general, be considered as commonly used electronic formats. However, the EDPB does not exclude the possibility that other formats may also be considered to be commonly used within the meaning of Article 15(3). When assessing if a format is a commonly used electronic format, the EDPB considers that it is of importance how easily the individual can access information provided in the current format. In this regard it should be noted what information the controller has provided to the data subject about how to access a file which has been provided in a specific format, such as what programs or software that could be used, to make the format more accessible to the data subject. The data subject should, however, not be obliged to buy software in order to get access to the information.

150. 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 embodied, permanent form (text, electronic). Since the information should persist over time, information in writing, including by electronic means, is, in principle, preferable over other forms. The copy of the personal data could, when appropriate, be stored on an electronic storage device such as CD or USB.

151. It should be noted that for a controller to be able to consider that data subjects have been provided with a copy of personal data it is not enough to have provided them with access to their personal data. For the requirement to provide a copy of personal data to be fulfilled and in case the data are provided electronically/digitally, the data subjects need to be able to download their data in a commonly used electronic form.

152. It is the responsibility of the controller to decide upon the appropriate form in which the personal data will be provided. The controller can, although is not necessarily obliged to, provide the documents which contain personal data about the data subjects making the request, in their original form. The controller could, for example, on a case-by-case basis, provide access to a copy of the medium as such, given the need for transparency (for example, to verify the accuracy of the data held by the controller in the event of a request for access to the medical file or an audio recording whose transcript is disputed). However, the CJEU, in its interpretation of the right of access under the Directive 95/46/EC, stated that "for *[the right of access]* to be complied with, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him"[87]. Unlike the directive,

[87] CJEU, Joined Cases C-141/12 and 372/12, YS and Others, para. 60.

the GDPR expressly contains an obligation to provide the data subject with a copy of the personal data undergoing processing. This, however, does not mean that the data subject always has the right to obtain a copy of the documents containing the personal data, but an unaltered copy of the personal data being processed in these documents. [88] Such copy of the personal data could be provided through a compilation containing all personal data covered by the right of access as long as the compilation makes it possible for the data subject to be made aware and verify the lawfulness of the processing. Hence, there is no contradiction between the wording of the GDPR and the ruling by the CJEU regarding this matter. The word summary in the ruling should not be misinterpreted as meaning that the compilation would not encompass all data covered by the right of access, but is merely a way to present all that data without giving access to the underlying documents which contain the personal data. Since the compilation needs to contain a copy of the personal data, it should be stressed that it cannot be made in a way that somehow alters or changes the content of the information.

Example 30: A data subject has been insured with an insurance company for many years. Several insured incidents have occurred. In each case there has been some written correspondence through e-mail between the data subject and the insurance company. As the data subject had to provide information regarding the specific circumstances of each incident, the correspondence entails a lot of personal information about the data subject (hobbies, flatmates, daily habits etc.). In some cases disagreement arose about the insurance company's obligation to compensate the data subject which caused a vast amount of communication back and forth. All this correspondence is stored by the insurance company. The data subject makes an access request. In this situation the controller does not necessarily have to provide the e-mails in their original form by forwarding them to the data subject. Instead the controller could choose to compile the e-mail correspondence containing the data subject's personal data in a file that is provided to the data subject.

153. Notwithstanding the form in which the controller provides the personal data, e.g. by providing the actual documents containing the personal data or a compilation of the personal data, the information shall comply with the transparency requirements laid down in Art. 12 GDPR. Making some kind of compilation and/or extracting the data in a way that makes the information easy to comprehend could, in some cases, be a way to comply with these requirements. In other cases the information is better understood by providing a copy of the actual document containing the personal data. Hence which form is most suitable must be decided on a case by case basis.

154. In this context, it is important to remember that there is a distinction between the right to obtain access under Art. 15 GDPR and the right to receive a copy of administrative documents regulated under national law, the latter being a right to receive a copy of the actual document. This does not mean that the right of access under Art. 15 GDPR excludes the possibility to receive a copy of the document/media on which the personal data appear.

155. In some cases, the personal data itself sets the requirements in what format the personal data should be provided. For example, when the personal data constitutes handwritten information by the data subject, the data subject may need to be provided with a photocopy of that handwritten information, as the handwriting itself is personal data. That could especially be the case when the handwriting is something that matters to the processing, e.g. scripture analysis. The same applies in general for audio recordings because the voice of the data subject itself is personal data. In some cases, however, access

[88] Questions related to this topic are at issue in cases currently pending before the CJEU (C-487/21 and C-307/21).

can be given by providing a transcription of the conversation, for example, if agreed upon between the data subject and the controller.

