11 March 2022

# EuroCommerce comments on the EDPB 01/2022 Guidelines on Data Subject Rights– Rights of Access

## About EuroCommerce

EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 28 countries and 5 million companies. Retail and wholesale is the link between producers and consumers and generates 1 in 7 jobs, offering a varied career to 26 million Europeans, many of them young people. EuroCommerce is the recognised European social partner for the retail and wholesale sector.

## Introduction

We welcome the EDPB Guidelines and the effort to provide clear criteria to assess whether and how data subjects are provided with access to personal data. Legal certainty on how to interpret and implement the complex GDPR is essential for companies, big and small. In this context clarity is also needed regarding the interplay between new European digital proposals such as the Data Act, the AI Act and the existing GDPR. Concrete guidance and examples that would not create additional administrative burden but would promote legal certainty will strengthen the protection of personal data and empower growth in the EU market. Nevertheless, we would like to point out some areas where further clarification is needed to give companies more assurance how to interpret the obligations to provide access to data subjects. Please find below our specific comments on the guidelines for your consideration.

*Paragraph 13/36: (un)Lawfulness of processing*

We read in paragraph 13 that *the controller should not assess "why" the data subject is requesting access, but only "what" the data subject is requesting*. In certain cases, using the right to access can constitute an abuse of rights, as access does not fulfill the purpose of guaranteeing privacy but obtaining proof for court proceedings. In addition, in paragraph 36 it is stated that data should not be corrected before handing it in, so the data subject has the possibility to know about unlawful processing. We believe that this might go against the controller's obligation to keep data up to date and correct.

As an evidence, in accordance with case law from the Netherlands[1], respectively the District Court of Rotterdam dated 21 January 2020, the Supreme Court dated 16 March 2018 and the Council of State dated 6 November 2019 have stipulated that Article 15 gives the right to access to data subjects to verify whether his/her personal data are correct and have been lawfully processed, which may lead

[1] District Court of Rotterdam 21 January 2020, ECLI:NL: RBROT:2020:515, nr. 4.8.; Supreme Court 16 March 2018, ECLI:NL:HR:2018:365, nr. 3.3.3; Council of State 6 November 2019, ECLI:NL: RVS:2019:3754, nr. 8.

to rectification, erasure or blocking of the data. But it does not give the right to – solely – obtain proof for court proceedings. Therefore, the "why" can most certainly be relevant for the controller.

- Could the EDPB elaborate on this by also taking the rights of the data controller into account?

### *Paragraph 35: Specification of Access Rights*

If we understand the wording in paragraph 35 correctly, it leads to the conclusion that no matter how broad and unspecific the request for access, the controller has the obligation to comply with such request. Such an interpretation of Article 15 does not seem proportionate. The interpretation given by the EDPB to Article 15 does not take the day-to-day practice into account nor the reasonableness of what would be required of businesses, big and small.

### *Paragraph 40/72: Compliance with data security requirements*

We believe that in cases of non-electronic transmission of the data additional and friendly measures should be put in place in order to avoid risks of exposing data to the wrong person and ensuring the security of the transmission without the establishment of a formal channel of transmission.

### *Paragraph 69-78: Identity verification data subject*

In paragraph 73 is stated that using a copy of an ID for verification of the identity of the data subject should be considered inappropriate as this *may* lead to unauthorized or unlawful processing. However, we are of the opinion that the identity of the data subject can be reliably verified - in line with the principles of the GDPR - by requesting – via a protected route – a copy of the ID of the party requesting access to personal data (without the photo and BSN being visible) to verify with a high degree of certainty that such person is indeed the data subject it states to be. Taking into consideration that the copy of the ID is deleted once the identity has been duly verified. Such a verification process can be necessary to prevent data from being shared with unauthorized third parties (such as ex-partners). In our opinion, this verification method guarantees proper identification without prejudice to the right of data subjects to contact an organization freely and without excessive processing taking place in view of the mitigating measures mentioned. We request the EDPB to take this into consideration and rewrite paragraph 73 to reflect that requesting a copy of an ID may be a reasonable verification method, in situations where the requesting party has not yet been authenticated as the data subject.

### *Paragraphs 79-81: Requests made via third parties / proxies*

According to para. 79 of the Draft Guideline, it is stipulated that "(i)n 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 (see section 3.3 above)" (emphasis added). It is unclear if this sentence should be read to imply that there might be cases when identity of the third party and authorization itself may *not* require verification. It is suggested to clarify that, in light of the risk of the data breach when providing access to data subject's person's to a third party, verification of authorization and the third party itself should always be required, while the means of verification can be subject to the data controller's discretion, based on the proportionality assessment as described in section 3.3 of the Draft Guideline. In our opinion as the danger of a data breach is really high in this case additional measures should be proposed.

- With respect to the personal data collected during the process of verification of the third party and the data subject's authorization provided to the third party, what would be the advised approach for determining a retention period to this category of data and documentation?

### *Paragraph 96/139: Copy of Personal Data/ Raw Data (Article 15(3)) - Understanding on "activity logs"*

In order to comply with an access request where this kind of data must be provided and to better understand what could be or has to be done to provide such data, it would be useful to provide examples with to guarantee this data subject's right.

