

11.03.2022

To the European Data Protection Board

Brussels

Dear Sirs,

Re: Feedback to the EDPB Draft Guidelines 01/2022 on data subject rights-Right of access

I welcome the great opportunity to provide my feedback on the above Draft Guidelines.

For any information or clarification, please contact me at the email address maria@privacyminders.com

2.AIM OF THE RIGHT OF ACCESS, STRUCTURE OF ARTICLE 15 GDPR AND GENERAL PRINCIPLES		
1.	2.2.2. Provisions on Modalities 2.2.2.1 Providing a copy Para. 25, p.13	<p>In line with the broad interpretation of the notion of a copy, it may be clarified that granting a copy of the personal data to the data subject may be achieved, not necessarily by exporting a copy of the personal data to the data subject, but also by way of directing the data subject to access a system where her/his personal data stored/processed are accessible/available.</p> <p>Recital 63 provides that <i>“where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data”</i>.</p>
2.	2.3.3. Time reference point of the assessment Para. 37, p.17	<p>The EDPB states that the controllers are not required to provide personal data, which they processed in the past but which they no longer have at their disposal, since they may have deleted them in accordance with their retention policy.</p> <p>It should be clarified, however, whether, in the absence of the personal data, the controller is still under the obligation, upon request, to provide the data subject, if available, with the information contained in article 15(1) of the GDPR in relation to personal data that were processed in the past, prior to their deletion.</p>

		<p>This is consistent with the third component of the right of access, namely ‘‘information on the processing and on data subject rights’’ (para.20, p. 12 of the draft guidelines). It also reflects the judgment of the CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. MEE. Rijkeboer’’ which held that the right must of necessity relate to the past.</p>
3.	<p>2.3.3. Time reference point of the assessment</p> <p>Para.38, p.17</p>	<p>The EDPB requires from the controller to implement the necessary measures to facilitate the exercise of the right of access and to deal with such requests as soon as possible and before the data will have to be deleted. In the case of shorter retention periods than the legal timeframe for responding, the EDPB requires from the controller to adapt the timing to answer the request 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.</p> <p>This, however, has the effect of reducing the legal time frame which is provided to the controller to respond to data subject requests. The GDPR even provides for the extension of the time frame for up to two months, where necessary, in order to allow the controller to handle the request.</p> <p>Requiring the controller to inform the data subjects on actions taken on the requests, prior to the lapse of the legal time frame, would deprive the controller from the legal right (corresponding to the relevant obligation) granted to the controller by the GDPR, i.e., to inform the data subjects about the actions taken on the requests at any time within the legal time frame. Further, it may pressurise the controller to squeeze the assessment of the request within a very tight deadline, leading to an erroneous assessment.</p> <p>Where the request is for the provision of the personal data themselves and at the time of the request, the personal data is available, instead of requiring from the controller to provide a copy of the personal data within the retention period, if this is shorter from the legal time frame, it would be reasonable to advise the controller to prolong the retention period to match the legal time framework, in order to be able to both assess the request and, if the assessment is positive, provide the personal data to the data subject within the legal time frame.</p>

		Where the request is not for accessing the personal data themselves, but for providing the information listed in art. 15(1) and (2) of the GDPR, it may be clarified in the guidelines that the personal data may be deleted at the lapse of the retention period prior to the lapse of the legal time frame for responding to the request, as long as the information requested are collected to be provided to the data subject during the legal time frame.
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. GENERAL CONSIDERATIONS REGARDING THE ASSESSMENT OF ACCESS REQUESTS

4.	<p>3.1.2. Form of the Request</p> <p>Paras. 55 and 56, p.27</p>	<p>The EDPB considers, in para.55, that where the data subject request is addressed to a member of the staff who deals with the data subject's affairs on a daily basis (single contact of a customer, such as e.g., personal account manager), 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.</p> <p>The example provided underneath, in para. 56, describes a situation where the controller provides both on its website and in the privacy notice, two email addresses, i.e., the general email address of the controller and the email address of the controller's data protection contact point, pointing out to the latter email address as the data protection contact point for submitting any inquiries or requests. In that case, the EDPB asserts, the Controller should make all reasonable efforts to respond to requests sent to the general email, so that they can be redirected to the data protection contact point and answered within the GDPR time limits.</p> <p>Understandably, the inclusion of the general email address in the privacy notice may create the expectation, even remote, that a request sent to that email address will be dealt with.</p> <p>Controllers should thus be encouraged by EDPB to include, in their privacy notice, only contact points which are trained and mandated to handle data subject requests, and, if any other contact points are included/mentioned in the privacy notice, these contact points should be trained to recognise the</p>
----	-----------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>requests and direct them promptly and efficiently to the appropriate contact point for handling.</p> <p>Contrary to the example in para. 56, sending a data subject request to an email address of a member of the controller's staff, who is not dealing with data protection issues, should not reasonably create equivalent expectations to the data subjects that their data subject request will be handled by that member, regardless of the recipient's exact duties and the proximity of her/his relationship with the data subject.</p> <p>If the EDPB considers that expectations for a response may exceptionally exist even if the request is not sent to the dedicated and indicated communicated channel and that such request may still trigger the legal time frame, it is recommended that it elaborates further on the situations where such expectations may arise. The mere reference to an example of an "employee who deals with the data subject's affairs daily (single contact of a customer, such as e.g., personal account manager)" may be inadequate. Dealing with the data subject's affairs may encompass a broad range of duties and activities, which may not reasonably involve the creation of expectations on the data subjects that their access request will be dealt with by the recipient, on behalf of the controller, or the controller itself.</p>
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5. HOW CAN A CONTROLLER PROVIDE ACCESS?

