AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

Public Consultation on the new Guidelines on data subject rights – Right of Access

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totaled more than €3 trillion in 2020, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium **T** +32 2 513 68 92
info@amchameu.eu amchameu.eu European Transparency Register: 5265780509-97

Introduction

Data controllers have invested extensively in procedures and processes that allow them to operationalise the handling of data subject access requests. Organisations levelled up those processes ahead of the entry into force of the General Data Protection Regulation (GDPR). To that end, the Draft Guidelines 01/2022 on data subject rights (the Guidelines) adopted on January 18, 2022 by the European Data Protection Board (EDPB) - although not binding - provide helpful directions that data controllers may take into account when defining the procedures and processes that apply to their business models while ensuring compliance with the GDPR. Therefore, the American Chamber of Commerce to the EU (AmCham EU) thanks the EDPB for their adoption and welcomes the opportunity to contribute to the important work of the EDPB in this regard.

While acknowledging the fundamental nature of the right for a data subject to exercise its right of access, it is necessary to strike a balance between the exercise of such right and the efforts deployed by data controllers, the challenges raised by the very broad nature of the right, as well as the way it is exercised in practice. In that regard, the Guidelines are an important point of reference that data controllers will consider when dealing with the various components of the right of access, ie: (i) confirmation as to whether or not the controller is processing personal data of the requesting person, (ii) access to the personal data of the requestor and (iii) provision of information on the processing activities. The Guidelines also provide an indication as to how supervisory authorities would be enforcing the exercise of this right. Those aspects, among many others, are what make the Guidelines particularly useful to data controllers.

The following document outlines AmCham EU's comments on the Guidelines. These are divided into two categories: (1) elements that are considered relevant to the Guidelines as a whole and that impact the extent to which the Guidelines are achieving their goals (ie, to assist organisations with interpretative guidance on the implementation of the right to access in different situations) and (2) specific comments on the current text of the Guidelines.

The comments are not meant to be exhaustive and are not presented in any hierarchical order; they attempt to follow the structure of the Guidelines.

1. Transversal comments on the Guidelines

Towards a more balanced approach

The Guidelines greatly emphasise and develop on the scope and breadth of the exercise of the right of access. In doing so, they focus on the fundamental nature of the right of data subjects. The Guidelines do not give sufficient consideration to the practicalities or the consequences of operationalising the views they expressed. They could sometimes even be considered as conflicting/contradictory among themselves or with the GDPR.[1] This situation poses concerns for organisations that wish to consider the Guidelines in their processes and procedures.

For example, the Guidelines affirm that it is not up to data controllers to assess 'why' the data subject is requesting access (para. 13). Nonetheless, the exercise of the right of access should always be understood in connection with data privacy and data protection. The Guidelines seem to accept that this is the case (see, for example, para. 188), but it would be beneficial to have this principle stated more affirmatively at the beginning of the Guidelines. Further, the statement in para. 13 of the Guidelines should also be rectified to avoid any confusion. Indeed, the need to provide data subjects with clear and intelligible explanations on the actual processing entrenches the exercise of the right of access in the context of data protection (to the exclusion of any other contexts). Taking a different position puts data controllers in very difficult situations; absent of a context of the request, it is almost impossible for them to meet their requirements on the various components of the right of access.

In addition, the Guidelines further state that data controllers should not deny access on the ground or suspicion that the requested data could be used by the data subject to defend itself in court in the event of a dismissal or a commercial dispute with the data controller (para. 13). In doing so, the Guidelines create a precedent. Rather than facilitating the effective enforcement of the right of access by the data subject, such a novel precedent would give data subjects access to actions that their domestic systems did not contemplate or authorise. The Charter of Fundamental Rights of the EU did not introduce a general e-discovery right within the EU; the GDPR should not be used for the same. Doing things differently would introduce an EU level procedural law through the GDPR, something that the GDPR does not contemplate and that goes well beyond the mandate of the EDPB.

Further, the legal concept of 'abuse of right/law' is broadly recognised and should also apply in the context of data protection. As a result, while the data controllers are not entitled to formally enquire the purpose of a request, it would nevertheless seem justified in certain circumstances to look into the possibility for the request to constitute an 'abuse of right/law'. It would be helpful to clarify, through a case study or otherwise, what other evidence of a request being excessive can be considered too and, if so, which ones (eg, can the circumstances in which a request of access is filed be considered in certain cases?).