156. It should be noted that the provisions on format requirements are different regarding the right of access and the right of data portability. Whilst the right of data portability under Art. 20 GDPR requires that the information is provided in a machine readable format, the right to information under Art. 15 does not. Hence, formats that are considered not to be appropriate when complying with a data portability request, for example pdf-files, could still be suitable when complying with an access request.

5.3 Timing for the provision of access

157. Art. 12(3) GDPR requires that the controller provides information to the data subject regarding action taken in respect of a request under Art. 15 without undue delay and in any event within one month of receipt of the request. This deadline can be extended by a maximum of two months taking into account the complexity and the number of the requests, provided that the data subject has been informed about the reasons for such delay within one month of the receipt of the request. This obligation to inform the data subject about the extension and its reasons should not be confused with the information that has to be given without delay and at the latest within one month when the controller does not take action on the request, as detailed by Art. 12(4) GDPR.

158. The controller shall react and, as a general rule, provide the information under Art. 15 without undue delay, which means that the information should be given as soon as possible. This means that, if it is possible to provide the requested information in a shorter amount of time than one month, the controller should do so. The EDPB also considers that the timing to answer the request in some situations must be adapted to the storage period in order to be able to provide access[89].

159. 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.[90] It is not necessary that the controller is in fact aware of the request. However, when the controller needs to communicate with the data subject due to the uncertainty regarding the identity of the person making the request there may be a suspension in time until the controller has obtained the information needed from the data subject, provided the controller has asked for additional information without undue delay. The same applies for when a controller has asked a data subject to specify the processing operations to which the request relates, when the conditions set out in Recital 63 are met. [91].

Example 31: Following the reception of the request, a controller reacts immediately and asks the information it needs to confirm the identity of the person making the request. The latter replies only several days later and the information that the data subject sends to verify the identity does not seem sufficient which requires the controller to ask for clarifications. In this situation there will be a suspension in time until the controller has obtained enough information to verify the identity of the data subject.

[89] See section 2.3.3
[90] In some member states there is national law determining when a message is to be considered as received, taking into account weekends and national holidays.
[91] See further section 2.3.1.

160. The time period to respond to an access request needs to be calculated in accordance with Regulation No 1182/71[92].

Example 32: An organisation receives a request on 5 March. The time limit starts from the same day. This gives the organisation until and including 5 April to comply with the request, at the latest.

Example 33: If the organisation receives a request on 31 August, and as the following month is shorter there is no corresponding date, the date for response, at the latest, is the last day of the following month, hence 30 September.

161. If the last day of this time period falls on a weekend or a public holiday, the controller has until the next working day to respond.

162. Under certain circumstances the controller can extend the time to respond to a request of access by two further months if necessary, taking into account the complexity and number of the requests. It should be emphasised that this possibility is an exemption from the general rule and should not be overused. If controllers often find themselves forced to extend the time limit, it could be an indication of a need to further develop their general procedures to handle requests.

163. What constitutes a complex request varies depending upon the specific circumstances of each case. Some of the factors that could be considered relevant are for example:

- the amount of data processed by the controller,
- how the information is stored, especially when it is difficult to retrieve the information, for example when data are processed by different units of the organisation,
- the need to redact information when an exemption applies, for example information regarding other data subjects or that constitutes trade secrets, and
- when the information requires further work in order to be intelligible.

164. The mere fact that complying with the request would require a large effort does not make a request complex. Similarly, the fact that a big company receives a large number of requests would not automatically trigger an extension of the time limit. However, when a controller temporarily receives a large amount of requests, for example due to an extraordinary publicity regarding their activities, this could be regarded as a legitimate reason for prolonging the time of the response. Nevertheless, a controller, especially one who handles a large quantity of data, should have procedures and mechanisms in place in order to be able to handle requests within the time limit under normal circumstances.

6 LIMITS AND RESTRICTIONS OF THE RIGHT OF ACCESS

6.1 General remarks

165. The right of access is subject to the limits that result from Art. 15(4) GDPR (rights and freedoms of others) and Art. 12 (5) GDPR (manifestly unfounded or excessive requests). Furthermore, Union or Member State law may restrict the right of access in accordance with Art. 23 GDPR. Derogations

[92] Regulation (EEC, EURATOM) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits.

regarding the processing of personal data for scientific, historical research or statistical purposes or archiving purposes in the public interest can be based on Art. 89(2) and Art. 89(3) GDPR accordingly and derogations for processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression can be based on Art. 85(2) GDPR.

166. 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 GDPR[93]. Furthermore, it is not permitted to limit or restrict the right of access in a contract between the controller and the data subject.

