Data Marketing Association Finland opinion on European Data Protection Board Guidelines 01/2022 on data subject rights – Right of access Version 1.0 Adopted on 18 January 2022

Data Marketing Association Finland is giving the following comments on the above mentioned guidelines.

1. General comments on the guidelines

The guidelines are very philosophical. It is hard to identify for what target group it is ultimately intended. Data protection professionals and data protection lawyers know the terms but other readers are more likely to have difficulties in understanding the contents. The guidelines should have a different type of structure. A clear rule should be presented first as a title followed by clear argumentation. Declarations and introductions are not in place in guidelines such as this one. In fact the guidelines should be layered the same way as the EDPB recommends controllers to inform data subjects about the processing of their data. Leading by example is a good principle for the EDPB as well.

It is unfortunate that a 60-page long, even ridiculously detailed, but still very vague guideline subject to interpretation has been drafted to clarify a single right. This creates a situation that is repeated with almost all other EDPB guidelines: they often end up extending rather than restricting the GDPR. The scope for interpretation is maintained and even worsened, with the result that predictability is only reduced. In the light of this, it is hardly surprising that final interpretations in unnecessarily many cases will be given by the European Court of Justice.

The EDPB guidelines at hand contain a number of far-reaching and detailed requirements and interpretations that are not based on the provisions of the GDPR. Data protection authorities should only issue guidance on matters which are based on the provisions of the GDPR and which are indisputably obligations of data controllers. The current text mixes clear obligations of the GDPR with other things that controllers can do if they so wish (so-called general recommendations).

In particular, the guidelines extend the interpretation of Articles 12 and 15 of the GDPR in a way that is not based on the actual text of the GDPR or the recitals. Never before have data protection authorities provided similar broad interpretations - this is a significant finding, as essentially the same regulation on access rights already existed during the Personal Data Directive and the national personal data laws that implemented it. The GDPR has been in place for almost four years now. It is strange that the EDPB provides guidance only after such a long delay and seeks to impose new types of broad obligations on controllers, the legal basis of which is unclear.

Implementing the requirements and recommendations contained in the guidelines would incur significant IT and process development costs for all types of controllers. The costs and impacts would be higher, 1) the wider the content of personal data being processed, 2) the more diverse the uses of the data, and 2) the longer the statutory retention periods.

The guidelines should be examined critically, above all, in so far as they impose obligations on controllers (supplementary information: Articles 12.1 and 15.1 - see, for example, paragraphs 111, 112, 125, etc. in the guidelines). Until now, the main content of access rights has been the provision of concrete personal data content concerning the data subject insofar as the data have been stored in, for example, information systems, applications and manual archives (provided that there is no need to restrict access rights). In addition to this obligation, the guidelines introduce the so-called obligation to provide additional information which is interpreted very widely. This means e.g. the obligation for the controller to explain at the level of each data subject the nature of the processing that has taken place in practice with regard to personal data concerning him or her (see, for example, paragraph 112: *'information on the purposes according to Art. 15(1)(a) needs to be specific as to the precise purposes in the actual case of the requesting data subject")*: from which external sources the data have been obtained, where the data have been disposed of, what data contents have been used for a specific purpose, etc. It is recommended that this obligation be handled where each data subject can view their own data and descriptions as self-service at any time. The statements on this supplementary information issue are for the most part not supported by the articles or recitals of the GDPR. In addition, as the costs of implementing this obligation would be significant, it is necessary to amend the guidelines in this respect and to limit the requirements to those that have an undisputed legal basis.

As well the exact meaning and definition of the term 'categories of personal data' in the context of executing access requests is left unclear. There is no universal definition for this term. What difference does it have compared to the term 'copy of personal data'?

