FEDMA
Federation of European Data and Marketing

March 2022

FEDMA response to the EDPB consultation on Guidelines 01/2022 on data subject rights - Right of access

FEDMA had previously highlighted to the EDPB that these guidelines would be an opportunity to clarify the Data Subject Rights, especially about finding the right balance. We had shared situations where a balanced approach between the interests of the controller and the rights of the data subject (DS) needed to be found.

Overall, FEDMA takes note of clarifications and thanks the EDPB for this renewed opportunity to contribute to the guidelines. However, FEDMA considers that these guidelines did not fully seize the opportunity to reach a balanced approach. **We call for more examples or clarifications based on the risk-based approach. A balanced and risk-based approach will enable organizations, especially SMEs, to better answer DS requests.** We refer to the details below.

1. Aim of the right of access

Due to publicity around the DSAR, data subjects may use the DSAR when they could rely on their other rights, namely 1) right to be informed 2) right to request rectification 3) Right to erasure and 4) right to object to processing of their personal information. **Controllers should be able to remind DS of these other rights as this enables organisations to deal faster and more effectively with access requests** (see further our comments on the scope of personal data).

Furthermore, the Guidelines (paragraph 5 and 10) repeatedly mention that the objective of the right to access is to enable individuals to "have control" over their personal data. **We caution against using the term "control"** that may be understood to mean that individuals have absolute rights over their data. **We would suggest that the Guidelines are more nuanced and clarify that the right of access is primarily intended to verify the lawfulness of processing** (see Recital 63 of the GDPR). This clarification would avoid misleading individuals as to the extent of their rights in different data processing scenarios.

Finally, the Guidelines (Paragraph 13 of the Guidelines): provide that the **right of access applies in cases where the controller is aware that the right is exercised with a view to use the data in court against the controller**. We believe that this statement should be nuanced to avoid that access requests be weaponised individually or used for nefarious purposes (such as for instance as a phishing exercise, or to seek a balanced resolution in the context of a dispute, or be used as a tactic in the context of negotiations preceding termination of employment). In these cases, **the controller should be entitled to refer the individual to self-serving tools made available to download his/her personal data**. This would also avoid monopolising company resources to respond to requests made for nefarious purposes when these resources would be better allocated in responding to other legitimate access requests.

2. Scope of personal data

FEDMA had called for a balanced approach precisely to answer better the needs of DS. **We would like to insist on some clarifications, which are more balanced in our view, regarding some situations** (paragraph 96).

Personal data is not necessarily connected to the customer file, for example the technical data of the delivery of a product; to know if it went through a check point. This technical data is

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

linked to the postal address, but it's not linked in general to the customer file. It is not relevant to the individual unless they are following up because there is an issue with the delivery. It should therefore not in principle be included in the right of access. An organization should be able, through its internal policies, to determine when this data should be shared with the DS.

Asking the data subject (or the intermediary) for more information or referring to the scope assessment of personal data determined by the controller e.g. in its privacy statement is particularly recommended in the following situations:

- **blanket request on template form/request or automatically generated** (which could be simply to update some data)
- **blanket requests from third party services**. FEDMA is pleased the EDPB confirmed that controller needs to check validity of mandate. We also support the absence of obligation on controllers to upload the data under article 15 directly to the portal of the third party. Large scale data portability requests exercised by a business should not be used for the purpose to monetize individual's personal data and build up a competitive dataset with monopolistic dimensions.
- **data which reveals trade secrets**.
- **pseudonymous data**: we call on the EDPB to consider identification of individuals in relation to Article 11(2) and provide a balanced approach that does not discourage implementation of privacy preserving techniques. This should be the case for archived data.
- **data highly time consuming if not needed for the DS purpose or requested by the DS:**
  - **unstructured data:** references in internal chats/emails. Mention in meeting minutes, Mention on internal newsletter (Ms. Xyz (ex-employee) has ran a marathon for a charity), Appearance of the person in old outlook calendars of her colleagues, Pictures from company events and parties, sales call log ("today I (Ms. Xyz) visited prospect X. Prospect X runs an annual campaign for their summer collection in May. Contact him again in February to follow up"). An address book in a client's account sl (data has to be removed).
  - **telemarketing calls** where some voices or parts have to be erased.
- **back up data**: FEDMA Is pleased that the EDPB considers that back up data should only be included if there is a decrease in data in the live system. Nevertheless, we suggest taking better into account what the DS wants, needs or requests.

