11 March 2022

FEEDBACK ON EDPB'S GUIDELINES 01/2022 ON DATA SUBJECT RIGHTS - RIGHT OF ACCESS

COMMENTS

ACCIS is the voice of organisations responsibly managing data to assess the financial credibility of consumers and businesses. Established as an association in 1990, ACCIS brings together more than 40 members from countries all over Europe as well as associates and affiliates across the globe. ACCIS members include credit reference agencies, credit registers, business information providers and alternative credit reporting services providers.

ACCIS welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft guidelines 01/2022 on data subject rights - Right of access.

In our view, the draft guidelines include several positive elements, such as:

a) **In relation to the form of the request.** The EDPB confirms that a controller is not obliged to act on requests sent to "*a random or incorrect email (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests concerning data subject's right, if the controller has provided an appropriate communication channel, that can be used by the data subject*" (para 54).

b) **In relation to provision of a copy.** The EDPB confirms the position, as set out in CJEU case law, that data subjects have a right to access their personal data and not necessarily to the documents in which that personal data is contained. It is important that controllers can extract personal data from original documents and put them into a new document that is then furnished to the data subject.

c) **In relation to limits to respond to Data Subject Access Request (DSAR).** The EDPB confirms that limits in how organisations respond to DSARs can apply where the rights and freedoms of others are triggered. In this context, the EDPB says the controller's rights to protect trade secrets or intellectual property and in particular their copyright protecting software are factors that can be weighed, as is the right to confidentiality of correspondence, for example private emails in the employment context. However, these positive statements are very general. A high degree of legal uncertainty for data controllers remains. Further examples would be needed to provide more legal certainty.

We would also like to highlight areas where we believe the draft guidelines could be improved:

d) **In relation to excessive obligations on data controllers**. The draft guidelines provide that a DSAR shall be understood to encompass "*all personal data concerning the data subject*" (para 25) unless explicitly limited by the requesting data subject. The draft guidelines also direct controllers "*to give the broadest effect to the right of access*" (para 35) and to give "*complete access to the requested information* (para 128)." These phrases provide an unhelpful, expansive interpretation of the right of access that imposes significant obligations on controllers in responding to DSARs.

e) **In relation to excessive burdens imposed on data controllers.** We would like to draw you attention to four examples:

- The draft guidelines note that, in response to a DSAR that requests information about the processing of data, such as the purpose of processing, it may be insufficient for controllers to simply refer to the relevant information framed in general terms in their privacy policies. Instead, in order to comply with Art. 15(1)(a)-(h) GDPR, in certain circumstances, controllers may need to specifically tailor the requested information to each requesting data subject, "*unless the tailored information is the same as the general information*" in the privacy policies.

- The draft guidelines require that the requested information be disclosed to data subjects in a "*concise, transparent, intelligible and easily accessible form using clear and plain language*" (Section 5.2.3). Accordingly, if the personal data provided is complex and difficult to understand (such as raw data or machine-readable code), controllers may need to provide additional information. This obligation is a material extension of Article 15 GDPR (which contains no explicit obligation to "explain" personal data).

- The draft guidelines require the controller "*where technically feasible [to] provide access as requested by the data subject, including to personal data stored in the back-up*" (para 108). This

means that the deadline of four weeks can hardly be met. This is far too burdensome for companies. Since the data is not actively used for exchange in the information procedure and the data subjects are not associated with any externally effective legal consequences, the economic interests of the data controller should outweigh the need to surrender archived data.

- The draft guidelines also require that the controller generally names "*the actual recipients [to whom the personal data have been or will be disclosed], unless it would only be possible to indicate the category of recipients"* (para 115). If indeed the information was granted in such a detail, the data subject would be overloaded with data that are not meaningful to him/ her.

f) **In relation to unrealistic expectations on data controllers.** We would like to draw you attention to two examples:

- The EDPB has confirmed that organisations can ask individuals to clarify the scope of their DSAR. This is positive. However, it is unrealistic to expect that, in such cases, the controller should at that time give "*meaningful information*" about its processing operations to assist the requestor to find the information they are looking for, such as information about its different branches of activities or different databases.