167. According to Recital 63, the right of access is granted to data subjects in order to be aware of, and verify, the lawfulness of the processing. The right of access enables, *inter alia*, the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of personal data[94]. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the purposes behind the request should be regarded as irrelevant[95].

6.2 Article 15 (4) GDPR

168. According to Art. 15(4) GDPR, the right to obtain a copy shall not adversely affect the rights and freedoms of others. Explanations about this limitation are given in the fifth and sixth sentences of Recital 63. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. When interpreting Art. 15(4) GDPR special caution has to be taken not to unjustifiably widen the restrictions laid down in Art. 23 GDPR, which are permissible only under strict conditions.

169. Art. 15(4) GDPR applies to the right to obtain a copy of the data, which is the main modality of giving access to the data processed (second component of the right of access). It is also applicable, and rights and freedoms of others shall be taken into account, if access to the personal data is exceptionally granted by other means than a copy. For example, there is no difference justified whether trade secrets are affected by providing a copy or by granting on site access to the data subject. Art. 15(4) GDPR is not applicable to the additional information on the processing as stated in Art. 15(1) lit. a.-h. GDPR.

170. 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 merely as examples, as, in principle, any right or freedom based on Union or

[93] Where the controller processes a large quantity of information concerning the data subject, as mentioned in recital 63 GDPR, the controller may request the data subject to specify the information or processing activities to which the request relates. See also section 2.3.1.
[94] CJEU, Joined Cases C-141/12 and C-372/12, YS and Others.
[95] This is without prejudice to any applicable national law that comply with the requirements posed by Art. 23 GDPR, see Chapter 6.4.

Member State law may be considered to invoke the limitation of Art. 15(4) GDPR[96]. Thus, the right to the protection of personal data (Art. 8 European Charter of Fundamental Rights) can also be considered as an affected right in terms of Art. 15(4) GDPR. Regarding the right to obtain a copy, the right to data protection of others is a typical case where the limitation needs to be assessed. Furthermore, the right to confidentiality of correspondence has to be taken into account, for example with regard to private e-mail-correspondence in the employment context[97]. It is important to note that not every interest amounts to "rights and freedoms" pursuant to Art. 15(4) GDPR. For example, the economic interests of a company not to disclose personal data do not reach the threshold for the recourse to the exemption in Art. 15(4) as long as there are no trade secrets, intellectual property or other protected rights affected.

171. "Others" means any other person or entity apart from the data subject who is exercising their right of access. Hence, the rights and freedoms of the controller or processor (in keeping trade secrets and intellectual property confidential for example) might be considered. If the EU legislator wanted to exclude controllers or processors rights and freedoms, it would have used the term "third party", which is defined in Art. 4(10) GDPR.

172. 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. The controller must be able to demonstrate that in the concrete situation, rights or freedoms of others would, in fact, be impacted.

> **Example 34:** A person who is now an adult was cared for by the youth welfare office over a number of years in the past. The corresponding files may possibly contain sensitive information about other persons (parents, social workers, other minors). However, a request for information from the data subject cannot generally be rejected for this reason with reference to Art. 15(4) GDPR. Rather, the rights and freedoms of others must be examined in detail and demonstrated by the youth welfare office as the controller. Depending on the interests in question and their relative weight, providing such specific information may be rejected (e.g. by redacting names).

173. 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[98]. Hence also the exercise of the right of access has to be balanced against other fundamental rights in accordance with the principle of proportionality. When the Art. 15(4) GDPR assessment proves that complying with the request has adverse (negative) effects on other participants' rights and freedoms (step 1), the interests of all participants need to be weighed taking into account the specific circumstances of the case and in particular the likelihood and severity of the risks present in the communication of the data. The controller should try to reconcile the conflicting rights (step 2), for example through the implementation of appropriate measures mitigating the risk to the rights and freedoms of others**.** As emphasised in Recital 63, protecting the rights and freedoms of others by virtue of Art. 15(4) GDPR should not result in a refusal to provide all information to the data subject. This means, for example, where the limitation applies, that information concerning others has to be rendered illegible as far as possible instead of refusing to provide a copy of the personal data. However, if it is impossible to find

[96] The weight or priority of the conflicting rights and freedoms is not a question of the definition of the terms "rights and freedoms". However, balancing of such interests is part of a second step of the assessment, whether Art. 15(4) is applicable. See para. 173 below.

[97] ECHR, Bărbulescu v. Romania, no 61496/08, para. 80, 5 September 2017.

