EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066)

Introduction

Data Protection Impact Assessments (DPIAs) are one of the new accountability tools in Regulation (EU) 2018/1725[1] (the Regulation). They are amongst the most valuable sources to understand how the data processing landscape on the ground is changing. Following a good year of application of the Regulation, the EDPS decided in February 2020 to launch a survey to find out how the EU institutions, bodies and agencies (EUIs) have implemented this new tool so far and what the lessons learned and best practice recommendations might be.

This exercise will further feed into improving the EDPS guidance on Article 39 of the Regulation published so far[2]. It is exploratory in nature and decidedly not about naming and shaming – this Report only refers to EUIs by name for good practice examples.

By letter of 25 February 2020, DPOs of all EUIs were invited to provide their insights as a DPO as well as their EUI's response to a questionnaire (Annex I) by 8 April 2020. The structure of this Report largely follows the structure of this questionnaire and takes into account the 40 replies received from EUIs[3] by mid May 2020, i.e. despite the COVID-19 crisis. The EDPS is grateful to all stakeholders involved in replying and providing constructive and comprehensive feedback under truly exceptional circumstances.

Generally, the EDPS will carry out such targeted surveys more frequently in the future, as a further development of the biennial 'spring exercises' conducted under the old Regulation (EC) 45/2001. They are an important tool in compliance monitoring in view of the limited ability of the EDPS to check the situation on-the-spot in the immediate aftermath of the COVID-19 crisis.

[1] OJ L 295, 21.11.2018, p. 39–98.

[2] "Accountability on the ground", https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en.

[3] In chronological order of contribution / evaluation: S2R JU, CURIA, EIGE, EESC / CoR, ENISA, SESAR, CleanSky, FSA, EASA, Cepol, FCH 2 JU, ECHA, ECDC, Eurofound, eu-LISA, INEA, EIB, EACEA, Chafea, EASO, Ombudsman, EC, EASME, EP, EMA, Frontex, ERCEA, EMSA, EUIPO, ECB, REA, EIT, Eurojust, EDA, OSHA, Council, CPVO, FRA, EMCDDA, EDPS.

Contents

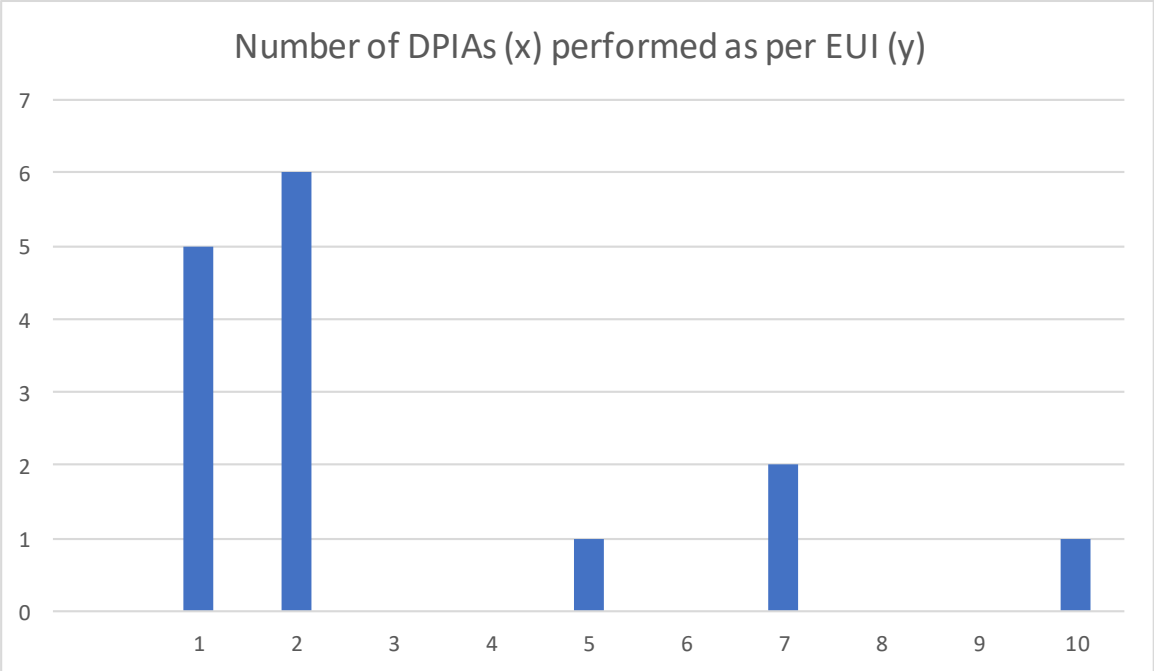
General questions

Number of DPIAs carried out

Whilst the **majority of EUI has so far not finalized a DPIA** in the sense of Article 39 of the Regulation, we have food for thought in the 40 replies received on how different EUI reacted in comparable situations. A number of EUIs noted that their first DPIA was currently still in the making ("several DPIAs currently under consideration", "currently working intensively to finalise the first DPIA since the Regulation became applicable", "work in progress").

Notably a Working Group of EU Agencies on data protection and procurement is looking into conducting DPIAs and six Joint Undertakings have taken preliminary steps for conducting a DPIA and an information security risk assessment of certain IT products and services.

Very few EUIs (only 4 of 39) have finalised more than two DPIAs by now. Interestingly, whilst the EUIs conducting a higher number of DPIAs are comparatively big EUIs, they are not the biggest.



Several EUIs mentioned that they had been conducting DPIAs even before the entry into force of the Regulation in December 2018.

One EUI noted that "All our processing operations that would require a DPIA have been cleared under the provisions of Article 27 of Regulation (EC) 45/2001 and at this point in time, new assessments with regard to those operations are not deemed necessary". According to EDPS guidance[4], processing operations that require a DPIA and that have been prior-checked with a positive result (with a closed follow-up procedure, where applicable) benefit from a grace period of two years, so no DPIA was necessary immediately. However, this grace period is over end 2020.

