Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

CEDPO comments on

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

CEDPO welcomes the Guidelines on the right of access and provides the EDPB with the following comments.

GENERAL OBSERVATION

CEDPO would welcome in an annex examples of practical implementation of the EDPB recommendation in responding to access requests in recurring real life use cases, which would exemplify how to make a distinction between personal and non-personal data, including business data; how to provide information in an intelligible form; how to respect the rights of others; when to provide a document and when to provide only the personal data and how to do it …

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

Section 2.3.3, Para 39: Information about the subsequent rectifications or deletions

The information on data rectification or deletion is not part of the transparency principle according to Art. 13 and 14 GDPR, nor is it mentioned in Art. 15 GDPR. Art. 19 GDPR requires controllers to communicate rectification or deletion to recipients of data, not the data subject. The information of the data subject by the data controller of subsequent rectifications and deletions can be mentioned as a best practice but should not be made an obligation.

GENERAL CONSIDERATION REGARDING THE ASSESSMENT OF ACCESS REQUEST

Section 3.1.1, Para 47: Other provisions regulating access to a certain category of data

As the EDPB mentions, the right of access needs to be distinguished from similar rights. Sect 630g of the German Civil Code for example allows patients to inspect their medical records.

Requesting a copy of the medical record us subject to the reimbursement of the treating party whereas Art. 15(3) GDPR allows for a first copy of personal data free of charge. CEDPO would welcome clarification on how to deal as data controller with two overlapping rights, especially concerning reimbursement of related costs.

Section 3.1.2: form of the request

CEDPO would like it to be clarified if a data controller who provides electronic means for data subjects to exercise their rights through an online request tool must also in parallel make available to data subjects dedicated email address and postal address.

Section 3.3, Para 69: Proportionality assessment regarding identification of the requesting person

Groups-of undertaking are facing the challenge that they have a single-point of contact for data subject requests and central data processing activities. This might lead to a situation where the entity acting as single point of contact is unable to identify the data subject in the group central systems.

Clarification is welcome whether the single point of contact may ask the data subject to provide background to specify his/her request, for example by asking for the group company he/she has been in touch with, contact names and dates within the group, email exchanges and any other useful information which can help find in which context personal data about the data subject would have been processed.

CEDPO would welcome this opportunity regardless of whether a large quantity of data is processed.

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

Section 4.3: Information on the processing and on data subject rights and specific information on the categories of recipients

The Guidelines provide for many additional sets of information to communicate to the data subject exercising his/her right of access.

Some information is not required *per se* by the GDPR. This is for instance the case for the information regarding the fact that the data subject may become controller if he/she obtains personal data regarding himself/herself but also other individuals while exercising his/her right of access (para 104).

Other information requirements result from an overly broad interpretation of GDPR provisions. This is for instance the case of the indication regarding the categories of data processed for each purpose, which does not appear in the GDPR (para 112). This is also the case of the name of the actual recipients when the mention of only categories of recipients is considered as sufficient at Articles 13 to 15 (para 115).

Such information requirements entail an excessive burden for controllers which goes beyond what was expected by the European regulator.

In addition, some of these requirements may impede controllers' ability to pursue their business activities as they would force them to reveal trade secrets. This is especially the case of the obligation to name every recipient whereas the lists of suppliers and clients of companies are very valuable information for companies and are protected against disclosure as trade secrets.

With reference to para 115, the Guidelines recommend that the "controller should generally name the actual recipients instead of the categories of recipients.

This level of details may sometimes be excessively burdensome, mainly when the number of recipients is high, which may for instance be the case when the access request relates to a large amount of personal data processed. The data controller may resort to several vendors for various similar types of services (e.g. numerous IT providers, training, recruiting, banking, payroll, accounting, legal, auditing, consultants, contractors …).

CEDPO believes that in such instances transparency can be achieved in answering the access request by providing the specific name of the main vendors which the data subject would consider as the most relevant and then the categories of other less meaningful recipients.

HOW CAN A CONTROLLER PROVIDE ACCESS?

Section 5.1: How can the controller retrieve the requested data?

Rights and freedom of other parties may not only be affected when communicating a copy of the data to data subjects. The retrieval of the data may also affect said rights and freedoms.