[98] See, for example, also CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 November 2010, para. 48.

a solution of reconciliation of the relevant rights, the controller has to decide in a next step which of the conflicting rights and freedoms prevails (step 3).

Example 35: A retailer offers its clients the possibility to order products via a hotline operated by its customer service. For the purpose of proving the commercial transactions, the retailer stores a call recording, in accordance with the strict requirements of applicable legislation. A customer wants to receive a copy of the conversation he had with an agent of the customer service. In a first step, the retailer analyses the request and realises that the record contains personal data that also relate to someone else, namely to the agent of the customer service. In a second step, in order to assess whether providing the copy would affect the rights and freedoms of others, the retailer has to balance the conflicting interests, especially taking into account the likelihood and severity of possible risks to the rights and freedoms of the customer service agent, that are present in the communication of the record to the client. The retailer concludes that there are very limited personal data relating to the customer service agent in the record, only his voice. The retailer/controller finds that the agent is not easily identifiable. Moreover, the content of the discussion is of a professional nature and the data subject was the interlocutor. On the basis of the aforementioned circumstances the controller objectively concludes that the right to access does not adversely affect the rights and freedoms of the agent of the customer service and therefore, the controller may provide the data subject with the full record, including the parts of the voice record that relate to the agent of the customer service.

Example 36: A client of a medical supply store wants access to the measuring results concerning her legs on the basis of Art. 15 GDPR. The medical supply store had measured the data subject's legs in order to craft individual medical compression stockings. Apparently the medical supply store had a lot of experience and had established a special technique to measure accurately. After the measuring in the medical supply store, the client wants to use the measuring results to buy cheaper socks elsewhere (ordering them in an online-shop). The medical supply store partially refuses access to the data on the basis of Art. 15(4) GDPR claiming that due to their special, accurate measuring techniques the results were protected as trade secrets. If and in so far the controller is able to prove that:

- providing the data subject with information about the measuring results is not possible without revealing how the measurements were taken and
- the information about how the measurements were taken including, if relevant, the exact determination of the measuring points are trade secrets

they may apply Art. 15(4) GDPR.

The controller would still have to provide as much information as it could about the measuring results that would not reveal its trade secret, even if that would imply the effort to revise and edit the results.

Example 37: GAMER X is registered as a user on the gaming platform of PLATFORM Y. One day, GAMER X is notified that his online account has been restricted. As he is unable to log in anymore, GAMER X asks the controller for access to all personal data relating to him. In addition, GAMER X requires access to the reasons for the account restriction. PLATFORM Y, the controller of the online gaming platform with which the request has been lodged, informs the users in its general terms and conditions available on its website, that any kind of cheating (mainly by the use of third party

software) will entail a temporal or permanent ban from its platform. PLATFORM Y also informs the users in its privacy policy about the processing of personal data for the purpose of detecting gaming cheats, in accordance with the requirements set out in Art. 13 GDPR.

Upon receipt of GAMER X's request for access, PLATFORM Y should provide GAMER X with a copy of the personal data processed about GAMER X. Regarding the reason for the account restriction, PLATFORM Y should confirm GAMER X that it decided to restrict GAMER X's access to online games due to the use of one or repeated gaming cheats which are in violation with the general terms of use. In addition to the information provided about the processing for the purpose of gaming cheat detection, PLATFORM Y should grant GAMER X access to the information it has stored about GAMER X's gaming cheats which led to the restriction. In particular, PLATFORM Y should provide GAMER X with the information that led to the restriction of the account (*e.g.* log overview, date and time of cheating, detection of third party software,…) in order for the data subject (*i.e.* GAMER X) to verify that the data processing has been accurate.

However, according to Art. 15(4) GDPR and Recital 63 GDPR, PLATFORM Y is not bound to reveal any part of the technical operation of the anti-cheat software even if this information relates to GAMER X, as long as this is can be regarded as trade secrets. The necessary balancing of interests under Art. 15(4) GDPR will have the result that the trade secrets of PLATFORM Y preclude the disclosure of this personal data because knowledge of the technical operation of the anti-cheat software could also allow the user to circumvent future cheat or fraud detection[99].

174. If controllers refuse to act on a request for the right of access in whole or in part under Art. 15(4) GDPR, they have to inform the data subject of the reasons without delay and at the latest within one month (Art. 12(4) GDPR). The explanatory statement has to refer to the concrete circumstances in order to allow the data subjects to assess whether they want to take action against the refusal. It must include information about the possibility of lodging a complaint with a supervisory authority (Art. 77 GDPR) and seeking judicial remedy (Art. 79 GDPR).

6.3 Article 12(5) GDPR

175. 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.