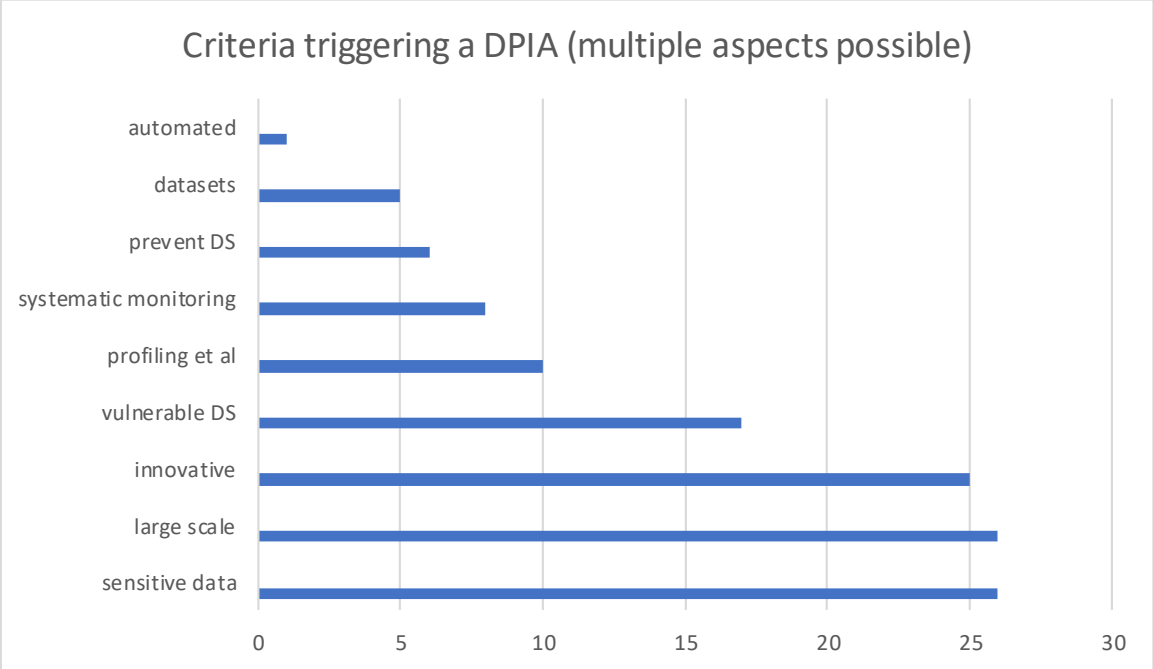
[4] https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf, p.21.

Nature of the processing operations for which DPIAs were conducted

The nature of processing operations for which DPIAs have so far been conducted is very heterogenic, with aspects mentioned more than once ranging from recruitment, CCTV, medical data, team building / training, events and surveys to cloud solutions and other IT issues, including security aspects. Main business areas covered are thus HR- and IT-related, which was an expected result given the varied nature of EUIs' core business. However, some of the more elaborate DPIAs have been conducted on core business activities of EUIs (see below).

Criteria under Article 39 triggering a DPIA

For each DPIA carried out, EUIs were invited to list the (possibly multiple) criteria triggering the need for a DPIA under Article 39 of the Regulation (as further explained in Accountability on the ground, part I, chapter 4.3 and annex 5).



In order of relevance, the most relevant triggering criteria were:

- Sensitive data or data of a highly personal nature = 26 times mentioned as trigger;
- Data processed on a large scale = 26 times;
- Innovative use or applying novel technological or organisational solutions = 25 times.

These criteria were followed in relevance by:

- Data concerning vulnerable data subjects = 17 times (one referring explicitly to an "unbalanced employer / employee relationship");
- Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting = 10 times;
- Systematic monitoring = 8 times;
- Preventing data subjects from exercising a right or using a service or a contract = 6 times;

- Datasets matched or combined = 5 times;
- Automated-decision making with legal or similar significant effect = 1 time (although, allegedly, no real legal or similar significant effect).

Other aspects that have been considered by EUIs when deciding to conduct a DPIA include the following:

- Physical aptitude test: "Type of processing taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons."
- DPIA on code of conduct for high level officials: "Nature of the data subject involved: the publication of such data could have caused a damage to the reputation or image of the official involved".

Insights from the full texts of the latest DPIAs provided

Following the request to provide the full text of the two latest DPIA reports, the EDPS received a total of **17 finalised DPIAs**. A number of EUIs did not provide the full text of DPIAs mentioned in their contribution, as these DPIAs had not been finalized yet (this explains the discrepancy between DPIAs conducted and DPIAs provided in full text).

Given the **very different nature of processing operations underlying these full text DPIAs** and their limited number, it is difficult at this stage to draw meaningful conclusions. However, the following two aspects became apparent:

Length of DPIAs provided

There is a remarkable spread regarding the length of the DPIAs provided, which **ranges from five to 55 pages**. The average DPIA consists of a little over 16 pages. Given the variety of topics and the very different formatting options used (anything from full text to excel tables in fine print), this is presumably a weak indicator. However, given the comprehensive analysis and the weighing of different risks needed to produce a meaningful DPIA, a five page solution would at any rate seem to be less than required.

The notion of "risk"

The wording of Article 39 of the Regulation leaves no room for doubt: the focus is on "a **high risk to the rights and freedoms of natural persons**".

As pointed out in Accountability on the ground, part I, section 3.2, p.7: "This 'risk mindset' is one of the big changes compared to the old rules: always think about how the processing could affect those whose data you process. What does it do to them? How does it affect them? **Both if things go according to plan and when things go wrong**." The angle is the one of the persons concerned by the data processing, not e.g. the reputational or physical damage to your EUI. The EDPS guidance document provides a checklist, which can be a tool for considering all aspects. While not formally speaking part of the record, it shows that you thought about the data protection implications of the processing.

Data security is an integral part of these considerations. As pointed out in Accountability on the ground, part I, section 3, p.22, you must process personal data in a way that ensures 'appropriate security'. What is 'appropriate' depends on the risks of the processing (see also

Article 26 of the Regulation). This includes both technical and organisational measures. In many cases, you will be able to refer to your general information security risk management (ISRM) documentation here. For further guidance, see EDPS guidance on security measures for personal data processing.

