

11/03/2022 Position Paper

## **EFAMRO and ESOMAR Consultation Response**

### **A Response to the draft EDPB Guidelines on data subject rights – Right of access**

This paper is submitted on behalf of:

**EFAMRO** the European Federation of Associations of Market Research Organisations. Founded in 1992, EFAMRO represents the interests of market, opinion and social research in Europe. Its members are national trade associations for research businesses.<sup>1</sup>

**ESOMAR** the global voice of the data, research and insights community since 1947, it promotes the value of market, opinion and social research and data analytics.<sup>2</sup>

#### **1. About Market, Opinion and Social Research**

- 1.1. EFAMRO and ESOMAR represent the data, research and insights sector, accounting for in Europe a reported annual turnover of €20.87 billion.<sup>3</sup>
- 1.2. Market, opinion and social research is the systematic gathering and interpretation of information about individuals or organisations using the statistical and analytical methods and techniques of the applied social sciences to gain insight or support decision making. It involves systematic study of different spheres of society, politics, and the economy. Research, insight and analytics stand at the heart of all well-informed commercial, social and political decisions. Insight into what makes a product, business initiative or government policy work is often the hidden – yet defining – factor between success and failure. It is our sector that provides the deeper intelligence needed for our world today.
- 1.3. Many research and analytics providers subscribe to established self-regulation schemes that enable research respondents and participants to enforce their rights. These are built on established international standards set forth by the ICC/ESOMAR International Code and national codes across many EU countries<sup>4</sup>.

#### **2. Purpose of our Response**

- 2.1. Our associations are responding to the European Data Protection Board's (EDPB's) proposed *Guidelines -1/2022 on data subject rights – Right of access*, which sets out the arrangements for meeting the right of access to personal data as one of the data subject rights provided for in Chapter III of GDPR among other rights.

---

<sup>1</sup> For more about EFAMRO see: <https://efamro.eu/>

<sup>2</sup> For more about ESOMAR see: <https://esomar.org>

<sup>3</sup> ESOMAR Global Market Research Report, which includes contributions from national associations including EFAMRO members: <https://esomar.org/global-market-research-report>

<sup>4</sup> ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics: <https://esomar.org/code-and-guidelines/icc-esomar-code>

- 2.2. Our associations largely support the guidance and welcome the clarity which the guidance brings to some of the key concepts and their application. We do however have some concerns and feedback about how some of the concepts relate specifically to research and insight data.

### 3. Detailed Feedback

#### Use of Language

***[Section 1.3 and footnote 3; Section 2.3.1 clause 35(b); Section 3.1.3 clause 61; Section 3.2 example 66 and 67; Section 3.3 example 76; Section 4.2.1 example 105; Section 5.2.5 clause 150; Section 6.2 clause 171 examples 2 and 3; and Section 6.3.2 clause 183 example 1]***

- 3.1. We recommend that throughout the guidance gender neutral language is adopted to ensure the guidance is inclusive for all data subjects and does not create barriers to representing the diversity of data subjects and their gender identities.
- 3.2. We appreciate that parts of the guidance are direct quotes from the GDPR and therefore cannot be changed but we recommend all other references (as detailed above) are changed e.g., ‘him or her’ to ‘them’.

#### Data Minimisation

***[Section 2.3.3 clause 38; 39]***

- 3.3. We would like to draw the attention to how the current text appear to prioritize the right of access over the principle of data minimisation. As in the example provided under clause 38, data controllers are encouraged to retain personal data beyond necessity only to comply with the timeframe imposed by Art. 12(3) GDPR.
- 3.4. As a consequence, we believe that data controller will be encouraged to create unnecessary data pools rather than investing in data minimization and other privacy enhancing technologies and processes.
- 3.5. We therefore recommend the following amendment to clause 38:

38. At the same time, the controller shall implement the necessary measures to facilitate the exercise of the right of access and to deal with such requests as soon as possible and before the data will have to be deleted. In the case of shorter retention periods than the timeframe to answer imposed by Art. 12(3) GDPR, 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 and to avoid the permanent impossibility of providing access to the data processed at the moment of the request. ~~In this respect, for example, the request for the right of access to personal data collected before entering a building for security purposes must be dealt with promptly before the personal data are erased.~~