This would be for instance the case when a data subject requests the copy of personal data contained in all emails sent by and to employees of the data controller. To comply with such request, the data controller would need to scan the emails of its employees which cannot be allowed (see for instance CNIL's publication on the right of access to emails by employees: https://www.cnil.fr/fr/le-droit-dacces-des-salaries-leurs-donnees-et-aux-courriels-professionnels).

In that case, a balance should be applied between the rights and freedoms affected and the right of access of the data subject. If the firsts prevail over the second, the data controller should not be forced to proceed to such retrieval.

Sections 5.2.3 and 5.2.5, Para 139 and 147: Requirement that the information is an 'intelligible' and relevant format

The controller must take the necessary measures to ensure that the information is 'intelligible' so that the data subject understands the data. The information shall be provided, where appropriate, by electronic means in a commonly used electronic form.

Taking into account that the data subject should not be obliged to buy specific software to get access to the information, CEDPO would like confirmation that it is appropriate for data controller to provide the data subject with a particular software that allows him to download the information easily and free of charge.

Section 5.2.4, Para 143: Layered approach

When deciding the information to be given in the different layers, the data controller should consider what information the data subject would regard as most relevant, considering the

information on the processing which has the most impact on the data subject and processing which could surprise them.

In this regard, CEDPO would welcome examples of data processing activities which could "surprise data subjects" and guidance on the parameters to be taken into account when deciding processing which could 'surprise' the data subject, considering that data subjects have normally already provided with notice of the processing under articles 13 and 14..

Section 5.2.5, Para 150: unaltered copy of the personal data

Regarding the format of the information to be provided to the data subject, CEDPO would welcome practical examples of implementation of the EDPB requirement that the copy of the personal data must be unaltered. A hash checksum for example can be deemed appropriate if the controller provides direct access to files. When giving access to a compilation of data, a hash could only ensure that the compiled file transferred to the data subject has not been altered. It would lack information regarding the question whether the personal data included has been changed.

Section 5.3, Para 157: starting point of the time limit

The one month time limit starts when the controller has received an art 15 request. The EDPB draft Guidelines specify that it is "when the request reaches the controller" through one of its official channels" but that "it is not necessary that the controller has in fact taken notice of it".

CEDPO would like to point that, while the controller must monitor its official channels, requests may reach the controller outside of business hours, including on week ends or during bank holidays. As in several countries organizations implement a "right to disconnect" and work for the well being of their employees, it cannot be expected from controllers to have "received" the request during these times. An online request made after usual business hours of the data controller, during weekends or bank holidays should be considered as received the next business day. That business day should be the starting point of the one month time limit.

Section 5.3, Para 157 and Section 2.3.1, Para 35: deadline extension in the event of a request for clarification/identity verification by the data controller

The possibility for a data controller to request clarification by the data subject on the scope of his/her request and/or to verify the identity of the data subject is clearly and rightly so acknowledged.

However, such request, when duly justified, should entail automatically a suspension of the one-month deadline to reply to the data subject's request and should not only be a possibility subject to subjective assessment. This would be otherwise a source of legal insecurity for controllers, even when their requests for clarification would be duly justified.

LIMITS AND RESTRICTIONS OF THE RIGHT OF ACCESS

Section 6.1, Para 164: Proportionality

According to Art: 15(4) GDPR the right to obtain a copy shall not adversely affect the rights and freedoms of others. As the EDPB acknowledges, the rights and freedoms of the controller or processor might also come into consideration.

The right of access which is specifically mentioned in Art. 8(2) of the EU Charter needs to be balanced with the rights of others including the right to conduct a business according to Art. 16 of the Charter. Besides, the concept of personal data having to be processed fairly according to Article 8(2) of the EU Charter and Article 5(1)(a) GDPR hovers over the entire processing. This is why, no disproportionate effort shall be demanded of the controller per se. However, very strict standards must be applied with regard to the disproportionality of transparency rights being an important right. The following criteria could be applied when assessing the proportionality of an access request:

Back-ups: Backups are usually designed to replicate a current status of a live system leading to identical data. When assessing an access request controllers should, on the one hand, be allowed to assess if there is a possibility of different data in backups compared to live systems at all (e.g. by checking lifecycle of a backup). Controllers should also be allowed to assess in a second step whether obtaining additional information in backups involves a disproportionate effort. It should be borne in mind that measures concerning availability controls on personal data are a legal obligation according to Art. 32(1)(b) GDPR. So primarily it is up to the data controller to assess the lawfulness of such a processing in order to avoid fines.