However, given that risks "to the rights and freedoms of natural persons" need to be assessed, i.e. from the point of view of those concerned by the data processing, **the examination should not stop there**. Regarding the use of thermal imaging cameras and the auto-track functionality of pan-tilt cameras, the EDPS has previously highlighted that the relevant data protection risks (including IT security ones) should be exhaustively identified and sized.

Actually, all rights and freedoms of these data subjects that are potentially at stake should be listed - and mitigating measures should be based on these considerations.

- ***Example***: One very comprehensive DPIA on the use of health data for communication activities inside a network refers to the "patient's vulnerability regarding the situation due to their rare diseases: potential long-term effects of the processing operation with reputational effect on their professional life".

- ***Example***: One DPIA template / methodology invites the controller to answer the following questions:
  - "Could this operation decrease the likelihood that people exercise their fundamental rights (e.g. freedom of expression, belief…)? E. g. When investigating e-mails, if one checked the content instead of only checking the traffic data, this would decrease the likelihood that people exercise their freedom of expression" and
  - "Could this processing operation lead to discrimination?"

- ***Example***: Several DPIAs and DPIA templates address the question of how easy it is for data subjects to exercise their data subject rights.

Some texts provided, however, seem to indicate that this is not yet fully engrained in the DPIA process at EUIs quite yet. This is supported by the following statement by a DPO: "In general the point of view of risks to the data subjects, not to the agency. When it comes to the DPIA, justification based on business activities instead of adopting the point of view of the data subjects should be the main driver. Unfortunately, it is not the case. Also, the risks towards the 'rights and freedoms' of the data subjects is a concept difficult to be grasped, as there is no immediate connection between the processing of personal data and how adversely that could affect rights and freedoms. Data processing is seen as something ethereal that has no direct impact on the lives of the data subjects, and if so happens, it is only limited cases under exceptional circumstances".

- ***Example***: A number of DPIAs were conducted on the use of **CCTV** by EUIs with premises located at potential routes of political demonstrations (some identifying demonstrators as potential security risk). Almost all fail to even mention the potential impact (chilling effect) of this surveillance measure might have on the freedom of expression and assembly, although the latter is explicitly referred to in the
  - EDPS Video-surveillance Guidelines (p. 29): "An impact assessment must be carried out... In case of surveillance in order to provide security during demonstrations... to ensure that the privacy and other fundamental rights of

the participants caught on the cameras, including, importantly, their rights to freedom of assembly, are not disproportionately intruded upon" as well as
- in Accountability on the ground Part II (p.11): "As an example, think CCTV in a publicly accessible area outside your EUI's entrance and how it may affect freedom of assembly and speech there".

- ***Example***: The EDPS' reply to a formal consultation on **social media monitoring** conducted by an EUI, which highlighted inter alia the following effects:
  - "...the diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy";
  - "The filtering by language and keywords might lead to assumptions of group behaviour that are inaccurate" and may thus create risks of group discrimination;
  - "The processing of personal data from social media - including special categories of personal data, personal data of individuals pertaining to vulnerable groups and personal data potentially related to criminal charges - creates risks to the fundamental rights and freedoms of individuals, including the rights to data protection and privacy, but transcending beyond them and potentially as far as to the right of asylum";
  - "The possible chilling effect on the freedom of the persons concerned to express their opinion and, possibly, their freedom of assembly and association and this effect's potentially severe implications need to be given due consideration".

Please find additional guidance and an illustrative example in **Annex II**, section 2 on **Understanding the risks to data subjects' rights and freedoms**.

Deciding on whether to do a DPIA

Threshold assessment

For most EUI, the majority of their finalised DPIAs, if not all (EASO, ECB, EIB), were conducted following a threshold assessment (see Accountability on the ground, part I, chapter 4.3 and annex 5).

Other reasons to conduct a DPIA

When invited to indicate how many DPIAs were done for other reasons (e.g. management decision) and what those reasons were, EUI mentioned the following:

- "...it concerned the first use cases...of cloud computing solutions. After those pilots, the risk assessment was limited to a documented legal compliance check";

- "...this is the only on-line platform the Agency has. As a result, there has been a conscious decision to move directly towards performing a DPIA";
- "Team building exercise – Controller's decision based on DPO's recommendations related to profiling and consent-based processing in the work environment";
- "...a DPIA was carried out because the developer of the platform was an external company chosen after a call for tender. The DPIA was carried out in order to demonstrate that the contractor was compliant with the data protection requirements";
- "Other identified processes relate to processes that were submitted to prior checking under Regulation 45/2001, we are in the process to review the already prior checked records."

Decisions *not* to carry out a DPIA

The next question concerned processing operations for which, following a threshold assessment, it was decided *not* to carry out a DPIA. Here, most replies noted that they had conducted threshold assessments, which simply had no resulted in two or more points: "all our records have scored 0 or 1 point"; "No processes were even close"; "The majority of assessments resulted in either zero or one positive answers to the risk assessment questionnaire, in those cases the DPIA was considered unnecessary".

***Example*:** One example provided concerns a threshold assessment for the follow-up of staff health and safety in the framework of COVID-19 pandemic crisis. Only one criterion for processing 'likely to result in high risk' was ticked ("Sensitive data or data of a highly personal nature"), noting that "the process involves health-related personal data of the [EUI's] staff members" as well as "information on COVID-19 symptoms of [their] household members, without mentioning their names".

The response to "Automated-decision making with legal or similar significant effect" as well as to "Data concerning vulnerable data subjects" and "Preventing data subjects from exercising a right or using a service or a contract" is simply "NO". One could envisage that showing COVID-19 symptoms might automatically exclude a staff member from being able to work on the EUI's premises and that household members, in particular children, could very well be considered vulnerable in this context. No further explanation for this is contained in the threshold assessment (see also below on the formatting of threshold assessment templates), which does not necessarily lead to a wrong result - but seems regrettable, as important considerations leading to the conclusion not to conduct a DPIA will remain undocumented.

Insights from full texts of two latest threshold assessments provided

Regarding **formatting**, most EUIs follow the format suggested for threshold assessments by the EDPS[5].

Those EUI using a checklist with full text instructions (rather than Excel sheets) including guiding examples and counterexamples, fare best in procuring proof of the controller actually having considered why the processing operation at hand merits a DPIA. This is in particular the case, where the controller is forced to explicitly *reason* respective box-ticking:

[5] See Accountability on the ground, part I, annex 5.

Example: DPIA Criterion: "*Applicable? Yes [if so, describe how] / No [if borderline: why not?]*".

From the threshold assessments and threshold assessment templates provided (26), it seems, however, that for some EUIS, this is a mere box-ticking exercise. One EUI provided the last threshold assessment with every single box ticked "no", but containing no further information.

Example *(see also above)*: For a threshold assessment for the follow-up of staff health and safety in the framework of COVID-19 pandemic crisis (including health data of staff, but also their household members), only the criterion "Sensitive data or data of a highly personal nature" was ticked. The response to "Automated-decision making with legal or similar significant effect" as well as to "Data concerning vulnerable data subjects" and "Preventing data subjects from exercising a right or using a service or a contract" was "NO", although one could envisage that showing COVID-19 symptoms might automatically exclude a staff member from being able to work on the EUI's premises and that household members, in particular children, could very well be considered vulnerable in this context. No further explanations were provided, as the template used contains no requirement to reason the "YES" or "NO" answer.

One reply indicated that the interpretation of "yes" / "no" replies allowed for **ex-post finetuning**: "Despite having ticked the box referring to the processing of health data, [we believe] that this processing operation does not constitute any risks to the rights and freedoms of data subjects. This is because as explained in ... this document, these health data are to a very limited scale and refer to the general conclusions that the Medical Service...reaches upon examining or receiving relevant information from the staff member."

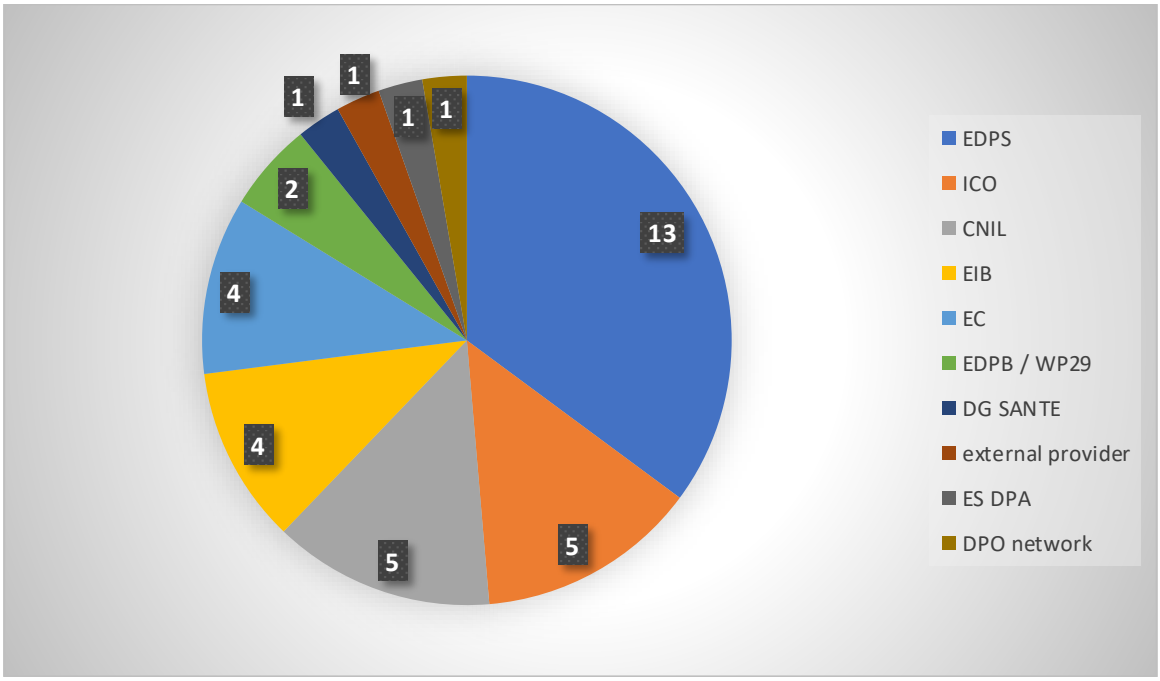
On **availability**, one EUI noted that "No threshold assessment has been carried out so far. However, the Data Protection team has created an online interactive tool for threshold assessment (pdf version of the form attached). The link to this tool is on the data protection intranet page, so that every controller would have easy access".

DPIA process

Please find additional guidance in **Annex II**, section 1 on **Systematic description of the envisaged processing operations and purposes**.

Methodologies used

EUIs have used multiple externally developed methodologies to conduct their DPIAs, with the majority taking their inspiration from the EDPS (Accountability on the Ground), the ICO, the CNIL, the EIB and the European Commission. Some EUIs have combined several externally developed methodologies to best suit their specific needs.



Internally developed methodologies

No less than 13 EUIs mention that they have developed specific **internal DPIA templates forms**, most including additional guidance to controllers: "Template based on EDPS template structure and guiding questions (accountability on the ground, Part II)"; "The DPIA template was developed within the DPO Network taking into account EDPS guidelines"; "In order to standardise the preparation of DPIAs, specific templates for Threshold Assessments and DPIAs have been prepared by CPVO, as well as guidelines for the assessment".

Other EUIs went even further, developing a **specific tool** ("In order to standardise the preparation of DPIAs and the link with DPO Records, [we have] updated the DPO Tool that was developed in-house in order to indicate if a DPO Record requires a Threshold Assessment and a DPIA"), a **DPIA checklist** ("DPIA Checklist was drafted internally also taking into consideration existing guidance from Article 29WP/EDPB and EDPS") or establishing a specific **internal methodology** ("Due to the difficulties to produce a DPIA and to understand what is needed in practice, an internal methodology is under preparation by the DPO to support the organisation with their tasks").

External consultants – experiences shared

Only very few (six of 39) EUIs relied at least partially on external consultants in drafting parts of their DPIA.

One EUI noted that it gets external help to review "the descriptive parts (reasons for the DPIA, description of processing) and to carry out an independent assessment as to the sections on necessity and proportionality analysis of risks, identification of control measures". Another EUI outsources only parts related mainly to ICT. One EUI highlighted that the methodology of splitting both roles (internal vs external) still remains to be defined.

One EUI shared that "Experience has demonstrated that heavy involvement and guidance from the internal interlocutors was necessary".

Another EUI noted the following: "When DPIA are contracted externally, there is a risk that those contractors do not come with the right knowledge and expertise and the DPIA cannot be completed successfully. For instance, we detected that the IT security professionals approach DPIAs as an opportunity for new business. Based on their IT security assessment background they trust they could produce a DPIA. However, this is not a guarantee since experience demonstrates that they struggle due to the need to count with the appropriate data protection skills. As lesson learnt, [we] will require that external companies ensure and prove that certified data protection professionals are part of the DPIA team – if possible, with certifications on conducting DPIAs."

One EUI requested guidance from the EDPS on the matter: "It would be advantageous to mention whether external contractors can be hired to carry out a DPIA and if that requires special procedures." In the light of the limited feedback received, it is difficult to conclude on any general guidance on the matter. However, it would seem safe to say that the involvement of external consultants is not a silver bullet.

Policy on publishing (summaries of) DPIAs

A significant number of EUIs (14) has no policy on publishing DPIAs or summaries of DPIAs; 11 EUIs explicitly note that, whilst they have no policy in place excluding publication, they do not publish DPIAs.

Arguments used to justify **not publishing** DPIAs include:

- "This is not a requirement and may reveal weaknesses in the system (e.g. security) which shouldn't be disclosed";
- "Due to confidentiality and security reasons, we do not publish summaries of the DPIAs";
- "No obligation seems to exist in the EUDPR to publish & in the EDPS guidelines".

12 EUIs **publish summaries** of their DPIAs, noting the following:

- "We are fully committed in having a high degree of transparency, and we consider using the dedicated data protection page we have in our website for publishing a short summary there";
- "As all EU bodies, [we follow] the applicable legislation and guidelines (recommendations from the Accountability on the ground toolkit.) We are currently envisaging the publication of summary of the future DPIA...".

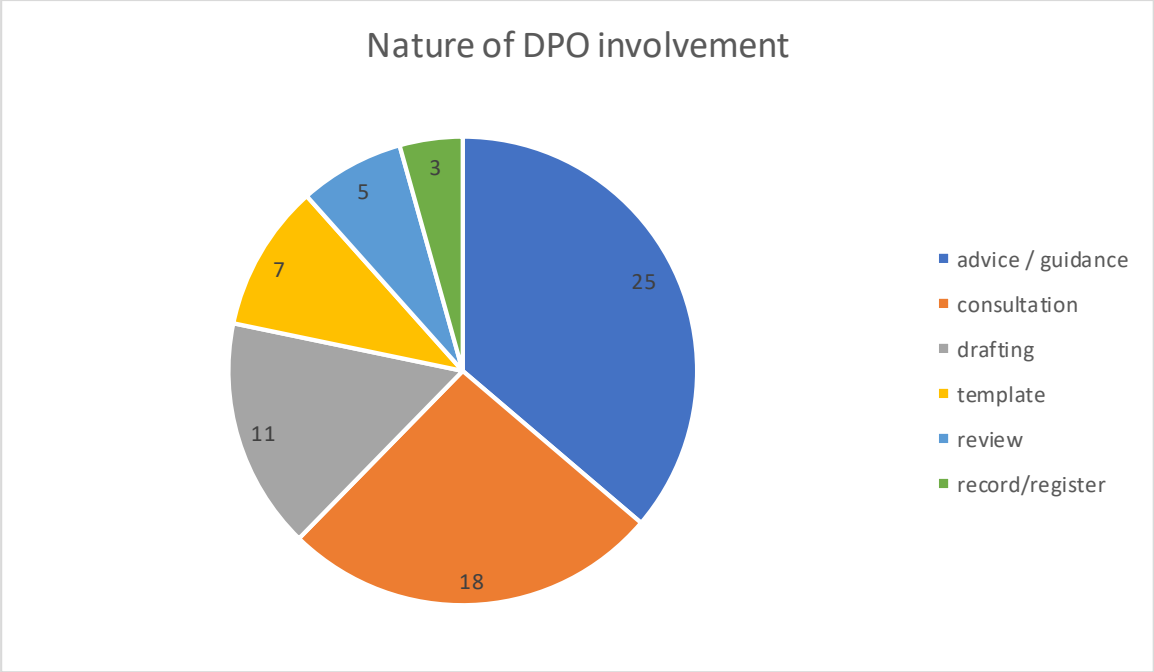
Only two EUIs (Curia, Eurojust) have a **policy stipulating that the DPIA should be made public - but only on the intranet**:

- Curia: "The DPIA is made available on the intranet together with the record and other documentation on the processing operation such as the compliance check, the threshold assessment and the information notice, unless the controller requests otherwise (for example for confidentiality reasons)";
- Eurojust: "We publish the full DPIA on the DP section of our Intranet".

DPO involvement

How does the DPO get involved?

According to the replies provided, DPOs tend to get involved in many ways and at all stages of the DPIA process: 25 noted that they give advice and provide guidance at various stages; 18 are consulted (mandatory in some cases: "the template for DPIAs provides explicitly that the Controller must seek the opinion of the DPO"); 11 are involved in drafting; seven are or were involved in the provision and the design of the respective template; five review the finalized product ("Consultation on drafts, plausibility assessment") and three mention their involvement in drafting the records and keeping the register.



One EUI reported that a specific overview documents the workflow (see **Annex III**) and explained: "Once the DPO is consulted regarding a specific project/initiative from the business area (controller):

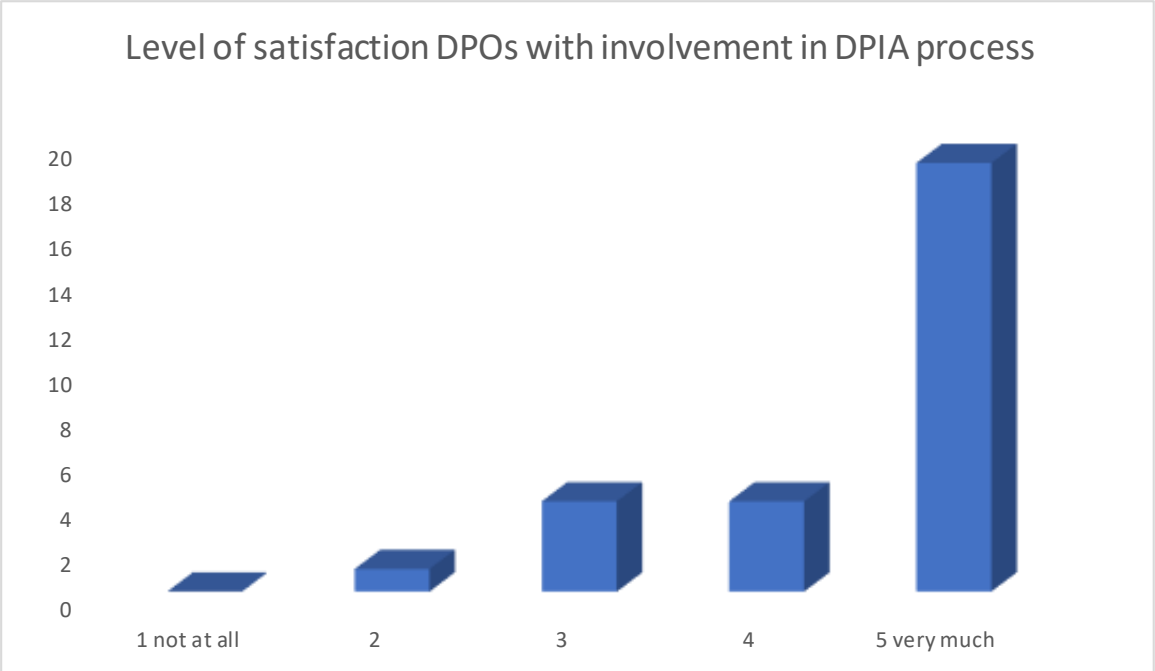
- The DPO advises if a DPIA is necessary;
- If the business area (controller), made aware of the risks, decides to conduct a DPIA, the DPO provides a DPIA template with guidance;
- The DPO assists the business area while drafting the DPIA;
- The DPO reviews the DPIA and provides comments".

Generally, comments provided suggest that for some DPO, the expectation of controllers is that the DPO gets very much involved in conducting the actual DPIA:

- "The DPO is part of the team that will conduct DPIAs, together with the business process owner and, if applicable, the external contractor";
- "Honestly, in most cases, the progress DPIA drafting mainly depends on the DPO input contribution";
- "The service might be too reliant on the DPO to conduct the DPIA. Ideally, the controller should lead with regard to the drafting of the DPIA."
- "It is usually the DPO the one who admonishes about the necessity of having to conduct a DPIA. It has never come from a controller in practice. After that, controllers do seek for advice indeed involving the DPO. However, in several occasions it is expected that the DPO takes decisions on data processing, whereas those decisions should always be taken by the controller itself. Also, when taking into account the risks and mitigating measures, I have noticed that either the risks are toned down or the mitigating measures are taken with the convenience of the EUI at heart, and that those decisions are not documented."

Level of satisfaction DPO involvement and suggested improvements

The level of satisfaction of DPOs regarding their involvement in the DPIA process is **surprisingly high**, with the vast majority of respondents (19 of 28) noting that they are "very much" satisfied (scoring 5 on a scale from 1 "not at all" to 5 "very much"). Four are pretty much satisfied (scoring 4 out of 5) and four have medium satisfaction levels (scoring 3 out of 5). Only one DPO is rather not satisfied (scoring 2 out of 5).



Several Agencies noted the following: "Considering that [we have] not done any DPIA yet, the experience that we have in practice is limited to providing the Controller with guidance at the stage of the threshold assessment. Regarding any future DPIA(s) that the Agency will have to

prepare, the template for DPIAs provides explicitly that the Controller must seek the opinion of the DPO."

DPOs came up with quite a number of ideas on what could be further improved:

- **Awareness raising/training** was the idea most often mentioned: "Awareness raising with controllers to empower on their accountabilities"; "In practice, the DPO often undertakes the burden of drafting the biggest part of the DPIA. We aim at more awareness raising within the controllers, in order for them to be in place to carry out such an exercise"; "In order to better evaluate the involvement of the DPO in this procedure, the Service is currently inviting all the administration to become familiar with the tool. Once more DPIAs will be conducted, it will be easier to do an evaluation"; "More awareness and feedback from the controllers having conducted the DPIAs"; "In general, we are satisfied with DPO involvement in DPIA. One area of improvement, however, would be on raising awareness internally to ensure the inclusion of the Data Protection Coordinator and the Data Protection Officer from the outset in order to timely identify and anticipate any potential risks from a data protection point of view"; "It will be necessary to provide targeted training to the persons involved".

  One contribution suggested that "Carrying out DPIAs when not strictly necessary can contribute to help controllers understand the process in practice" would be a good idea: "It also creates data protection culture and help to detect concepts that need further clarifications. Then, DPIA trainings and methodologies can be improved on those areas. For instance, the recommendation of seeking the views of the data subjects' representatives or other stakeholders when conducting a DPIA might need to be further explained to controllers."

- **More guidance or simplification**: "Simplification of the methodology"; "The methodology form has been perceived as rather complicated and cumbersome by the users. The DPO is thus working on an internal manual on the DPIA to facilitate the filling in of the methodology form in order to make the DPIA more straightforward"; "[we] would appreciate having centralized guidelines in implementation of the data protection regulation applicable to EU institutions and bodies so as to avoid different set of rules and different practices – such as conducting a DPIA (specific methodology per area of application)".

- **Additional internal support for the DPO**: A number of statements referred to a lack of resources at DPO level: "As part-time DPO, I entirely lack resources for such awareness-raising"; "Delay with the progress of the DPIA is linked to lack of resources and the high workload the relevant colleagues have to deal with. This applies for me as well as I am part-time DPO (I am also the legal officer of the Agency)"; "Also, some agencies have limited resources in those units. Thus, the participation on the drafting of the DPIA is not taken as a priority, or simply not supported as it is not view as an added value towards the Unit's objectives."

Two EUIs mentioned the involvement of DPCs as a possible way to resolve this issue: "We are currently considering the possibility of assigning data protection correspondents which could also be involved in providing assistance to data controllers in filling in this information"; "One area of improvement is perhaps the operational involvement of the DPCs in this process to help DPO, and in particular in terms of drafting (parts of) and carrying out a preliminary risk assessment".

Last, but not least, the EDPS was invited to "share a good example of a finalized DPIA". To not get stuck with the specificities of a particular processing operation at one EUI, please find in Annex II a section providing some additional orientations to the ones provided in the Accountability on the Ground Guidelines, raising awareness about certain best practices in a DPIA and common pitfalls.

Lessons learned

On the process of doing a DPIA

Lessons learned on the *process* of doing a DPIA (timelines, stakeholder involvement, etc.) consist of the following:

- Need to **flag data protection early on - and keep that focus**: "reflection on data protection issues should take place at an early stage, in order to provide the time and means for a potential DPIA"; "Timeliness regarding when DPO has to be involved in this process is one of the issues we learned in this process... we carried out an awareness campaign highlighting the importance of DPIA prior starting an affected processing operation and the involvement of DPO"; "The DPIA is carried out in a more effective way if the DPO is timely involved in a project (i.e. at an early stage)"; "In the designing phase of the tool receiving comments by stakeholder was fundamental in order to make the tool more user-friendly and readable".

  "In quite some occasions, the drafting of a DPIA requires a horizontal approach between different stakeholders within an Agency (i.e. ICT, Legal) that are able to enrich the DPIA from a different point of view besides that of the controller in practice. However, this elongates the process of drafting of a DPIA. A practical advice is to plan well in advance as the process can be very lengthy";

  However, "When involved at an early stage in development, it is worth double-checking that the DPIA submitted accurately describes the final product. Circumstances change from the initial proposal as different functionalities may be added/removed during the development and testing phases";

- Special caution regarding **involvement of processors / third parties**: "In case of a new process/tool: Identify whether third parties will be involved and in which capacity (e.g. services providers, consultants so on and so forth)"; "When processors are involved in the processing activity (e.g. external contractors), a DPIA cannot always be conducted

before contract signature, as the co-operation of the processors is needed. Therefore, in case of high risk, the contract with a processor should be conditional to the successful conduction of the DPIA, which should be done before the processing activity starts; also, the obligation of the processors for co-operation in the DPIA process should be included in the contract"; "For outsourced services, it is important that the service provider/ selected contractor contributes to the DPIA, which he is obliged to according to the contract (Art. II.9). There are discussions in DPO network as to when a DPIA should be done in the context of procurement outsourcing. In my opinion, the DPIA can happen after signature of the contract, perhaps conditional for the first interim payment".

"In case of platforms: Ask for detailed breakdown of tools that may be integrated in the platform and take into account that for software purchased under the Framework Contract of the Commission (in case the latter qualifies as SaaS) a lot of information should be already available to the procurement colleagues due to the need to have in place ad hoc clauses on inter alia data protection".

- Get the **controller in the driving seat**: "Kick-off the process by organising an ad hoc meeting to go through the template of the DPIA your organisation has. Many topics that may appear self-explanatory to a DPO may not appear as such to the rest of the organisation"; "...there may be a certain reluctance from the relevant services to conduct a DPIAs given the amount of work it requires"; "It is very time consuming and the business Units are reluctant to do it"; "Carrying out a DPIA is a very burdensome exercise for data controllers. Without additional resources allocated to cope with the increased administrative work required under the EUDPR, implementation of its provisions is a very challenging exercise. Awareness should be raised on this issue, since without additional resources granted by DG BUDG the Agencies cannot meet all the requirements of the EUDPR – and this is particularly evident when it comes to the need to implement a DPIA";

- **It ain't over till it's over**: "The DPO has to dedicate resources on monitoring the implementation of the outcome of the DPIA".

On the substance of the DPIAs conducted

Regarding lessons learned on the *substance* of the DPIAs conducted (usefulness for the controller, additional issues discovered, etc.), EUIs' statements can be grouped as follows:

Why conduct a DPIA?

The opinions on how useful conducting a DPIA can be considered and by whom seem to differ. Whilst there seems to be agreement that it is a beneficial exercise for a DPO, "selling" the need for a DPIA to the controller seems to be a challenge in some cases:

- "So far it has proven a very useful exercise... I consider it a fundamental document as a) it can serve as **starting point for any newcomer DPO**, b) it can serve as reference

document for **internal control and audit purposes**, c) it ensures that the controller… has an understanding on how well the [processing] 'scores' when it comes to protection of privacy";

- "The DPIA has proven to be a useful tool for the controller in order to think in detail the processing operation, identify risk scenarios and improve the quality of the processing";
- "Although a demanding exercise, DPIAs have proven to be a very important tool for the **controllers to realise the risks to the rights and freedoms of individuals** arising from processing operations; leading to increased data protection awareness within the Institution. The involvement of different stakeholders (controller, DPO, Information Security) leads to a more comprehensive assessment of the processing operation under consideration (identification of more/different risks, providing for appropriate mitigating measures)";
- "This DPIA has proven useful for the controller to ensure her readiness to complete additional ones in the future."

"The controller does not see any benefit in performing a DPIA. Also, it is lengthy and **not very practical**. Controllers perform a DPIA on request and insistence of the DPO, but since not all DPIAs need to be sent for prior consultation to the EDPS it is viewed as **unnecessary bureaucracy**. In several cases, the details to be provided overlap with the previous documentation requested (record, threshold assessment or other internal policies). As per substance improvements, in addition to be able to offer some extra incentive and to present it not only as a legal obligation, it would benefit if more detailed examples could be given, or a model could be shared with all Agencies (not only the template, but also the answers given) for other controllers to try to replicate the details".