## Definition of Personal Data and Scope of Data to be Supplied

### [Section 4.1, 4.2 and 4.3; and Section 2.3.1]

- 3.6. We are concerned by the breadth of the definition of personal data as it concerns any personal data which is being processed without distinction between the purposes (clause 107). Only anonymous data is exempted (clause 99). We believe that purpose and contextual assessment is a necessary consideration when responding to subject access requests for personal data.
- 3.7. In the case of market and social research, a data subject may have taken part in a number of research projects for a research supplier. The personal details of the data subject may still be identifiable depending on whether the research materials have been made anonymous or not (this will often depend on the stage in applying quality processes such as those defined in *ISO 20252: 2019 Market, opinion and social research, including insights and data analytics – Vocabulary and service requirements*)<sup>5</sup>.
- 3.8. Unlike with customer records, market and social research files containing data subjects may only be linked to individual research projects and not to individuals. If a data subject has participated in a range of projects a subject access request could require supplying personal data, including data knowingly and actively provided by the data subject via quantitative and qualitative research techniques (such as questionnaires and participation in groups), across multiple projects and multiple clients. As such controllers may struggle to provide complete information if they are unaware of all the research projects undertaken by a data subject because, in adherence to professional codes of conduct, research organisations apply by default a principle of no-return-path to safeguard the identity of research participants.
- 3.9. We believe that the research scenario specified above is an exceptional situation similar to the public authority example provided in Section 2.3.1 clause 35 b) example 1. The multiple research projects being similar to the multiple departments processing data concerning various contexts and as such Recital 63 GDPR could apply. Whilst research practitioners are unlikely to have large amounts of data on any data subject, it is likely that it will be dispersed across different projects in entirely different contexts. We would welcome the EDPB recognising research as another ‘exceptional’ example within its guidance and including it as another scenario whereby Recital 63 could apply.

## Timing for the Provision of Access

### [Section 5.3 Clause 161]

- 3.10. While the guidance helpfully specifies when extra time can be taken to respond to a request, making it clear that it depends upon the specific circumstances of each case, we would like to receive further guidance concerning the parameters to take into account when assessing what constitutes a complex request. The clause lists a set of factors that could be considered relevant, e.g.:
- the amount of data processed by the controller

---

<sup>5</sup> For more information about ISO 20252: 2019 see: <https://www.iso.org/standard/73671.html>

- how the information is stored, especially when it is difficult to retrieve the information, for example when data are processed by different units of the organisation
- the need to redact information when an exemption applies for example information regarding data subjects, and
- when the information requires further work to be intelligible

For research and insight projects many of the listed factors in clause 161 can apply, particularly to how the information is stored, the need to redact information and the need to undertake further work to make the data intelligible. It is helpful that the guidance emphasises the need to consider the complexity of a request, as in the research scenario it is not the amount of data that can be a challenge rather the complexity of making such data suitable to meet data subject access requests.

3.11. We recommend including an additional bullet point to clause 161 to reflect the necessity of research organizations to safeguard commercial confidentiality when complying with data subjects' access requests, for example when personal information such as data subjects' answers are embedded in concept testing.

3.12. We therefore recommend the following amendment to clause 161:

- the amount of data processed by the controller
- how the information is stored, especially when it is difficult to retrieve the information, for example when data are processed by different units of the organisation
- the need to redact information when an exemption applies for example information regarding data subjects, and
- when the information requires further work to be intelligible
- **when the controller needs to sanitize business sensitive information to comply with its contractual confidentiality duties.**

## Scope of the Right of Access

### *[Section 4.1 Clause 96 example]*

3.13. The example in Clause 96 illustrates a scenario where personal data may not be shared when releasing the personal data could identify another individual (e.g., the identity of another employee testifying about someone's professional performance). Some organisations use third party organisations to undertake performance assessments of staff using techniques derived from research including mystery shopping.

3.14. Mystery shopping is when research practitioners undertake the role of customers/users in order to evaluate business/service performance<sup>6</sup>. Mystery shoppers should have the same level of protection as an employee in the scenario outlined and it would be helpful if the example could be expanded to clarify that suppliers who provide such services, such as mystery shopper's, may be subject to limitations under Art. 15 (4) GDPR in the same way as employee data.

