EDPS's informal comments on the draft DPIA submitted by [...] on a database related to [...]
(Case 2021-0116)

Background

The [EUI]

[...].

The legal basis

[...]

There is, therefore, a clear legal basis for the establishment of a [...] database of information from [relevant] authorities relating to [...] by the [EUI].

The request

On 29 January 2021, [...] asked the European Data Protection Supervisor (the 'EDPS') informal advice on a draft Data Protection Impact Assessment (the 'DPIA') it had prepared (the 'Request').

The DPIA relates to the [EUI]'s plans to set up a [...] database concerning [...]. The [EUI] "*welcome*[d] *informal exchanges with the EDPS supervision team*" in this respect.

The approach

The DPIA was primarily assessed against the principles set out in Articles 39 of the Regulation 2018/1725 (the 'EUDPR')[1] and the EDPS's Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation document (the 'Accountability toolkit')[2]. The Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679[3] were also taken into consideration, to the extent applicable by analogy.

The EDPS's previous Opinion on the European Public Prosecutor's Office's prior consultation on the risks identified in the DPIA carried out on its Case Management System (the 'EDPS's Opinion on the EPPO DPIA')[4] has served as a further guidance document during the analysis.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725
[2] https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf
[3] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[4] https://edps.europa.eu/sites/edp/files/publication/20-10-01_prior_consultation_opinion_eppo_dpia_cms_2020-0568_en.pdf

Analysis of the DPIA

At the outset, we welcome that the DPIA follows the Template structure of DPIA report provided for in the Accountability toolkit[5]. We will analyse each of the elements of the DPIA to see whether they provide for information required by the EUDPR as further developed in the Accountability toolkit. Our main recommendations and suggestions for improvement are underlined in the comments below.

1. Project name: The title focuses on what the processing is about. This notwithstanding, it would be more reader-friendly if the [EUI] were to resort to a somewhat more descriptive formulation (for example, "*The establishment of a* [...] *database... on* [...]... *pursuant to....*"). We would also suggest explaining what an acronym stands for before using it throughout the text (for example, [...]).

2. Validation/sign off: The list sets out the approval chain. However, it is not clear who finally signs-off the DPIA. Whilst there is a mention to the step where the "*Delegated controller approves*", the next step seems to be that of the "*Delegated controller reports to ED*", this latter being, presumably, the [EUI]'s Executive Director. The ED's approval, or at least his/her acknowledgement of the DPIA approved by a delegated controller, appears to be missing. In sum, we recommend that the Executive Director's, that is the highest management level's, endorsement of the DPIA be clearly set out in the DPIA itself.

3. Review: The text provides for information on the current status of the DPIA. A DPIA should also include information on the review cycle. According to the Accountability toolkit, the length of the review cycle should be based on the risks posed by the processing operation. By default, the EDPS recommends a review cycle of 2 years, with an extraordinary review in case of significant changes to the processing operations[6]. It is therefore recommended that the [EUI] considers an appropriate review cycle and refers to it in the DPIA.

4. Summary: The [EUI] provides for a good overview of the processing operation and of the main risks and measures to address them, as they currently stand in the DPIA (see Point 9.f of the DPIA). .. Additionally, it is worth of note that [EUI] is considering the need for a joint controllership agreement with [relevant] authorities, in accordance with applicable EDPS guidelines[7]. This is certainly welcomed. It is trusted that, at the relevant time, the [EUI] will set out the relevant obligations and responsibilities in the said agreement to the appropriate detail.

5. Reasons for this DPIA: The [EUI] explains the need for the DPIA on arguments that are in line with Article 39 of the EUDPR and the elements set out in the list of criteria for assessing whether processing operations are likely to result in high risks of the EDPS's Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments document[8].The [EUI] further explicitly refers to the

[5] See Annex 3 of the Accountability toolkit.
[6] See section 3.8 of the Accountability toolkit.
[7] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725:
https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf
[8] See the threshold assessment template of Annex 1 on page 29:
https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf

EDPS Decision of 16 July 2019 on DPIA lists issued under articles 39 (4) and (5) of Regulation (EU) 2018/1725[9]. In sum, as suggested in the template, the [EUI] uses a positive list, which it moreover complements with a brief explanation on the outcomes. This is satisfactory.

6. Main actors involved: The Accountability toolkit suggests that an overview of "*who was involved, when, on which part*" is provided here. The description provided is not incompatible with this suggestion. However, it is, at present, obviously limited due to the fact that the DPIA is still a draft and has not been finalised. In other words, the [EUI] should make sure to complete the relevant information as work progresses.

7. Description of processing[10]: The DPIA follows the template. We would, nevertheless, recommend that the [EUI] include here a more detailed explanation as regards the legal basis, namely by means of describing precisely the scope of the applicable provisions, so as to ensure that the DPIA is a self-standing document, understandable without the need for the reader to resort to other information.

(a) The DPIA provides for a **data flow diagram of the process (flowchart)**, which explains the interaction between the different [relevant] stakeholders with the database;

The DPIA also explains (i) **the sources of the data**. Here, however, it would be helpful to the reader if the [EUI] were to identify clearly (not only using acronyms) who the relevant authorities are and include footnotes quoting the relevant legal provisions that are already mentioned in the text (in particular [...]);

The DPIA further (ii) lists **what data is collected**. Here, we would recommend that a short explanation of some concepts is included, even if only in footnotes [...]

The DPIA further explains (iii) **what is done with the data**, namely its collection, analysis, sharing with [relevant] authorities, and use by the [EUI] for the purpose of [...]. This seems to be satisfactory. However, we recommend that [EUI] further explain which analytic third party tools the [EUI] may use and what are the roles and responsibilities of these third parties in the actual processing.

The DPIA also explains (iv) **where and for how long data is kept**. The retention period proposed is 10 years. The [EUI] explains that it may decide to delete data before that period expires, on a case-by-case basis. It is therefore understood that the standard action that is applied to data retained once that 10-year period expires is that of deletion. It would be nevertheless useful to make this clear in the text of the DPIA. It would also appear appropriate that the [EUI] explains better how the regular

[9] See the positive list of Annex 2 on page 7:
https://edps.europa.eu/sites/edp/files/publication/19-07-16_edps_dpia_list_en.pdf
[10] Article 39(7)(a) EUDPR: "*The assessment shall contain at least... a systematic description of the envisaged processing operations and the purposes of the processing...*"

assessment of the necessity of the data kept in an identifiable form is performed.

Similarly, the [EUI] acknowledges that the standard retention period that is set out in [...] is 5 years, which may nevertheless be added of extra 5 years in some circumstances[...]. In this respect, the [EUI] argues that retention periods vary in the Member States and emphasises that the issue of retention in a similar case has been already addressed by the EDPS in an opinion [...] in a prior check. [...] also the [EUI] is ready to reassess and adapt the retention period if it proves excessive or insufficient. Here, it is therefore worth of recommending to the [EUI], in the same terms as in the EDPS's opinion [...], that when the [EUI] has experienced the first 10 years of practice [...] an evaluation of the necessity of the 10 years period should be conducted. On the basis of such evaluation, the [EUI] should be able to demonstrate whether such longer conservation period is indeed necessary;

Finally, the [EUI] clarifies (v) **where to and on which basis it transfers the data**: the DPIA lists the [relevant] authorities to whom it may transfer data. While this appears to be satisfactory in principle, it could be argued that further detail should be provided, namely the exact references to the protocols and Memoranda of Understanding (the 'MoUs') mentioned, if possible.

(b) Detailed description of the purposes of the processing: The Accountability toolkit suggests that the [EUI] explain the process step-by-step, distinguishing between purposes where necessary. The [EUI] appears to provide information that is likely satisfactory having regard the fact that the project is still in its very early stages.

(c) Description of interactions with other processes: The explanation in this respect appears to be satisfactory. It would, nevertheless, appear useful to clarify how data may be fed in from databases or platforms already controlled by the [EUI]. Firstly, a more comprehensive legal analysis on purpose compatibility should be addressed for reinforcing the accountability principle. Then, a technical and organisational explanation is needed in order to better understand eventual risks at stake.

(d) Description of supporting infrastructure: This has not been defined yet. A precise description of the infrastructure with particular emphasis on data sharing feature will be of outmost importance for evaluating the adherence of legal requirements and any possible risk arising from the application. What is more, a thorough information security risk assessment should be performed in order to demonstrate the appropriateness of technical and organisational measures on security of personal data and IT systems supporting their processing as stated by art. 4(1)(f) and 33 of the EUDPR, and by the Accountability toolkit.

8. Necessity and proportionality[11]: This point is misnumbered: it should be a separate point (8) and not an additional sub-category (e) of the descriptions included in point (7)

[11] Article 39(7)(b) EUDPR: "*The assessment shall contain at least... an assessment of the necessity and proportionality of the processing operations in relation to the purposes*..."

of the draft DPIA. The [EUI] appears to sufficiently explain (a) why the personal data are necessary to fulfil the mandate assigned to it. As regards (b) proportionality, however, that is whether the data necessary are also within the limits of what is proportionate to achieve the tasks, the [EUI] essentially refers to the relevance and the accuracy of the data used and the safeguards in place to ensure that these are processed properly. In accordance with Article 39(6)(b) of the Regulation, the Accountability toolkit requires a comparison between the benefits of the processing against the risks to the fundamental rights posed by the processing. We would recommend that the [EUI] make a clear statement as to why the processing as it is envisaged is proportionate to ensure that the [EUI] fulfils its mandate.

9. Analysis of risks and establishment of controls for identified risks[12]: This point is misnumbered: it should be a separate point (9) and not an additional sub-category (f) of the descriptions included in point (7) of the draft DPIA.

The Accountability toolkit suggests that the focus should be primarily on the risks to the rights and freedoms of data subjects and then on the compliance risks for the institution, and not only in the event of anything going wrong but also in that of all processes working as planned.

The draft DPIA appears to provide exactly for that and the analysis appears to be at a good standpoint, but will require further advances in relations to specific features that still need to be defined. In particular, the design and the effectiveness of controls and mitigations related to risks No. 12 and 13 should be better explained in order to reach the intended residual severity and likelihood.

10. Data subjects' comments (if applicable): Considering the scope of the processing operation that is related to the DPIA it would appear reasonable that no consultation of data subjects is envisaged.

11. DPO Comments: Information possibly to be updated as the work on the DPIA evolves.

Summary of the EDPS's recommendations and suggestions for improvement

Recommendations:

- Explain clearly who signs-off the DPIA;
- Include an appropriate review cycle of the DPIA;
- Describe the applicable legal provisions better, namely by including exact quotes;
- Make sure that the future joint controllership agreements will provide for the information necessary to understand the obligations and responsibilities of the joint controllers;
- Update the information on main actors involved as the project evolves;
- Identify clearly the sources of the data and quotes of relevant legal provisions included;
- Explain the concepts used in the part of what data is collected, such as [...];

[12] Article 39(7)(c) EUDPR: "*The assessment shall contain at least... an assessment of the risks to the rights and freedoms of data subjects...*" and Article 39(7)(d) EUDPR: "*The assessment shall contain at least... the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*"

- Explain what are the third party analytic tools that may be used and clarify what are the roles and responsibilities of the said third parties;
- Explain clearly what happens to data after the retention period expires;
- Explain better how the regular assessment of the necessity of the data kept in an identifiable form is performed;
- whenever possible for the [EUI] to conduct an evaluation of the necessity of the 10-year retention period, be able to demonstrate whether such long conservation period is indeed necessary;
- Include references to exact protocols and Memoranda of Understanding on transfers of data, if possible;
- Clarify how data may be fed in from databases or platforms already controlled by the [EUI];
- Describe the infrastructure with particular emphasis on data sharing feature;
- Refer also to the thorough information security risk assessment performed;
- Dedicate a separate point (8) to necessity and proportionality should be; Include a clear statement as to why the [EUI] considers the data to be proportionate; and
- Dedicate a separate point (9) to Analysis of risks and establishment of controls for identified risks; Explain better the design and the effectiveness of controls and mitigations related to risks No. 12 and 13.

Other suggestions for improvement

- Consider using a more descriptive title and explain what the acronyms mean; and
- Once finalised, consider publishing the DPIA, or at least a summary of it, on the EUI's website.

26 February 2021