176. 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 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.

6.3.1 What does manifestly unfounded mean?

177. 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

[99] The extent of the information provided to individuals will be heavily context dependent, taking into account the nature of the controller and the nature of the breach of the terms of service. In some cases, it may only be possible for the controller to provide basic information in response to an access request to which Art. 15(4) applies.

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) GDPR in terms of requests for the right of access.

178. Furthermore, it is important to recall that prior to invoking the restriction, controllers must carefully analyse the content and scope of the request. For example, a request should not be regarded as manifestly unfounded if the request is related to the processing of personal data not subject to the GDPR (in this case, the request should not be dealt with as an Art. 15-request at all).

179. Other cases in which the applicability of Art. 12(5) GDPR is questionable are requests related to information or processing activities that are clearly and obviously not subject to the processing activities of the controller.

> **Example 38**: A data subject addresses a request to a municipal authority concerning data that are processed by a state authority. Instead of arguing that the request is manifestly unfounded it would be more suitable as well as easier for the authority addressed to confirm that these data are not being processed by the authority (first component of Art. 15 GDPR: "whether" personal data are being processed)[100].

180. A controller should not presume that a request is manifestly unfounded because the data subject has previously submitted requests which have been manifestly unfounded or excessive or if it includes unobjective or improper language.

6.3.2 What does excessive mean?

181. 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*.

182. 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 controller[101]. 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.

183. In case of subsequent requests, it has to be assessed whether the threshold of reasonable intervals (see Recital 63) has been exceeded or not. Controllers must take into account the particular circumstances of each case carefully.

184. For example, in the case of social networks, a change in the data set will be expected at shorter intervals than in the case of land registers or central company registers. In the case of business associates, the frequency of contacts with the customer should be considered. Accordingly the "reasonable intervals" within which data subjects may again exercise their right of access are also different. The more often changes occur in the database of the controller, the more often data subjects may be permitted to request access to their personal data without it being excessive. On the other

[100] A different question is whether the authority which the access request was addressed to is entitled to transmit the request to the competent state authority.
[101] According to the second sentence of Article 15(3), the controller may charge a reasonable fee for further copies requested.

hand, a second request by the same data subject could be considered to be repetitive in certain circumstances.

185. When deciding whether a reasonable interval has elapsed, controllers should consider the following in the light of the reasonable expectations of the data subject:

- how often the data is altered – is information unlikely to have changed between requests? If a data pool is obviously not subject to a processing other than storage and the data subject is aware of this, e.g. because of a previous request for the right of access, this might be an indication for an excessive request;
- the nature of the data – this could include whether it is particularly sensitive;
- the purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed;
- whether the subsequent requests concern the same type of information or processing activities or different ones[102].

Example 39 (carpenter): A data subject lodges access requests **every two months** with the carpenter that manufactured a table for them. The carpenter answered the first request completely. When deciding whether a reasonable interval has elapsed, one should consider that the carpenter only occasionally (first bullet point above) and not as part of its core activity processes and collects personal data and it is even less likely that the carpenter often provides services to the same data subject. Indeed, in the case, the carpenter did not provide more than one service to the data subject, rendering it unlikely that changes occurred in the dataset concerning the data subject. Notably given the nature and amount of the personal data processed, the risks related to the processing can be considered as low (second bullet point above), such as the purpose of the processing (billing purposes and compliance with obligation to keep records) is not likely to cause detriment to the data subject (third bullet point above). The request furthermore concerns the same information as the last request (forth bullet point above). Such requests may as a consequence be regarded as excessive due to their repetitiveness.

Example 40 (social media platform): A social media platform whose core business is the collection and/or processing of personal data of the data subject carries out large-scale complex and continuous processing activities. A data subject that uses the services of the platform lodges access requests **every three months**. In this case, frequent changes to the personal data relating to the data subject are highly likely (first bullet point above), the broad range of collected data includes inferred sensitive personal data (second bullet point above) processed for the purpose of showing relevant content and network members to the data subject (third bullet point). Access requests every three months may - under these circumstances - in principle not be regarded as excessive due to repetitiveness.

Example 41 (credit agencies): As with social networks, it cannot be ruled out that modifications of the relevant data held by credit agencies will occur at much shorter intervals than in other areas (first

[102] If the subsequent request concerns the same type of information in scope AND time, this is not a question of excessiveness but a question of request for an additional copy, see section 2.2.2.2.

bulletpoint above). This results from numerous factors of which the data subject, as a person from outside, is usually not aware due to the complexity of the business model. The answer to the question as to which types of data were collected for a score value calculation by the controller and which are currently included in the calculation can therefore only be provided by the credit agency itself. In addition, data processing through credit agencies and the resulting score value can have far-reaching consequences for the data subject with regard to intended legal transactions, such as the conclusion of purchasing, rent or leasing contracts (third bullet point above).