- In addition, when an organisation discovers when responding to a DSAR that it has unlawfully processed data or holds inaccurate data, the EDPB expects the controller to inform the requestor of that in its response. The example it used is where a controller realises it has not adhered to its own retention procedures. In that scenario, the controller should provide the data in its response and thereafter delete the information.

g) **In relation to the principle of proportionality.** The draft guidelines note that, besides the limits explicitly provided in the GDPR, *"the right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subjects request under Art. 15 GDPR"* (para 164). The draft guidelines indicate that controllers cannot limit their searches on the basis of proportionality in light of the burden on controllers to provide requested information. This expansive interpretation of the right of access means that controllers cannot rely upon a principle of proportionality, thus undermining the balancing test that should be undertaken to assess the rights of the controller against the requestor. DSARs can be an extremely burdensome, time-consuming, and costly task. Controllers' search duties are not to make every possible effort to find someone or something when searching for relevant data. The EDPB should therefore recognise that organisations are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information.

We would also like to highlight areas where we believe the draft guidelines need a clarification:

h) **In relation to the identification of the applicant**. The draft guidelines assume that the controller must provide information to a victim of identity fraud without addressing the issue of the unambiguous identification of the applicant. This is particularly problematic for the person responsible if the data set of the injured party's data contains only a few correct data. This aspect should be clarified.

i) **In relation to right to obtain a copy**. The EDPB says that "*Art. 15(4) GDPR is not applicable to the additional information on the processing as stated in Article 15(1) lit. a.-h. GDPR*". This sentence is unclear. Article 15(4) GDPR states that the right to receive a copy must not adversely affect the rights and freedoms of others. This also refers to rights such as trade secrets of the controller, as the EDPB emphasizes in para. 169 of the draft guidelines.

Finally, we would also like to highlight areas where we believe the draft guidelines are materially incorrect or flawed:

j) **In relation to disclosure of incorrect data**. The EDPB says that "*the information included in the copy of the personal data given to the data subject (…) includes the obligation to give information about data that are inaccurate or about data processing which is not or no longer lawful*" (para 36). Incorrect data must always be deleted, so that a right to information should generally amount to nothing. In addition, the transmission of incorrect data (e.g., in the case of incorrect assignment to another person concerned) to the person concerned may represent a reportable data breach, since there would a disclosure of someone else's data to an unauthorized third party.

k) **In relation to the identity of the data subject**. The EDPB says that "*information on the ID that is not necessary for confirming the identity of the data subject, such as the access and serial-number, nationality, size, eye colour, photo and machine-readable zone, may be blackened or hidden by the data subject before submitting it to the controller*" (para 75). In case of doubt, it is necessary to verify the authenticity of an ID copy and any interference with a scan prevents such verification. Furthermore, the EDPB recommends, as good practice, after checking the ID card, that "*the controller makes a note e.g., " ID card was checked " to avoid unnecessary copying or storage of copies of ID cards"*. This seems fundamentally flawed and should be removed altogether. The ID copy is extremely relevant for investigation should the controller suspect later on (perhaps due to identifying another attempt) that the identity of the data subject has been stolen or faked.

We thank you for your attention and are available to discuss about the issues raised in this document.

Contact: Enrique Velázquez
Director General, ACCIS
e.velazquez@accis.eu

ACCIS

ACCIS is the voice of companies responsibly managing data to assess the financial credibility of consumers and businesses. Established as an association in 1990, ACCIS brings together more than 40 members from countries all over Europe as well as associates and affiliates across the globe.

Contact

ACCIS Secretariat
Rue du Luxembourg 22-24
1000 Brussels
Belgium
Tel: +32 2 761 66 93
secretariat@accis.eu

Follow us !

Twitter
Linkedin
Youtube