## Format of Access Request Evidence

---

<sup>6</sup> See ISO 20252:2019 for further details about research processes: <https://www.iso.org/standard/73671.html>

**[Section 3.2 Clause 64 example; and Section 5.2.5 clause 148, 150 and 153]**

- 3.15. It would be helpful if the guidance could clarify circumstances where personal data can only be provided in the original format. For example, if a data subject requests access and/or copies of CCTV images or photographs, presumably these must be provided as digital visual files or photographs as no other format can be used which would enable the information to be intelligible and accessible? Unlike for example providing a written transcript of an audio file as an alternative format to a copy of the original audio. Clarity about this is essential particularly when such images may include other data subjects and some form of masking and/or editing may be required to protect other data subjects' rights.

**Establishing the Identity of Data Subjects**

**[Section 3.2. clause 64 example]**

- 3.16. We would welcome further clarity in the guidance about the range of circumstances when refusing a request due to challenges of identification could apply. In Section 3.2, clause 64 the CCTV example states that the controller may refuse to take action as they are not able to identify the data subject due to the volume of data to be accessed. Would this still apply if a data subject provided a photograph of themselves to help a controller identify them in the volume of data? Realistically having a photograph/image of a data subject is no more helpful with a large volume of data. It would however be helpful to have the example expanded to include such a circumstance.

**Technical Specifications and Expectations**

**[Section 3.2 clause 67 example]**

- 3.17. The guidance contains a number of useful examples to illustrate the application of the subject access requirements. One of these, example 67, illustrates a potential behavioural advertising example. Within this example the guidance states:

*"...however, If Mr X tries to exercise his access right by e-mail or by regular mail, then in this context C will have no other choice to ask Mr X to provide "additional information" (Art.12(6)) in order to be able to identify the advertising profile associated with Mr X in this case, the additional information will be the cookie identified in the terminal equipment of Mr X...."*

It would be helpful if the guidance could clarify the EDPB's expectation as to the degree which controllers need to assist data subjects in providing information such as cookie identifiers stored on data subject's equipment. For those data subjects who are not digitally literate asking for such information may cause data subjects' difficulties. Is the expectation that controllers would provide technical assistance to data subjects to provide such information where the data subjects are unable to source it themselves?

**Providing Access**

**[Section 5.2.3 Clause 140; and Section 5.2.4. clause 143 example]**

- 3.18. We welcome the guidance about providing subject access data in a format which is suitable, including accessibility considerations. It would be helpful to understand whether it would be

reasonable for controllers to collect as standard any accessibility requirements upon receipt of subject access requests. We believe this is a sensible way for controllers to be addressing accessibility considerations but in doing so would not want to be perceived as exceeding data minimisation principles (Art.5 (c)). Would asking for any accessibility considerations be deemed relevant and necessary for subject access purposes?

## **Limits and Restrictions of the Right of Access**

***[Section 6.1, Clause 163; Section 6.2 Clause 171 example 3; and Section 6.3.2 Clause 183]***

- 3.19. It would be helpful to explain the application of clause 163 with an example of a research project based on Art.89 (2) and Art.89 (3).
- 3.20. We welcome the addition of example 3 in clause 171. This kind of scenario could apply in a research context where software is used to identify potentially fraudulent professional participants who wish to bias or prejudice research results.

## **4. Implications to the sector**

- 4.1. Overall, we welcome the creation of the Guidance. It will assist research and insight controllers to meet their subject access requests, particularly if the concerns noted above could be addressed in the final version of the Guidance.

## **5. Next Steps**

- 5.1. EFAMRO and ESOMAR welcome the opportunity to assist the EDPB in updating and finalising the Guidance. To contact us for more information:
- Kaleke Kolawole, Head of Policy: [kaleke.kolawole@efamro.eu](mailto:kaleke.kolawole@efamro.eu)
  - Claudio Gennaro, Senior Advocacy Programmes Coordinator: [claudio.gennaro@esomar.org](mailto:claudio.gennaro@esomar.org)