Volume: Large organisation process high volumes of data in a structured and unstructured way. Such large volumes often result from a legal obligation to store data. In some cases, it can be considered to be disproportionate to grant access to data which is solely processed to comply with a legal obligation. Besides, such data is often stored in archives which are difficult to access for the controller himself.

Indexation: The controller will have to search for personal data throughout all IT systems and non-IT filing systems. Not all systems are structured in a way to identify data subjects easily

and accurately. Individuals in unstructured data can be referred to in several ambiguous ways using abbreviations or acronyms.

Mixture of information: Not every information is an information on the data subject but includes business information or personal data of other data subjects. Controllers have to manually redact or exclude information, especially when having to assess unstructured data sets. Mixed datasets therefore should be taken into account when assessing the proportionality of the efforts involved for the controller.

At the end of the assessment the controller would have to document the balancing of interest taking into account whether the provision of information to the data subject would involve a disproportionate effort and the interest of the data subject in the provision of information is to be regarded as minor in the circumstances of the individual case.

Section 6.2, Para 166: Limits to the Right of Access

Paragraph 166, which concerns the balancing of the data subject's rights with the rights and freedoms of others, where responding to an access request might adversely affect the latter, could benefit from less strict language.

The following excerpt is particularly relevant: '*That right [of access] 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.*'

With respect to the highlighted sentence, it can't be predicted categorically that there won't be any situation ever where, in the interests of balancing rights in a fair manner, the results of those considerations may well necessitate refusing to provide all information. The sentence could, perhaps, be qualified as such: 'However, the data controller should endeavour to ensure that the result of those considerations should not, *where possible*, be a refusal to provide all information to the data subject.'

Section 6.2, Para 171: reconciliation of right of access with other rights and freedoms

There is another way to reconcile a right of access with other rights and freedoms than redacting or extracting data from documents. In some case, it may be appropriate to transfer only aggregated data.

This solution is for instance suggested by the European Data Protection Supervisor regarding selection procedures in order to preserve the principle of the secrecy of selection board proceedings and to avoid communicating information regarding the individual marks or assessments attributed by each individual evaluator/jury member involved. In that case, for the EDPS, '*the average mark resulting from the aggregation of the individual marks/assessments by all evaluators/jury members should be disclosed in a transparent manner*' (EDPS, Guidelines on the Rights of Individuals with regard to the Processing of Personal Data, 2014, pp. 13-14).

Section 6.3.1: What does manifestly unfounded mean?

The definition of an unfounded access request remains unclear.

According to the present version of the Guidelines, an access request would be unfounded '*if the requirements of Art. 15 GDPR are clearly and obviously not met when applying an objective approach'*.

However, it is difficult to identify which requirements it is referred to as the Guidelines tend rather to exclude any requirement in terms of form, content and purpose for the access request.

If it becomes clear for a data controller that the motivation of a request by a data subject is not to safeguard his or her personal rights under the GDPR but to pursue other objectives, it must be possible for controllers to refuse to act.

Accordingly, controller shall be allowed to deny access requests used as leverage in judicial or extrajudicial disputes with them.

Art. 12(5) GDPR does not restrict such right to refuse to repetitive requests by data subjects as the wording 'in particular' indicates. With regard to the accountability principle the controller shall bear the burden of demonstrating the manifestly unfounded character of the request.

Some examples of unfounded access requests and/or of the requirements to be considered would help to clarify these paragraphs.

Section 6.3.2, Para 188: Examples of what 'excessive' means

Paragraph 88, which describes what might be considered 'excessive' in the context of Article 12(5) of the GDPR could benefit from additional examples.

Specifically, the below examples would offer additional useful guidance on deciding whether a request is excessive:

- The request makes unsubstantiated accusations against the controller or its employees,
- The individual is targeting a particular employee against whom they have some personal grudge.

11/03/2022

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu