Spolek pro ochranu osobních údajů

Comments on the EDPB's draft "Guidelines 01/2022 on data subject rights – Right of access"

We welcome the opportunity to present our comments to the recently published EDPB draft Guidelines 01/2022 on data subject rights – Right of access (Guidelines).

General comments

We greatly appreciate the EDPB for preparing this comprehensive opinion. It is really very complex and addresses a number of issues. We are afraid that the level of the detail and repeating of the GDPR principles could negatively affect the overall comprehensibility of the document as such and do not bring any added value. Also its scope can be a bit discouraging for some smaller controllers, as they will have no capacity to familiarise themselves with so much text. We believe the document should focus more on creating a practical framework for a correct application of the GDPR in the everyday life of the DPOs and privacy experts. Perhaps the solution could be to expand the introductory executive summary.

As far as the content itself is concerned, we must point out that we sometimes see too much simplification of the issues. We know from practice of the members of our association that there are several methods in exercising the right of access. In particular, we recommend adopting a more pragmatic approach that takes into account both the importance of the right of access from the point of view of data subjects and the legitimate interests of controllers. E.g. we often find that the data subjects remain inactive after initial contact in case of additional questions. In such cases, or in cases where the request is unclear and the data subject refuses to specify it, the request should not be considered "qualified" and the controller should be able not to proceed with it until the data subject provides additional information requested.

Not much attention is paid to the protection of rights of the third parties and of the controller (e.g. confidentiality protection, intellectual property rights protection). In this direction we would appreciate this point of view to be more acknowledged/addressed by the Guidelines.

In our view, it is also important to take into account the controller's approach to data subjects' requests. If the controller is clearly acting in good faith and is trying to comply reasonably with the requests of the data subjects, such procedure should be considered compliant with the GDPR. It should also be noted that data subjects should also take care of their rights and controllers cannot be blamed for non-compliance with GDPR if the data subject does not provide the necessary cooperation to the controller.

In addition, we would like to point out that some of the requirements imposed on EDPB in the guidelines are rather unrealistic from the controllers' point of view (e.g. access to data stored in backups). Both the rights of data subjects and the requirements for controllers need to be balanced, including in terms of the resources that controllers can (is obliged to) make available

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

to meet the GDPR requirements. Especially at a time of impending crisis and transformation of the society, a realistic framework for controllers needs to be established.

Specific comments

In Paragraph 13 EDPB states: „*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)."*

We believe, that such an approach is only partially correct. In some cases, it will also be necessary to also examine "why" the right of access is exercised. E.g., this may be important for a proper assessment of a refusal of access pursuant to Article 15 (4) or for refusals in cases provided for by specific rules (e.g. whistleblowing and protection of whistleblowers).

We very much appreciate the EDPB's position, which (quite rightly) confirms that the right of access does not apply to copies of original documents (see paragraph 23).

We do not believe that the issue of a "reasonable fee" (see paragraph 30) is linked to the principle of accountability. Although the controller is required to demonstrate the adequacy of the costs claimed (especially in the event of a dispute, the DPA may request this information), this issue is not linked to the accountability principle under Article 5 (2), which is connected „only" to topics listed in Article 5 (1) of GDPR.

We fully support the view (see paragraph 35 (b) of guidelines), that "*In situations where the controller processes a large amount 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."* On the other hand, we cannot agree that this can only be applied in this particular situation: *"These may arise 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.*" Our members routinely encounter cases where the general right of access is exercised, even though the data subject actually intends to obtain information on one part of processing or processed data only. From a procedural economy point of view, we believe that the data controller could request additional information from the data subject in these cases. An important aspect for us is whether the controller acts with regard to the circumstances in good faith (see above).

We would like to point out that the conclusion in paragraph 35 (c) that "*For example, confirmation of the processing of personal data itself (component 1) will mostly not be affected by the exception*." could be too simplistic. We would like to point out that there are a number of cases where even providing the fact that processing is taking place can be contrary to the purpose of the processing. An example might be the right to access request made by a person who suspects that his/her colleague has made a whistleblowing notification, whether this person is being investigated. Already simply answering "yes" in the early phase of whistleblowing notice examination would lead to disclosing the identity of the whistleblower (the similar applies for paragraph 166 and paragraph 167 regarding the additional information) and limit the purpose of the whole whistleblowing process. These cases are also common in the context of processing for journalistic purposes, etc.