The Guidelines state that the request does not need to be in any particular form and can be sent via any communication channel normally used by the data controller. At the same time, they do note that the controller 'is not obliged to act on a request sent to a random or incorrect e-mail (or postal) address, not directly provided

[1] This is particularly so in relation to how the Guidelines approach the principle of proportionality. Indeed, it is difficult to reconcile the Guidelines' reliance on proportionality (for example, at paragraphs 64, 69 and 171) with the executive summary that states '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'.

by the controller, or to a communication channel that is clearly not intended to receive requests regarding data subject rights' (see para. 52-57). AmCham EU would welcome further examples of channels to submit access requests that are considered appropriate (or not) for the purpose of avoiding unreasonable expectations from the data subjects and providing some comfort to data controllers.

Finally, and even if the Guidelines remind data controllers of the risks that improperly dealing with a request of access may lead to a personal data breach (eg, when the personal data are provided to someone who is not the relevant data subject), little consideration is given to how data controllers could seek to mitigate such risk. This is an element where the Guidelines could elaborate and go further. Further, in some instances, the Guidelines, if followed, would present a risk of a personal data breach. One illustration can be found in the solution presented at the end of the example in para. 67; indeed, by stating that the cookie identifier will be the additional information used to identify the advertising profile of the requestor, the Guidelines suggest that a cookie identifier or other information alone would be appropriate for the purpose of verifying the identity of the data subject. This is not the case and further raises unacceptable security risks if exclusively relied upon.

Limited justification means less transferable guidance

The Guidelines provide interesting case studies and examples (including variations within those examples). Examples are, by their very nature, always very fact-specific and the situations data controllers are confronted to are often more complex than what the Guidelines suggest. It would be beneficial for data controllers if the Guidelines provided more background or reasoning on why the EDPB is arriving to certain conclusions in particular contexts. The Guidelines should also acknowledge that the cases described are intended to illustrate in a simplified form the often-complex situations that data controllers and individuals may face. This would allow the reasoning to be more easily transferable to other cases. For example, when discussing what would amount to a 'reasonable interval' (in the context of assessing whether a request may be considered excessive or not), the examples (see para. 183) quote 'two months, three months and one year'. Absent of granular details on each of those timeframes and why they would (or not) be acceptable, it is difficult for data controllers to set what may be considered a proper benchmark in their context.

Additional guidelines

The Guidelines cover a wide range of topics in the overall context of the exercise of the right of access. They often focus on elements that are relevant or important to data subjects.

The Guidelines would benefit from a more developed section 3.4.2. (Exercising the right of access through portals/channels provided by third-party). In this sense, the Guidelines primarily: (i) recognise that aggregators exist, (ii) stress that data controllers need to make sure that personal data is not disclosed to unauthorised parties and (iii) emphasise that data controllers still need to handle those requests within the timeframe ascribed by the GDPR.

The massive and random exercise of the right of access by portals or platforms are a reality. It is very difficult for data controllers to determine whether or not those requests are genuine and fulfil the legal requirements for the exercise of the right of access in those circumstances.

The EDPB should come up with more actionable guidance on what elements data controllers may consider when confronted with such requests. In particular, the Guidelines should focus on how to verify that the data subject requesting personal data from a third part service is in fact the individual to whom the personal data relates, in compliance with the GDPR. AmCham EU members are ready to share with the EDPB practical examples of requests they received from such aggregators and discuss the difficulties raised by those requests in practice.

2. Specific points of attention

Assessing proportionality when responding to access requests

The Guidelines fail to properly take into account the principle of proportionality in responding to access requests. In some situations, responding to requests might entail an excessive burden for the data controller. The Guidelines current position, where 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 subject´s request', seems to contradict Recital 4 and article 62 GDPR, as well as the general EU principle of proportionality. It is clear from both the language of the GDPR and the case law of the Court of Justice of the European Union (see C-70/10 Scarlet Extended v. SABAM [2011] ECR I-11959) that the right of access is not an absolute right and it should be applied in a proportionate manner.