Definition of personal data in the context of a job interview (Paragraph 95 of the Guidelines): The Guidelines consider that a controller is under the obligation to provide a job applicant with the subjective comments made by the HR officer during a job interview. We believe that this example should be reviewed to better balance the right of access of the job applicant to his/her personal data and the right of the HR officer to the protection of his/her personal data as the subjective comments made by the HR officer are themselves an assessment or opinion of the HR manager. The personal data of the HR manager cannot be subject to a lesser standard of protection than the personal data of the job applicant. We therefore recommend the EDPB reviews this example in line with Article 15(4) of the GDPR which provides that the right to obtain a copy of personal data shall not adversely affect the rights and freedoms of others (see also the example in Paragraph 96 of the Guidelines). In order to avoid affecting the rights of the HR manager while mitigating the risks for the job applicant, the Guidelines could provide that while the job applicant cannot access this data, such data must be deleted promptly by the controller after the end of the interview process.

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

3. Further procedural improvements

Time reference point of the assessment (Paragraph 38 of the Guidelines): We believe the Guidelines go beyond the requirement of the GDPR by requesting that the controller "shall deal with such requests as soon as possible and before the data is deleted" and that "the timing to answer the request should be adapted to the appropriate retention period in order to facilitate the exercise of the right of access". This overlooks the fact that the controller may sometimes receive a huge amount of access requests simultaneously and will work primarily towards complying with Article 12(3) of the GDPR. We would therefore request that the EDPB adapt the Guidelines accordingly.

Handling large number of requests in specific circumstances (Paragraph 162 of the Guidelines): We welcome the acknowledgement by the EDPB that extraordinary events could be regarded as a legitimate reason for prolonging the time of the response. We suggest the Guidelines also specifically refer to situations such as cyber-attacks, security incidents and data breaches as examples justifying more flexibility in addressing access requests. In these specific cases, controllers may be facing large amounts of requests, especially if they are under the obligation to notify potentially impacted individuals. Controllers may be investigating the causes and impact of the breach while receiving access requests. In this specific case, controllers may also want to require temporary enhanced identification measures to mitigate possible adverse effects of the breach and prevent fraudsters from taking advantage of the situation.

Excessive request (Paragraphs 187 and 188 of the Guidelines) : The Guidelines recognise that a request should not be regarded as excessive on the ground that improper or impolite language is used by the data subject. We believe however that the EDPB should go further in specifically condemning the use of improper or impolite language in communicating with the data controller and remind that some of these behaviours can be criminally sanctioned under national laws. Employees of the data controller are the recipients of such messages and should be free from insults and harassments while performing their daily employee obligations.

Self service tool (paragraph 54 of the Guidelines): When a **self-service tool** is made available by the controller and the DS chooses not to use it, the EDPB should provide that the controller can request more time to answer the request.

Use of ID cards to identify the requesting person (Paragraphs 73 to 78 of the Guidelines): While we agree that requesting a copy of an ID card as part of the authentication process may create a risk for the security of personal data, we believe that this risk should be better balanced with the risk for the controller to provide access to data to another person than the data subject to whom the personal data relates. This is the case in particular when the controller only processes pseudonymised data and needs to receive the cookie ID from the data subject before it can retrieve any information. In order to protect individuals against fraud and identity theft, the controller must ensure that the information it receives is indeed that of the individual and not that of a third party. Otherwise, there is a risk that an individual could access the browsing history of someone else through a simple access to someone's terminal allowing to obtain the cookie identifier. To avoid this, the controller asks for a sworn statement that the individual is the owner of the device together with a copy of an ID card in support of the sworn statement. Such documents are kept for the time strictly necessary to ensure that the individual is the

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

person to whom the personal data relates and will thereafter be immediately deleted from the controller's systems. This is in line with Recital 64 of the RGPD which provides that : "The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers". Merely requesting the cookie identifier as additional information does not seem to be a sufficient reasonable measure to verify the identity of a data subject to address the risk of fraud and identity theft. We would welcome specific reference to Recital 64 of the GDPR in the Guidelines as well as confirmation that requesting a sworn statement and a copy of an ID card together with a cookie identifier is proportionate to address the risk of fraud and identity theft when personal data is pseudonymised . Such clarification from the EDPB would be very useful for the industry as well as for individuals exercising their rights.

4. **Layered approach**

While we are pleased to see the guidelines enable a layered approach (paragraph 142-143), we consider that information on the segments, in which a customer has been put into by a controller, should not necessarily have to go in the first layer. The example provided should better reflect the case-by-case approach of controllers. Indeed, although relevant, segmentation does not have any legal consequences or similar effects (article 22 GDPR) nor is the segmentation automatically linked to sensitive data (article 9 GDPR). There may be more important information to be put in the first layer. Eg mortgages, loans, insurances. Bold classifications for information linked to the processing of data would not work as it might end up overwhelming the data subject. For example, a data subject might write to a company to ask for his/her personal data. The DS wants to make sure the company has the correct postal address. The DS receives all personal data in a layering which does not reflect his/her needs or intentions.

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org