5.	<p>5.2.3 Providing access in a "concise, transparent, intelligible and easily accessible form using clear and plain language"</p> <p>Para. 139, p. 43</p>	<p>Where the information is not by itself intelligible and it needs to be made understandable to the data subject, it may be clarified, that this may justify the extension of the one-month time frame, as it adds on the complexity of the data subject request.</p>
----	-----------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


6. LIMITS & RESTRICTION OF THE RIGHT OF ACCESS

6.	<p>6.2. Article 15(4) GDPR para. 166, pp. 48-49</p>	<p>A clarification that the inseparability of the personal data of the data subject/requester from the personal data of other data subjects may be a reason for refusing access to the requester, would be useful.</p> <p>For example, where a data subject's personal data are processed for AI training sets and, as a result, they are</p>
----	---------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>combined with the personal data of other data subjects, this generates inseparable data, consisting of data belonging to multiple data subjects.</p> <p>In such cases, the controller may correspond to the request for access to personal data by providing to the data subject a copy of the personal data that were provided prior to them being combined with the personal data of other individuals.</p> <p>Additionally, where the algorithmic model no longer contains personal data, linking any possible combinations of possible input values (predictors) to a corresponding likelihood of default (target), but group data, concerning the set of multiple individuals sharing similar characteristics, it may be clarified that the data subject-request has no right to access this non-personal data.</p>
7.	<p>6.3 Article 12(5) GDPR</p> <p>6.3.1. What does manifestly unfounded mean?</p> <p>paras. 175-178, p.53</p>	<p>The EDPB stresses the very limited scope of relying on the ‘manifestly unfounded’ ground for either charging a reasonable fee or refusing to act on the request and describes situations where controllers should not rely on that ground, i.e.:</p> <ul style="list-style-type: none"> • Where the requests are related to the processing of personal data not subject to the GDPR, • Where the requests relate to information on processing activities that are clearly and obviously not subject to the processing activities of the controller. <p>We contend that a ‘manifestly unfounded’ request is one that has, undoubtedly, no legal or pragmatic basis.</p> <p>This necessarily includes the case where the controller can assert with certainty, and demonstrate as such, that the requests are related to the processing of personal data not subject to the GDPR. The non-applicability of the GDPR renders the request manifestly unfounded, with no legal basis.</p> <p>Additionally, requests related to information on processing activities that are clearly and obviously not subject to the processing activities of the controller are, similarly, manifestly unfounded, where the controller can demonstrate that the requester cannot reasonably expect, under the circumstances, that the controller processes personal data outside of the context of the processing activities of the controller.</p>

		<p>It is notable that the EDPB, whereas it excludes the applicability of the ‘manifestly unfounded’ ground on specific cases, it does not provide a single example where the ‘manifestly unfounded’ ground can be successfully raised. This further challenges the appropriateness of the decision to exclude the two situations mentioned above in bullet points, which the EDPB is invited to revisit.</p> <p>Lastly, the EDPB is invited to provide guidance as to the situations that may trigger the ‘manifestly unfounded’ ground.</p>
8.	<p>6.3 Article 12(5) GDPR</p> <p>6.3.2. What does excessive mean?</p> <p>Para. 180-185</p> <p>Para. 186</p>	<p>An additional factor that may render a request excessive is the data subject’s option to access, at all times, to a secure system which provides her/him with direct access to his or her personal data (Recital 63 of the GDPR).</p> <p>Whereas, understandably, the vast amount of time and effort needed to provide the information or the copy of the personal data to the data subject cannot on its own render a request excessive, we believe that the EDPB has given little weight to how this factor can contribute to rendering access requests excessive.</p> <p>The EDPB has linked this factor to excessiveness in cases where data subjects abusively rely on art. 15 of the GDPR, i.e., where the data subject makes an excessive use of the right of access with the only intent of causing damage or harm to the controller.</p> <p>We contend that the EDPB is conservative in attributing excessiveness only where the vast amount of time and effort needed is accompanied with malice intention by the data subject, a state of mind which may not be easily and clearly recognisable.</p> <p>For example, the amount of time and effort needed to act on the request may render a request excessive where it is a repetitive request within unreasonably intervals. Hence, for deciding whether a reasonable interval has elapsed for an additional request, the amount of time and effort needed to act on the request, should be one of the factors indicated in para. 183 of the guidelines.</p>

Yours Sincerely,

A handwritten signature in blue ink, appearing to be 'Maria Raphael', written in a cursive style.

Maria Raphael

Managing Partner at RF Privacy Minders Ltd

Partner at I. Frangos & Associates LLC

Committee member of the European Technical Committee CEN/CLC/JTC13

"Cybersecurity and Data Protection"