It follows then that a reasonable and proportionate approach should be adopted, at all stages of the process, including with respect to assessing the personal data that is produced in response to the exercise of the right of access by a data subject. The current language of the Guidelines translates into a significant burden on many data controllers in practice of all sizes and in all industries, without any appreciable benefit for data subjects. A more balanced approach should be considered such that 'reasonable efforts' should be made to retrieve information, but which would exclude personal data that has been deleted, as part of the data controller's general records management.

The situations outlined below are purely illustrative examples where responding to the exercise of the right of access by a data subject would be very onerous and technically difficult, if not impossible, to comply with. If the scope of the searches cannot be appropriately limited on the basis of proportionality, it is likely to result in excessive burden for data controllers, something the GDPR itself does not require or that has not been developed by case law of the Court of Justice of the European Union.

Here are two examples:

- Emails and other 'free' formats: organisations of most sizes are likely to have millions, if not billions, of emails and other electronic documents. Emails often consist of a mixture of different types of information that may (intendedly or unintendedly) relate to various individuals. For example, emails might contain information on a number of different topics or about a number of different individuals. Hence, data controllers are often unable to accurately identify information about a particular individual without processing more personal data to this effect. Further, an expansive interpretation of what would be necessary leads to extended accesses to content of inboxes. While an individual's name may be redacted, various other parties would need to review correspondence to determine what should or should not be disclosed, leading to a material loss of privacy.
- Databases/data warehouses: most organisations are likely maintaining databases/data warehouses to store the data generated by their services 'offline'. Such databases/data warehouses may (or may not) contain personal data that may (or may not) be potentially relevant to a specific exercise of the right of request. Searching across various information sources, in particular when they are not structured, would be disproportionate, costly and technically challenging. Moreover, if such search is ultimately conducted, the personal data extracted is: (a) likely to be 'raw data' that should not have to be provided in response to a data subject access request; and (b) unlikely to provide the data subject with information required to understand and verify the lawfulness of the processing of their personal data.

Scope of the right to access

The Guidelines may lead to consider that 'data in a raw format' (which may not be 'directly meaningful' to the data subject) is covered by the right of access and that, when providing data in a raw format, it is important for the data controller to: 'take the necessary measures to ensure that the data subject understands the data, for example by providing an explanatory document that translates the raw format into a user friendly form'. In stating so, the Guidelines are going beyond the text of the GDPR. Further, the Guidelines seem internally conflicting where they state that 'It should be stressed that the information provided to the data subject always

must be in a human readable format'. Indeed, 'data in a raw format' is (more often than not) not in a human readable format.

According to various GDPR provisions (see Recital 63 and article 12[1]) and findings of the Court of Justice of the European Union (see joint cases C-141/12 and C-372/12 YS and al). The GDPR requires data controllers to provide users with 'intelligible access', in order to allow them to understand and verify the lawfulness of the processing only. If personal data is processed in an unintelligible format, it is the data controller's obligation to determine how they can provide people with information that 'enables them to become aware of this information processed lawfully. The Guidelines should be amended to take this element into account.

Modalities and methods of response to a subject access request

The Guidelines suggest (see para. 108) that access should be provided to data in a back-up system where data in a front-end system has already been erased. Unless limited to cases where the data controller is specifically aware that personal data responsive to a subject access request has been deleted, this provision seems to disregard the concept of a reasonable search for personal data by the data controller. Where personal data only resides on a backup system, data controllers will often be unable to access a requestor's data without restoring an entire back-up system, which could contain the information of many data subjects. Restoring such back-ups could then conflicts with other GDPR provisions, such as those on data minimisation or storage limitation. It can also result in the restoration of data which other individuals have actively deleted, amended or objected to. Paragraph 108 of the Guidelines should be revised with this in mind.

The Guidelines recommend offering answers in the language that is understood by the data subjects in a specific country (see para. 140). AmCham EU' understanding of that paragraph is that this paragraph does not intend to request the data controller to translate the personal data in relation to the data subject, and thus, should be clarified. Further, there is a benefit for the Guidelines to promote the use of dedicated communication channels, when these are provided to the data subject by a data controller. Such use might, for example, ease the tracking of requests by data controllers to ensure that those are responded to in accordance with the requirement set for the under article 12 (3) of the GDPR.