Regarding the requirement in paragraph 39, that "*In order to comply with the principle of transparency, controllers should inform the data subject as of the specific point in time of the processing to which the response of the controller refers*." We must point out that, in practice, it might be difficult for controllers with complex processing activities to meet this requirement. We must also point out that such a requirement cannot be directly deduced from the GDPR. We believe that this requirement should be executed at the level of the *best practice* (and only for cases where it will be fair for the controller) but this is not a requirement arising from the law.

Rather unrealistic from the practical point of view is the requirement to notify changes occurred between the 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.*" We believe that it is necessary to adopt an interpretation of GDPR that allows, on the one hand, a reasonable overview of the processing for data subjects but, on the other hand, does not place a disproportionate burden on the controllers. Unfortunately, such an interpretation does not meet this requirement.

In the example in paragraph 40, it would be useful to provide a more detailed explanation of how the last sentence was meant *("In cases 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*"). Even when sending by e-mail, it is of course possible to encrypt the content and send the password to the content through another communication channel (which, for this purpose, could be provided by the data subject). Therefore, we do not understand the requirement for sending the USB-stick by registered letter post.

Unfortunately, paragraph 45 is also partially simplistic. Especially with regard to the case-law of the Court of Justice[1], the range of data that can be considered pseudonymised is very wide. We recommend emphasizing that in many cases it will be necessary for the data subject not only to provide an identifier, but also to provide credible evidence that it is his/her identification data in specific time (e.g., his / her IP address).

With regard to the view stated in paragraph 48, i.e., that the controller is obliged to assess the request himself if the data subject does not answer the additional question and does not provide any further explanation, we consider that this is from a practical point of view as an inappropriate concept. We know from practical experience that many data subjects submit applications and they will subsequently lose interest in processing (not rare are "strangely" worded requests sent late at night). It is not an exaggerated requirement for the data subject to clarify his request. If the data subject does not do so, even though he could and should have done so, in our opinion the controller is not obliged to respond to the original vague or unclear request. Without wanting to downplay the protection of personal data, it is necessary to draw attention to the ancient Roman legal principle of *vigilantibus iura scripta sunt.* And again, it would be appropriate to emphasize the concept of acting in good faith by the controller. An

[1] For example Judgment from 19 October 2016, in Case C-582/14, Patrick Breyer

extension of the 30-day response time should also be considered for unclear applications. The question here is WHEN the time limit for proceeding with the request actually starts running. We do believe it should be at the time of serving a qualified request by the data subject.

With regard to paragraph 49, we would like to draw attention to the interpretation of Article 23 of the GDPR as far as a potential conflict of European legal acts (not national law) is concerned. The GDPR is a “common regulation” and Article 23 of the GDPR does not constitute a "super-regulation" that should perhaps take precedence over other EU regulations. Therefore, in the event of a conflict between another EU regulation and Article 23 of GDPR, common legal principles such as “*lex posterior derogat legi priori*” and “*lex specialis derogat legi generali*” should apply. We would also appreciate the addition of specific practical examples for the case where, in addition to the right of access under the GDPR, a very special right of access under sectoral legislation is enshrined (e.g., access to medical records).

With regard to paragraphs 55 and 56, we believe that if the controller extensively publishes, and provides, easily accessible contacts for the exercise of rights under the GDPR, then if the request for access is sent to another contact (for example to the controller´s employee who deals with the data subject´s affairs on daily basis, as mentioned in paragraph 55), the time limit for processing the request should run from the internal transfer of request to the contact designated for the processing of the request. This interpretation could be limited to the situation only when this period from delivery to handover is reasonable and does not exceed a few days.

From a practical point of view, we recommend that you carefully consider placing additional demands on the controller that do not result from the GDPR, even if they are only in the good practice regime. In particular, the requirement to confirm receipt of the request by post (see paragraph 57) or to black information in ID cards (see paragraph 76) seems to be clearly disproportionate and lacks a clear legal basis.

We understand the remark given in the example of paragraph 67, i.e., that the data obtained from cookies are pseudonymous data (or data associated with pseudonymous identifiers), in disagreement with the opinion of the Austrian authority ruled in case GZ: D155.027, 2021-0.586.257 from 22.12.2021. Could you please clarify your position regarding this point?

Paragraph 69 imposes a new obligation on the data controller to “*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…”* in case of requiring additional information to identify the data subject. We find such an obligation clearly disproportionate and burdensome.

We understand the remark about the need for proportionality assessment in paragraph 69 in the way that such an assessment can be made entirely informally. Should the EDPB insist that such an assessment be documented, we draw attention to a significant increase in the administrative burden for the controller, which would be fully unjustified.

With regard to paragraph 72, we would like to point out that it is common practice to consider a data subject request sent from an e-mail address used as a registration address in the service as sufficient proof of identity of data subjects (in the context of usual internet services). From this point of view, it is not necessary to require him to log in to his account for identification.

Regarding paragraphs 74 and 75 we would like to point out, that the identification requirements should be reasonably proportional to the circumstances, taking into account in particular whether the controller knows the identification and contact details of the data subject or does have preexisting access credentials in place with the data subject. The personal data processed can range from trivial data up to financial data and even special categories of data. The identification requirements should match the importance and sensitivity of the data in question.

Where the data controller processes special categories of data or data of similar importance (for instance financial data) the controller should, in the absence of preexisting trustworthy credentials, be always entitled to require the provision of identity documents and to assess their integrity and validity. Where necessary for such assessment the data controller should have the right to reject identity documents or scans thereof which have been partially blackened or otherwise manipulated with.

Similarly, in situations where unlawful access to personal data could be harmful to the controller or the data subject, the controller should have the right to retain copies of identification data submitted. This aims in particular on situations where the personal data in question is of value similar to the identity copies themselves.

We consider it questionable to set a requirement that processing should be strictly necessary (see Example 2 in paragraph 76) where the GDPR does not require it. The law clearly distinguishes between cases where processing is “necessary” (see art. 6 of GDPR) and cases where it is strictly necessary (see for example ePrivacy Directive). We fully believe it is highly important to keep this distinction to respect the purpose of specific legislation.

We assume that the reference to "personal activity" in paragraph 91 also includes “household activity”, as stated in Article 2 (2) (c) of the GDPR.

Paragraph 95: Here we would like to point out that subjective comments can also represent the personal data of the commentator (who will often be identifiable to the subject concerned). The possible application of Article 15 (4) must therefore be carefully considered.

With regard to paragraphs 96 (and 98) and the overview of data provided, we must point out that we often find that the data subject is not even interested in providing some categories of data (for example security logs). At the same time, exporting such data will in most cases be a burdensome and time-consuming process for the controller. Therefore, it is always necessary to assess the data subject's requests carefully, also from the point of view of whether he/she really wants all types of data to be provided.

With regard to paragraph 105, we consider that the assessment of an identity theft case is rather simplistic. In our opinion, the controller should proceed very cautiously in such cases and always consider whether or not to release data relating to that person but clearly imposed by another person (suspected of identity thief). We could imagine situations where the release of the data (only) to the police in connection with the investigation could be a more appropriate solution. It cannot be ruled out that in the end it will be proven, for example, that there was no identity theft, but the situation was caused by mistake, etc.

Regarding paragraph 106, we would like to respectfully point out that Article 24 of the GDPR cannot be interpreted as requiring the controller to ensure that “no data breach occurs”. It is

the controller's responsibility under Article 24 to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. No provision of the GDPR can be interpreted as establishing an entirely objective liability of the controller for data breaches. In this context, we also refer to the decision of the Czech Supreme Administrative Court No. 1 As 238/2021 from 11.11.2021.

We consider the requirement to provide data from back-ups mentioned in paragraph 108 to be usually very unrealistic from a practical and mainly security point of view. Again, in our opinion, it is necessary to take into account whether the controller acts in good faith or not. It is also necessary to highlight that it is not always possible to observe from the system logs the extent of the deleted data (after all, such an approach would negate the effects of the deletion of data). It is also important that restoring data from a backup to a readable format can be in some systems a time-consuming and technically demanding process and can endanger business continuity management. We believe that a more balanced approach is needed in this regard, which takes into account practical procedures and problems.

Paragraph 111: We generally agree with the following: "*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 or the processing operations actually carried out with regard to the data subject making the request.*" On the other hand, always tailoring information to a *particular data subject* can be quite challenging and time and resource consuming. Rather, a compromise solution seems to be more appropriate - that the controller would prepare information aimed not at a specific data subject but at a specific group (e.g. "current customers", "former customers", "employees", etc.).

Similarly, we do not believe that the conclusions set out in the example in paragraph 113 are correct. In our view, the GDPR does not in Article 15 (1) (b) impose an obligation to provide completely targeted information. Specific information on specific data processed is ensured by the transmission of a copy of the data, the need to always individually select the data actually processed for the purposes of information according to Article 15 (1) (b) appears to be superfluous and unnecessarily burdensome for the controller.

Paragraph 115: The provision goes well beyond Art. 15 of the GDPR by requiring *"to name all data recipients, unless it would only be possible to indicate the category of recipients."* No such obligation can be derived from Art. 15(c) of the GDPR which sets out the obligation to *"provide information on the recipients or categories of recipients to whom the personal data have been or will be disclosed"*. As follows from the wording, the GDPR establishes no priority to either providing information on recipients or their categories and the choice is clearly in the controller´s disposition. This fact is also to be reflected in the provided example.

With regard to Article 15 (1) (c), we still believe that it is the controller's choice whether the controller will inform the data subject only about the categories of recipients, or specifically about the identity of recipients. A very good example is the situation described in paragraph 115. In practice, information about all hotels and travel agencies to which data of employees have been passed are often stored only in e-mails and not in a centralised database. Such a requirement would mean keeping further extensive centralised records, which we believe would be disproportionate (after all, the employee usually knows, for example, in which hotel

he or she spent the night) and would multiply the systems processing personal data in breach of the data minimisation principle.

Similarly, in paragraph 118: the example extends the existing obligation under Art. 15(g) of the GDPR on providing information with regards to the data source in case it is not collected from the data subject. The GDPR in this connection requires *"any available information"* to be served. However, the example in paragraph 118 discloses exact companies *"being involved exactly"* when it expects such additional information to be established later in time. Again, the GDPR does not extend the information obligation to be updated later, as it would pose a disproportionate burden on the controller and its processes.

With regard to paragraph 128, for the sake of completeness, we would like to point out that in specific cases it may be appropriate to provide information to the data subject from multiple sources within the controller (and not only from the department dealing with data protection issues). An example is the processing of data within a whistleblowing system, where the interest in protecting the identity of whistleblowers should prevail and (a relevant part of) requests for access should be handled by a person in charge of whistleblowing.

Regarding the last sentence in paragraph 128, we do not fully understand this example (clickstream, etc.), because it will often be data stored only on the end user's end device, to which the controller will not otherwise have access. We would appreciate further clarification regarding this issue.

Paragraph 140: We agree that information should, as far as possible, be provided in the language of the country where the controller provides its services (to not a negligible extent and if the service itself is offered in the language of that country), but this cannot be extended to an obligation for the controller to submit raw data processed in the language of that country (if the controller does not use a raw data translated to the specific language).

As far as the "commonly used electronic format" is concerned, we do not believe that it depends on the "expectations of the data subject", but rather on the commonly used formats in the industry.

With regard to paragraph 157, we consider that the question of when the legal act (access request) should be considered as delivered to the addressee must be resolved in accordance with the relevant national law. E.g. for example the request delivered to the letter-box on the weekend can only be considered delivered on Monday etc.

In paragraph 168, we would welcome a more detailed view of the EDPB on the question of issuing information contained in the controller's (e-mail) correspondence, as this issue is dealt with very inconsistently in the legal practice across the Member States.

Paragraph 171: We believe that it is necessary to carefully consider the use of Article 15/4, as there is also a risk for the agent of the customer service that the recording of his/her voice could be misused by the data subject.

The explanation of paragraph 175 is not very clear. It would also be useful to provide some examples.

We believe that it is not excluded that a request for access is considered excessive even if it includes not exactly the same information (in the case when the volume of changes will be minimal and could be expected from the data subject's point of view). See paragraph 185.

Regarding paragraph 190, we would like to note that according to Article 12 (5), it is indeed up to the controller to decide whether to request payment of a fee or to reject such a request. We agree that in some cases could be more appropriate to charge a fee, but the final decision as to which option to use is up to the controller.

We are grateful for the opportunity to provide our comments on the draft Guidelines.

Prague, 11.3.2022

JUDr. Vladan Rámiš, Ph.D.
Chairman of the Committee
Spolek pro ochranu osobních údajů

Alice Selby, LLM, Ph.D., CIPP/E, CIPM
Member of the Committee
Spolek pro ochranu osobních údajů