In addition regarding raw data, the EDPB states that the data subject has a right to access the raw data it provided. Could the EDPB elaborate how this relates to the decision of the European Court of Justice (YS)[2].

### *Paragraph 14: Duty to inform data subject becoming controller*

In paragraph 104 it is mentioned "*the controller should inform the data subject about the fact that they may become controller in such case*".

- Could the EDPB elaborate where such an obligation is based upon?

### *Paragraph 20/116*

Individual calculations and tailored approaches should be avoided as they risk to pose additional administrative burden to the companies. We call the EDPB to consider this issue.

### *Paragraph 108: Technically feasible access to back-up data*

In paragraph 108 there is an obligation to provide access to back-up data "where technically feasible". Are we right to assume, taking into consideration our remark about proportionality (point 1), that what is technically feasible is dependent on the "reasonable factually practical possibility" and not on the "theoretically conceivable disproportionate possibility"? It is worth noting that to regain access to data in (binary/raw) back-ups in many cases an entire backup will have to be restored which results in excessive processing of personal data and could adversely affect the rights of others and add to the overall administrative burden of the controller.

### *Layered approach for the recipients (Article 15(1)(C))*

On paragraph 115 the EDPB seems to prioritize the indications of the concrete recipients (as the example states in the guidelines). In order to make the exercise of this right less complex, we understand that a layered approach on the disclosure of the recipients should be applied. Unless the Data Subject firsts asks on concrete information about the recipients, the Controller should only be required to disclose the categories of recipients.

[2] ECLI:EU:C: 2014:2081, Joint decisions C-141/12 and C-372/12 YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S, Judgment of 17 July 2014, paragraphs 58 and 59, 17 July 2014. Recital 58: "Therefore, in so far as the objective pursued by that right of access may be fully satisfied by another form of communication, the data subject cannot derive from either Article 12(a) of Directive 95/46 or Article 8(2) of the Charter the right to obtain a copy of the document or the original file in which those data appear.

### *Paragraph 119: Omission of reference to article 22*

In paragraph 119 it seems that the EDPB has omitted that article 15(1)(h) requirements relate to art 22 paragraphs 1 (and 4), which refer to *solely* automated decision making *with legal or similarly significant effect*. From the perspective of legal certainty, it is important to include the reference to article 22 in paragraph 119.

### *Paragraph 147: Commonly used electronic form*

In paragraph 147 it is stated that the data controller should be "based upon the reasonable expectations of the data subjects and not upon what format the controller uses in its daily operations." "Commonly used electronic formats" (Article 15.3 GDPR) does not necessarily mean the same as "the reasonable expectations of the data subjects". The EDPB has the task to issue guidelines, recommendations, and best practices in order to encourage consistent application of the GDPR.[3] The EDPB has no legislative powers and should refrain from interpretations which are reserved for the legislator and the competent court. The same is to be said of the last sentence of paragraph 147. Nowadays, the Word-format as well as the PDF-format are in our opinion commonly used electronic formats. If the data subject, however, does not have these programs on its electronic device, he/she might have to buy such software to be able to read the document. We request the EDPB to delete the wording of 147 which entails an interpretation which goes beyond what is stipulated by the legislator.

### *Point 5 of EDPB's Guideline: How can a controller provide access?*

Please find below some specific questions regarding point 5 ("how can a controller provide access" – page 39 ff.), focusing on the typical systems / standard systems which shall be scanned against a personal identifier (e.g. employee number, name, customer number).

- To what extent should the company identify personal data?
- Is it sufficient for the company to search / scan on the basis of a personal identifier all systems falling under the category of the data subject (standard systems)?
- Whether and to what extent is the company obligated to search for personal data even in further systems?
- Are there criteria against which the required efforts can be measured?

### *Copy of Personal Data (Article 15(3)) – Profiles*

In some cases, businesses might create profiles for its clients which are only internal references and we understand not relevant to share within a Data subject access request. Is there an obligation to share with the data subject the name of its profile since this is in conflict to the trade secret rights of the Controller?

### *Format of the Copy of Personal Data (Article 15(3)) – Audio recordings*

Paragraph 153 states that a transcription of the conversation of an audio recording instead of the audio recording itself could be shared with the Data Subject if this is agreed between the data subject and the controller). We would advocate to follow the decision of the Finish Data Protection Authority

[3] Article 70 paragraph 1 sub e GDPR

on this matter (case number 3592/152/2019), in accordance to which, the Data Controller wouldn't need an agreement with the Data Subject in order to give him the transcription of an audio recording instead of the audio recording itself. In many cases the transcript of an audio recording is often the most appropriate format to provide the requested data, especially given that in many scenarios audio recordings involve personal data of other data subjects (e.g., call center employees). As such, a transcript allows the data controller to effectively balance the requirement of data minimization (Article 5(1)(c)) and protection of the rights and interests of the third parties (Article 15(4)) and therefore should be recognized as a default format for audio recordings requests.

### *Format of the Copy of Personal Data (Article 15(3)) – annex with examples of the format of copies*

It would be helpful to have an annex to the Guidelines giving concrete examples of cases where the Controller should give access to the original documents. The case-by-case basis analysis would be much easier if we had broader examples in place.

### *Chapter 6 of EDPB's Guideline: Limits and restrictions of the right of access*

1. Chapter 6 of the Guidelines ("limits and restrictions of the right of access, page 49 ff.) focuses on certain limits and restrictions of the right of access. Regarding documented testimonies or employee statements, for example within the scope of internal investigations or clarification of compliance cases, there are some open questions:

- Is it necessary to provide access to their (e.g. witnesses) names?
    - What is more important: to protect the witness or to give the accused the possibility to take action against defamation etc.?
- What criteria should the company use to weigh both interests?
- Does the company have a primary responsibility to protect third party data in case of doubt?

2. In the scope of chapter 6, confidential evaluation requests can be made on the system among colleagues (e.g. on topics like cooperation, professional teamwork) whereby the requesting person sends an evaluation request to several people. The feedback shall remain "anonymous", meaning: The requesting person does not know who wrote the respective feedback.

- In this case is it necessary to provide access to their names?
- Does "confidentiality" or the assurance that something remains anonymous per se excludes the right of access?

### *Proportionality (paragraph 164 Guidelines – recital 13 GDPR)*

Could the EDPB elaborate on its remark in paragraph 164 that "*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 article 15 GDPR"*, in relation to the general principle included in recital 4 of the GDPR that "*The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*." As well as in relation to recital 13 of the GDPR that "*Union institutions and bodies, Member States and their supervisory authorities are encouraged to*

*take into account the specific needs of micro, small and medium-sized enterprises in the application of the Regulation*." It seems that proportionality should be relevant for all obligations under the GDPR. There is no discernible reason why the right to access is without a general reservation to the principle of proportionality, certainly not regarding SME-controllers. We request the EDPB to take the principle of proportionality into account regarding the implementation of Article 15.

### *Paragraph 168: Article 15(4)*

Could the EDPB elaborate on its wording in the last sentence of paragraph 168 where it states "It is important to note that not every interest amounts to "rights and freedoms" pursuant to Art. 15(4) GDPR. For example, *economical interests of a company not to disclose personal data are not to be taken into account when applying Art. 15(4) as long as they are no trade secrets, intellectual property or other protected rights*"? In recital 63 GDPR it is not narrowed down to *fundamental* rights and freedoms. If such an extra requirement would, however, be included in the guidelines, this would mean that the scope of paragraph 4 of Article 15 is narrowed down by the EDPB. The EDPB has the task to issue guidelines, recommendations, and best practices in order to encourage consistent application of the GDPR.[4] The EDPB has no legislative powers and should refrain from interpretations which are reserved for the legislator and the competent court. Maintaining the fundament of the trias politica is of utmost importance.

### *Paragraph 175: Practical examples of a 'manifestly unfounded' request*

In paragraph 175 of the Draft Guideline, the EDPB emphasized that " there is only very limited scope for relying on the « manifestly unfounded » alternative of Art. 12(5) in terms of requests for the right of access". A number of examples where a request is not considered to be manifestly unfounded are included in the Draft Guideline, however, it is unclear in what cases the 'manifestly unfounded' test stipulated in the GDPR would actually be satisfied. The EDPB is invited to consider cases where access requests are submitted by the third party DSR-as-a-service intermediaries – such requests are often not only repetitive, but also directed at the wrong data controllers (i.e., the requests directed at controller A are submitted to controller B), drafted in intentionally ambiguous and unclear language and do not include evidence of authorization provided by the data subject. It could be considered that such requests constitute an example of 'manifestly unfounded' access requests and can be refused by the data controllers.

### *Clarification of terms and role of DPO*

- In paragraphs 35b, 64, 127, 134, 138, 141-145, 150, 161, 162, 186 and in the executive summary the terms *very vast amounts/vast amounts/large quantity/large amounts of data* are used to justify asking a data subject to specify their access request on the one hand and an obligation to provide supplementary information in layers on the other:

  a) are these words used interchangeably throughout the text of the draft guidelines?
  b) do they mean the same as "large scale" data processing as defined in the "Guidelines on Data Protection Impact Assessment (DPIA)"? It seems that there is a difference since the draft guidelines also consider at least the structure of controller

[4] Article 70 paragraph 1 sub e GDPR

and modalities of data processing.
c) an additional example or further explanation of the meaning of “very vast amounts” / “vast amounts” / “large quantity” / “large amounts” of data would be helpful.”

- Could EDPB please elaborate on the tasks of the DPO in the context of the right to access; Can the DPO also be tasked with honoring the right of access; Does the DPO have a task to monitor how the right of access is executed; If a DPO honors the right of access and monitors execution, what bearing does that have on potential conflicts of interest?

Contact:
Savvina Papadaki - +32 456 35 6163 -papadaki@eurocommerce.eu Transparency Register ID: 84973761187-60