Finally, the Guidelines appear to advance new and restrictive interpretations that are not based on the text of the GDPR by stating that response times should be revised to facilitate the exercise of an access request in case of shorter retention periods. This interpretation would create an undue burden on data controllers who take additional steps to ensure and promote data minimisation. Such language should be reviewed so that this recommendation is considered on a case-by-case basis, according to the accountability principle and in view of the technical feasibility of doing so.

What is meant by a 'copy of the personal data'?

The Guidelines contain a number of apparent contradictions around the breadth of the right to obtain a copy of the personal data.

The Guidelines (see para. 150) seek to give information and guidance on what is meant for data controllers to meet the requirement to provide data subjects with a copy of the personal data undergoing processing. They indicate that a summary is not sufficient, while at the same time they mention that the right to a copy does not necessarily require a reproduction of the original documents.

Irrespective of the length of paragraph 150 and the fact that this paragraph also includes an example, at this stage, we believe that the actual threshold that the EDPB proposes data controllers should meet when they decide that they will not provide a copy of the documents containing the personal data, is still unclear. That part of the Guideline needs to be reworked. Indeed, the Guidelines do quote a distant (non-GDPR) Court of Justice of the European Union' case (C-141/12 and C-372/12) stating that it is sufficient for the applicant to be provided with a 'full summary of those data in an intelligible form'. The Guidelines then include a reference to 'a compilation containing all personal data covered by the right of access', as an alternative. What those are and what they should look like is not further described, and the attempt to reconcile the two elements is confusing. The case study (see pages 46 and 47) does not help to gain a better understanding of what is a basic feature of the right of access.

It would be particularly helpful to better understand the distinction made in the Guidelines in the above paragraph, through further examples of the type of information that could potentially be left out when providing a copy of personal data in reply to a subject access request (eg, when a request for access relates to years of email correspondence or employment records related to an individual), the purpose being to allow flexibility as the circumstances where request of access can be exercised are highly diverse.

Balancing the rights of two equally protected data subjects

The Guidelines seek to deal with a key difficulty when providing copies in the context of a request of access, namely identify where the line should be drawn between the rights of two equally protected data subjects when a single piece of information relates to both of them (see, para. 95 and 103). Echoing the example in the Guidelines, while it is clear that subjective comments about a candidate employee constitute personal data about the candidate, they are just as much personal data about the recruiter, whose personal data should also be protected. The same is true in case of whistleblowing (regulated by EU Directive 2019/1937).

The Guidelines seem to refer to a balancing exercise based on how the exercise of the right of access would affect the rights and freedoms of the individual who did not file the request and whose personal data would be disclosed (see example 1, para. 171). Such reference is, however, not detailed in any way elsewhere. Further guidance on when a balancing exercise should be conducted (and how) is fundamental to help data controllers consider where to draw the line and to appropriately protect the rights and interests of all affected parties in accordance with article 15 (4) of the GDPR. Further examples would also be welcome to help understanding the situation and allow the necessary flexibility required by the variety of scenarios of the exercise of the right of access.

Similarly, the Guidelines suggest (see para. 105) that 'in case of identity theft, a person fraudulently acts in the name of another person'. In this context, it is important to recall that the victim should be provided with information on all personal data the controller stored in connection with their identity, including those that have been collected on the basis of the fraudster's actions'. This seems to disregard that personal data collected on the basis of the fraudster's actions could be information that directly or indirectly relates to the fraudster and thus constitute their personal data, which is equally protected under the GDPR. Disclosures of personal data of a third party under the argument that it constitutes a response to the exercise of a right of access could result in an unlawful processing of personal data relating to another individual, in violation of the GDPR. The Guidelines should be revised in this respect.

Given that this aspect determines the extent of redaction' exercises required, in particular when access is requested to thousands of emails of a professional nature, this question is crucial to allow data controllers to fully consider their obligations and account for their actions in this respect. Similarly, the Guidelines should also clarify when full (unredacted) disclosure of personal data, including personal data related to third parties, is acceptable.

Balancing the right of access with the right not to self-incriminate

There is an inherent tension between the obligation to provide a copy in response to a request of access and another fundamental right, namely the prohibition against self-incrimination. This is even more so as the Guidelines provide for the obligation to point out errors in the data provided to the data subject (see para. 39). The interpretation of the right of access in the above section seems to disregard the right not to self-incriminate entirely. It would be useful to understand how, in the EDPB's view, the prohibition on self-incrimination can be reconciled with the right of access, knowing that both are fundamental rights.