It is not possible to generally determine any specific interval in which the submission of a further access request could be deemed excessive under Art. 12(5) second sentence GDPR. An overall consideration of the circumstances of the individual case is rather required. However, given the importance of data processing for the data subjects' reality of everyday life, it can be assumed that a **one-year interval** between information provided free of charge will in any case be too large for the request to be considered excessive. If a request is submitted within a very short interval, the decisive factor should be whether the data subject has reason to assume that the information or the processing has changed since the last request. For example, if the data subject has conducted a financial transaction, such as taking a loan, the data subject should be entitled to request access to the credit information even though such a request was submitted and responded to shortly before.

186. 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.

187. If a request overlaps with a previous request, the overlapping request can generally be regarded as excessive, if and insofar as it covers exactly the same information or processing activities and the previous request is not yet complied with by the controller without reaching the state of "undue delay" (see Art. 12(3) GDPR). In practice, as a consequence both requests could be combined.

188. 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 excessive[103]. 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.

189. Against this background, a request should not be regarded as excessive on the ground that:

- no reasons are given by the data subject for the request or the controller regards the request as meaningless;
- improper or impolite language is used by the data subject;
- the data subject intends to use the data to file further claims against the controller.[104]

190. On the other hand, a request may be found excessive, for example, if:

[103] No proportionality test, see above para. 166.
[104] This is without prejudice to any applicable national law that comply with the requirements posed by Art. 23 GDPR, see Chapter 6.4.

- an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller or
- the request is malicious in intent and is being used to harass the controller or its employees with no other purposes than to cause disruption, for example based on the fact that:
    - the individual has explicitly stated, in the request itself or in other communications, that it intends to cause disruption and nothing else; or
    - the individual systematically sends different requests to a controller as part of a campaign, e.g. once a week, with the intention and the effect of causing disruption[105].

6.3.3 Consequences

191. 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.

192. The EDPB points out that controllers are – on the one hand – not generally obliged to charge a reasonable fee before refusing to act on a request. On the other hand, they aren´t completely free to choose between the two alternatives either. In fact, controllers have to make an adequate decision depending on the specific circumstances of the case. Whereas it is hardly imaginable that charging a reasonable fee is a suitable measure in case of manifestly unfounded requests, for excessive requests – in line with the principle of transparency – it will often be more appropriate to charge a fee as a compensation for the administrative costs the repetitive requests are causing.

193. 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 proper documentation of the underlying facts. In line with Art. 12(4) GDPR, if controllers refuse to act on an access request in whole or partly, they must inform the data subject without delay and at the latest within one month of receipt of the request of
    - the reason why,
    - the right to lodge a complaint with a supervisory authority,
    - the possibility to seek a judicial remedy.

194. 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.

195. Unjustified rejections of requests of the right of access can be regarded as infringements of data subject rights pursuant to Art. 12 to 22 GDPR and can therefore be subject to the exercise of corrective powers by competent supervisory authorities, including administrative fines based on Art. 83(5)(b) GDPR. If data subjects consider there is an infringement of their data subject rights, they have the right to lodge a complaint based on Art. 77 GDPR.

[105] "Systematically sending as part of a campaign" means that requests which could easily be combined to one are artificially split into not just a few but many single pieces by the data subject with the apparent intention to cause disruption.

6.4 Possible restrictions in Union or Member States law based on Article 23 GDPR and derogations

196. 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[106].

197. 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. Furthermore, it is important to note, that restrictions of the right of access in Member States (or Union) law which are based on Art. 23 GDPR must strictly fulfil the conditions laid down in this provision. The EDPB has issued the Guidelines 10/2020 on restrictions under Art. 23 GDPR with further explanations on this. In terms of the right of access, the EDPB recalls that controllers should lift the restrictions as soon as the circumstances that justify them no longer apply[107].