2. Comments on the executive summary

It is positive that the EDPB acknowlegdes that requests by data subjects to controllers should be sent to formal points of contact instead of to random recipients: *"The controller is not obliged to act on requests that are sent to completely random, or apparently incorrect, addresses."* (page 2) However, unlike EDBP DMA Finland strongly suggests that in case the controller has provided data subjects with a specific channel of communication it should be regarded as the primary and sole channel of communication. Such channels are monitored by employees with focus on data protection issues. By contacting the controller via such a channel data subjects will have their requests addressed promptly and with the best professional expertise. Although controllers are obliged to train their staff to process personal data according to the GDPR one cannot expect every single employee to be aware of the details of the process for requests by data subjects.

About the scope of the right of access on page 3 there is a following statement: "*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.*" DMA Finland does not agree with this because the access rights of a data subject that has expressed a request should not override those of other data subjects that are not necessarily even aware of another data subject having access to their personal data. Such is also stated on page 4: *"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).*" There is also a heavy burden of proof laid on the controllers in case they are obliged to edit the data given to the data subject who is exercising their access rights: "*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."

DMA Finland agrees with EDPB that when for instance the data is not sensitive by nature e-mail is an appropriate channel for issuing a copy of it to the data subject: "*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 - -*" (page 3).

However, a suggestion that when large amounts of data are concerned a layered approach in providing the data is not sustainable in our opinion. Page 3: "*Sometimes, when the amount of data is very vast 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 requests it.*" In many industries such an interpretation would result in unreasonable costs in handling occasional data subject requests.

DMA Finland agrees that it is appropriate and reasonable that the controller is entitled to charge a fee on excessive requests. Page 4: "*The more often changes occur in the controller's data base, the more often the data subject maybe permitted to request access without it being excessive. Instead of refusing access, the controller may decide to charge a fee from the data subject*."

3. Detailed comments on the numbered paragraphs of the guidelines

Paragraph 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*." The previous citation does hardly meet with the criteria 'concise, transparent, easy-to-understand and in an accessible format written in clear and simple language'.

Paragraph 18. Delivering the data to the data subject should be an adequate act in executing the access rights. There is no need to specifically confirm that the controller does process his or her personal data.

Paragraph 19. Paragraph 19 takes a very wide interpretation to the extent of data that the data subject should have access to. (See section 4 above in General comments on the guidelines): " - - *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 para. 35). 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.*"

Paragraph 20. The EDPB clearly wants to make the exercising of the access rights very individual, ie the controller should execute all requests "customized" (see paragraph 20 "*Such information could be based on text taken, for example, from the privacy notice of the controller or from the controller's record of processing activities referred to in Article 30 GDPR, but may have to be updated and tailored to the data subject making the request*"). This interpretation adds on the administrative burden on controllers unnecessarily. Such requirements are detrimental to controllers in the financial sector in particular, as they need to be able to process a large number of requests through a standard process.

Paragraph 31. A prior notice to the data subject on the exact costs of executing access rights in case of excessive or ungrounded requests is unreasonable. When the fee is based on the cost (usually the amount of time spent, sometimes even external costs) incurred, the fee cannot be calculated until the request has been completed.

Paragraph 37. "*Controllers are thus not required to provide personal data, which they processed in the past but which they no longer have at their disposal*." Self-evident directives like this should be erased from the guidelines.

Paragraph 40. "*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.*" In this paragraph the authentication of the data subject is not mentioned at all. Does the EDPB consider that collecting the file against signature is adequate?

Paragraph 48. If the data subject has been unclear with her or his request and does not act when the controller specifically asks for clarification it is unreasonable that the controller must in these cases guess what right the data subject wants to exercise and act within the period of time set in the GDPR for executing the requests as well. In these cases there should be right to extend the period.

Paragraphs 54-55. It may be an unreasonable demand to expect that all employees who have a close daily contact with certain clients or other data subjects are always aware of the details of the data subjects access rights process in their organization. In white collar jobs this is often so but in blue collar jobs employees don't even always have access to personal computers and hence they don't have access to internal databanks etc where to look for information about data protection practices in their company.

Paragraph 66. Implementing a two step authentication system is very costly. It also requires that the controller has the phone number or e-mail address of the data subject in its client register or other register. If a controller does not have one for other purposes it is an unreasonable demand only for identifying data subjects in the access rights process.

Paragraph 67. The overall decription of the usecase in paragraph 67 is somewhat obscure. It is stated: "- - *[controller] 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. [Controller] 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." The paragraph does not address situations where the equipment is used by several individuals either in a private environment (such as a home) or a public one (such as a public library). An identifyer is not a sufficient element to link data with a specific individual.

Paragraph 72. It is assumed that controllers already have existing authentication procedures and channels that can be used for the purpose of executing access rights. In reality, for instance a webshop may use warehouses and other subcontractors to whom the data is delivered whose systems do not support a data subject access rights process.

Paragraphs 79-81. Paragraph 79 states that a third party is in principle entitled to make a request on behalf of a person but that in certain situations verification of the right to act on behalf of a person may be required: " - - *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*". However, in Finnish practice, it has been considered that access rights cannot be exercised by a power of attorney (this has been stated, for example, in section 9.2 of the Guidelines on bank secrecy 2021 issued by Finance Finland https://www.finanssiala.fi/julkaisut/pankkisalaisuusohjeet-2021/). Also acting as a legal trustee on behalf of a data subject requires an official document issued by a public authority. A power of attorney is not adequate. Additionally, according to the Finnish patient register legislation parents or other legal guardians have no access rights to the patient data of a child who has reached a certain age.

Paragraphs 87-89. Paragraphs 87-89 imply that it is acceptable to express an access rights request via a third party, a service provider. It is questionable whether this is legitimate taking into consideration ensuring that the data subject must be authenticated in a reliable way. Phising is an increasing risk in processing data in digital form. Allowing the use of service providers in the access rights process may impose a serious risk of an identity theft for data subjects.

Chapter 4.1. In Finland the e-mail correspondence of employees by using their business / organizational e-mail address (form: firstname.surname@organization.fi) is covered by confidentiality of correspondence. Employers do not have access to the e-mails their employees have sent or received without the consent of the employees. The confidentiality may be broken only in situations strictly covered in law. E-mail correspondence should not therefore be subject to access requests by data subjects.

Paragraph 98. " - - *right of access includes both inferred and derived data*." In case the inferred or derived data is not public such as a trade secret this interpretation is questionable.

Paragraph 99. The demand of a company to provide a data subject ”*individual IT incident reports*” is hardly executable.

Paragraph 108. "*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.*" DMA Finland finds the scope of the interpretation to provide the data subject also with back-up data too wide, expensive and unrealistic to execute.

Paragraphs 111-112. What is the purpose of providing the data subject with the categories of personal data when she or he is provided with the personal data? Most people are not even aware of what categories of their data are being processed. Besides it is possible to categorise data in several ways. These categories are not necessarily generic.

Paragraph 115. "*The controller should therefore generally name the actual recipients unless it would only be possible to indicate the category of recipients*." This interpretation is very demanding and may be diffcult or even impossible to execute.

Paragraph 116. Giving the exact expiry date of all data as a standard element in executing access requests is an unnecessary and costly step. Instead it should be delivered only if the data subject specifically asks for it.

Paragraph 133."*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*." It is surprising how superficially information safety issues are approached in example 2. For example the exact sums in question are financial information. Therefore, the identity of the data subject should be authenticated in a reliable way when delivering such data by e-mail. It is also questionable if such information should be delivered by e-mail at all.

Paragraph 140. The national legislation about official languages used in each EU country should be taken into account in this paragraph. In case the controller has the right to choose in which of the official languages it operates there should not be an obligation to translate the data into other languages even if the data subject speaks another language that is also spoken in the country in question.

Paragraph 143. DMA Finland expresses its strong opininon that all segment data is not public data but may be internal data that reveal economical interests and hence the access rights of data subjects do not apply to it.

Paragraph 158. There is binding legislation in Finland about calculating time periods. The demand to apply Regulation 1182/71 in calculating the period of time during which the data subject's access rights must be executed does not take into account national legislation.