Layered/tailored approach advocated in the Guidelines

The Guidelines re-use the concept of a layered approach (see para. 141 et seq.) that is often discussed in the context of compliance with the transparency principle, ie, primarily in relation to privacy notices.

AmCham EU is not completely positive as to whether the introduction of the concept is meaningful or will actually prove to be helpful when dealing with the exercise of the right of access. The use of a layered approach, especially when all personal data should be provided to a data subject anyway, adds an element of complexity

to data controllers and a layer of potential dispute in the handling of the request. Echoing earlier comments, a layered approach would need to consider the rationale behind the request being made and the volume of personal data processed by the data controller which is responsive to the request, in order to make sense.

The Guidelines emphasise (see para. 111 to 118) that information provided to data subjects under article 15 should be tailored to the specific circumstances of the processing of that data subject's data. AmCham EU welcomes an approach that allows data subjects to understand the personal data being processed about them. This approach is in line with best practices adopted by organisations in their global privacy compliance programs. However, the conclusion of the case study in paragraph 118 is concerning. The last paragraph of the case study suggests that, in the context of responding to a request for access to personal data, data controllers have to provide information on the third parties, such as service providers, that they actually disclose personal data to (rather than keeping the approach accepted in privacy notices where the recipients can be grouped by categories, in certain circumstances). In some instances, those service providers can change on a very regular basis. Introducing this high and burdensome requirement on data controllers increases the risk that incorrect information will be provided to the data subject. Further, the Guidelines should also acknowledge that there are circumstances where personal data are processed in a standard and predictable way such that: (i) a link to a website privacy notice should be able to satisfy the requirements of article 15 (provided that notice contains all necessary information); and (ii) a privacy notice provided at the time when personal data were first collected can continue to be an up-to-date and accurate representation of the information necessary under article.

What is meant by 'large scale'?

In two distinct instances, the Guidelines refer to the concept of 'large scale'. They do so, first, when discussing the appropriate measures that a data controller should take to investigate the request of the right of access exercised by a data subject (para. 127). Second, it is used in one of the examples discussing what an 'excessive' request might mean (see example 2, para. 183).

The GDPR refers to the concept of 'large scale' in multiple instances (such as in article. 27, article. 35 and article. 37). The EDPB has already commented on the conditions to be fulfilled to meet the definition of 'large scale' in previous guidelines. There is a benefit in the EDPB clarifying what it meant by the concept of 'large scale' in the two instances where it refers to the concept of large scale in the context of these Guidelines, and to ensure this is aligned and not in conflict with or in addition to the concept of 'large scale' as already established by the EU legislator.

Limits and restrictions of the right of access

The Guidelines state that 'in principle any right or freedom based on Union or Member State law may be considered to invoke the limitation of Art. 15(4) GDPR'. This is a correct interpretation of article 15(4). However, the Guidelines then contradict this statement stating that not every interest should be taken into account when assessing article 15(4): 'For example, economic interests of a company not to disclose personal data are not to be taken into account'. This does not seem a correct interpretation of article 15(4) GDPR and it would directly contradict article 12(5) GDPR.

This broad exclusion of economic interests from the balancing assessment should be amended in the Guidelines. Article 15(4) GDPR (read in conjunction with Recital 63) anticipates taking all rights and freedoms of others, including economic interests, into account. For example, data controller's trade secrets, IP and the ability of providers of online services to offer safe and secure service should be taken into account. Further, Recital 4 of the GDPR explicitly acknowledges that the right to data protection must be balanced against other fundamental rights, which rights include the freedom to conduct a business. Limiting 'rights and freedoms' to 'protected rights' would only create confusion around what constitutes such a 'protected right' and would result into too narrow an interpretation of article 15(4) GDPR.

The Guidelines should also properly acknowledge that in certain circumstances data controllers cannot provide specific information to data subjects about the reasons why data has not been disclosed in response to an access request. This is particularly relevant where disclosure of such information would reveal the operation of tools and procedures used to detect bad actors or breaches of terms and policies. Requiring that data controllers

disclose this information undermines the security of online services and prejudices the rights and freedoms of the users of online services, who have a right to be protected from bad actors.