198. Legislative measures which relate to 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[108].

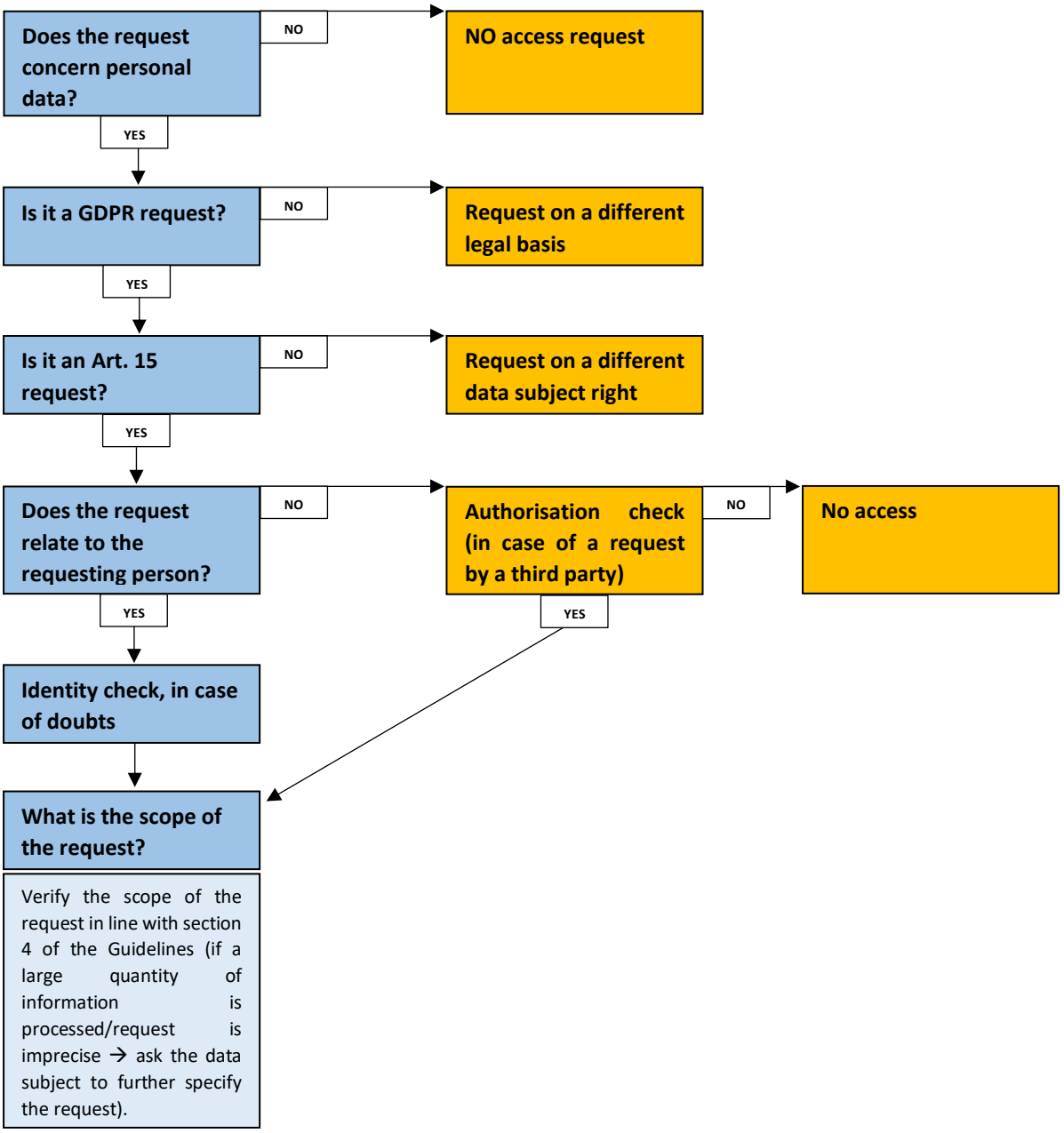
[106] See for example sections 32 to 37 of the German Federal Data Protection Act (BDSG), sections 16 and 17 of the Norwegian Personal Data Act and chapter 5 of the Swedish Data Protection Act.

[107] Paragraph 76 of the Guidelines 10/2020 on restrictions under Art. 23 GDPR, Version 2.0, adopted on 13 October 2021.

[108] Paragraph 12 of the Guidelines 10/2020 on restrictions under Art. 23 GDPR, Version 2.0, adopted on 13 October 2021. Section 34 (3) of the German Federal data protection act for example states that if a public authority doesn´t provide information to a data subject complying with a request for the right of access because of certain restrictions, such information shall be provided to the federal supervisory authority at the request of the data subject, unless the responsible supreme federal authority (of the authority which was subject to the request) determines in the individual case that doing so would endanger the security of the Federation or a Land. The Italian DPCode provides for indirect access (through the authority) in case the access could impact with adverse consequence on a number of interests (e.g. Interest to contrast money laundering) see Art. 2-L of the Italian DPCode.

ANNEX – FLOWCHART

Step 1: How to interpret and assess the request?



Step 2: How to answer the request (1)?

3 main components of the right of access (structure of Art. 15)		
Confirmation whether or not personal data are being processed	Access to the personal data	Additional information on purposes, recipients etc. (Art. 15(1)(a) – h))

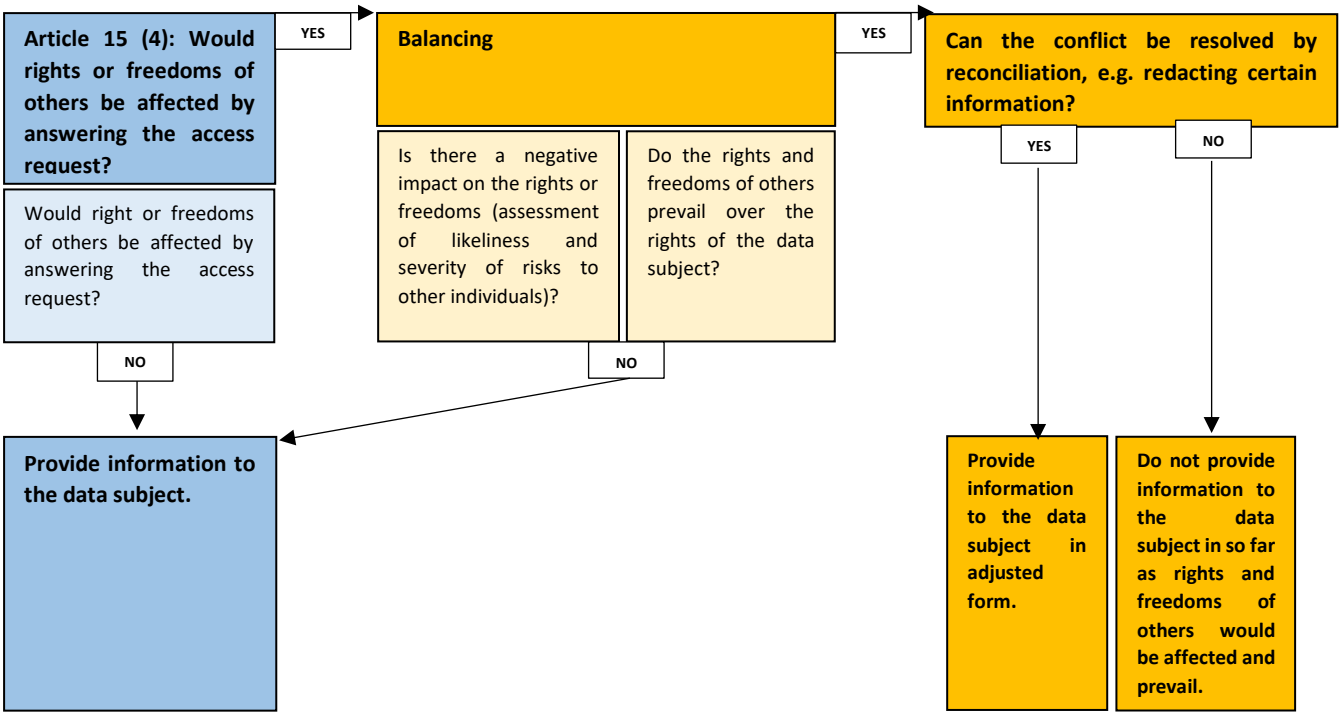
Step 2: How to answer the request (2)?

Take appropriate measures			
Art. 12(1): concise, transparent, intelligible, easily accessible	Art. 12(2): facilitate the excercise of the right of access		
Choose between different means	Provide a copy, if not agreed otherwise (Art. 15(3))	Use a layered approach if appropriate (most relevant in online-context)	Timing – without undue delay, in any event within one month (extension by two further months in exceptional cases) (Art. 12 (3))

Step 2: How to answer the request (3)?

How can the controller retrieve all data about the data subject?			
Define search criteria – based on what the data subject has provided, other information that the controller holds about the data subject and the factors on which data is structured (e.g. customer number, IP-addresses, professional title, family relations etc.).	Identify any technical functions that may be available to retrieve data.	Search through all relevant IT or non-IT filing systems.	Compile, extract or otherwise collect data that relates to the data subject in a way that fully mirrors the processing, i.e. that includes all personal data regarding the data subject, and enables the data subject to be aware of and verify the lawfulness of the processing. The retrieving of the information could be done case-by-case or, when relevant, by the use of a privacy by design tool already implemented by the controller.

Step 3: Checking limits and restrictions (1)



Step 3: Checking limits and restrictions (2)