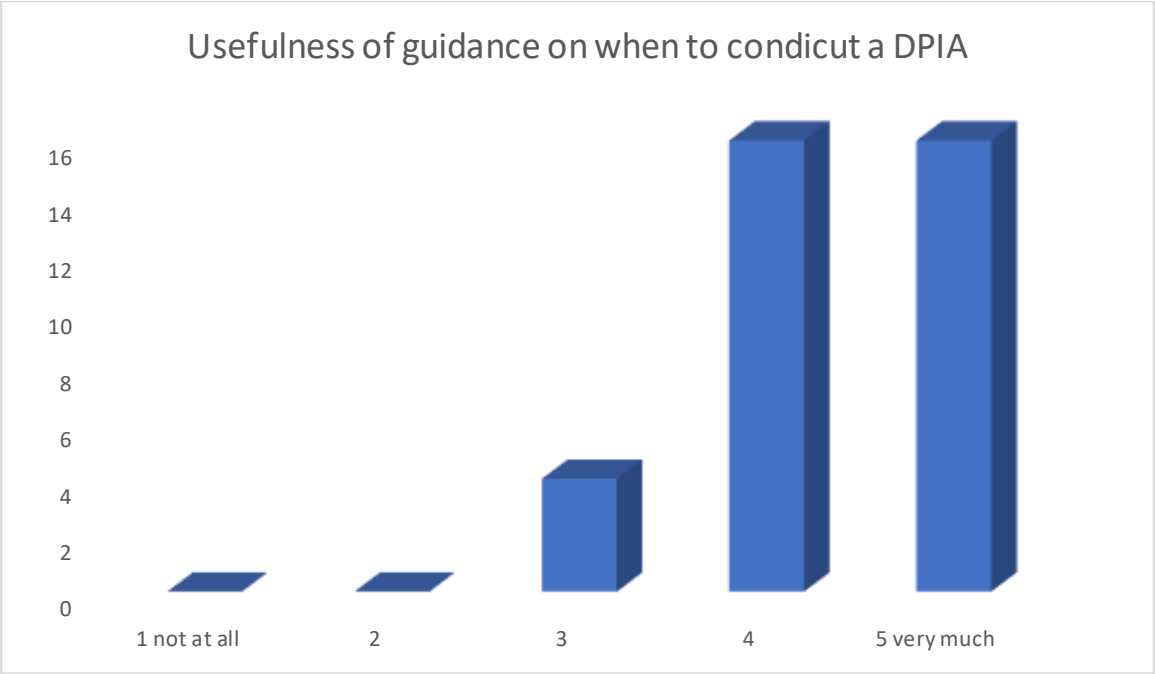
Other lessons learned

- **Scope DPIA**: "The DPIA we are going to conduct includes, as a matter of choice, not only the data protection risks, but also information security risk assessment. We believe that since the product under assessment is IT related, all aspects of risk should be investigated ";
- **Timing DPIA**: "Conducting a DPIA can be a lengthy process, sometimes it is difficult to obtain all the necessary information, especially if external processors are involved";
- **Tools DPA**: "A workflow is not requested systematically, but might be a helpful tool in some case where the procedure followed for the processing operation is not (yet) clear".

Feedback on EDPS guidance and suggestions for improvement

Usefulness of EDPS guidance on when to conduct a DPIA

When asked whether they consider the EDPS Guidance on when to conduct DPIAs useful (Accountability on the ground, part I), those of our stakeholders providing feedback (36 of 39) replied remarkably positive:



The suggested improvements consisted of the following (summary):

Keep it simple and eye your target audience: There EUIs asked for simplification of the procedure and the way the document is drafted in view of its target audience:

- "Language could be improved. Most controllers in practice find DP a useless obligation and also very cryptic, mainly because of the specific language the Regulation uses, which is viewed as very cryptic and only for professionals to understand. If the Document is addressed to a wide variety of Controllers, the language used should be one that all non-practitioners should be able to understand. Now all the weight of the "translation" has been placed onto the shoulders of DPOs, who not only need to offer advice, but to explain in understandable terms what each concept ad word means and entails."
- "The guidelines are very useful, but rather for DPOs than for controllers. Based on our communication efforts with our controllers, we have all reasons to believe that they would struggle to go through these guidelines. They are addressed to them, but we need to keep in mind that controllers in EU institutions are not data protection experts. We need to keep in mind the audience: heads of unit/Directors who want to comply with the Regulation, but would rather have clear guidance in less legalistic language on how to be accountable and transparent."

Going beyond the spirit of the Regulation? One EUI complained about the document going beyond what is required under the Regulation, noting that "It is a useful document, but it shows on several crucial elements signs of **voluntarism** in the side of EDPS in contradiction with the legal text. One cannot invent additional requirements that fit one's wishes but which are not in the legal text". According to this EUI, "the records template is made out much longer than it ought to be according to Article 31 (more precisely part II is **not at all legally required**, but smells of a wish to hang on to old Article 25 notifications...)". Indeed, there is no obligation

to use the template (which is explained in the EDPS' guidance). However, whilst Article 31 of the Regulation (demonstrate what you are doing as a controller) might not require such extensive documentation, it goes a long way towards fulfilling the controller's obligation under Article 26 of the Regulation, i.e. to demonstrate why certain processing operations happen the way they do - and not differently.

Also, according to this EUI, "the 'threshold criteria' for DPIAs are legally wrong and misleading. The legal text only has three criteria, while the EDPS... insists on nine". According to this EUI, this "smells of a wish to hang on to old Article 25 notifications, which were abolished" and goes counter the intention of the Regulation to **cut red tape and reduce paperwork**. In fact, as already noted by the WP29, the legal text refers to "in particular", which indicates that this is meant as a non-exhaustive list. The EDPS guidance is in line with the one given by the WP29 / EDPB and in no way differs from what DPAs all over Europe implement.

This request for a hands-off approach is difficult to square with the request by a significant number of EUIs (13) for **more EDPS guidance**. Whilst some just want **more concrete and practical examples** ("It is always very useful to increase practical examples"; "Relate to practical examples and respective guidance"; "More examples in grey areas could be provided"; "Some more specific examples for cases that are common for many EUIs could be very useful to support controllers and promote harmonised application across EUIs"), other EUI provide an insight into where they would expect additional examples:

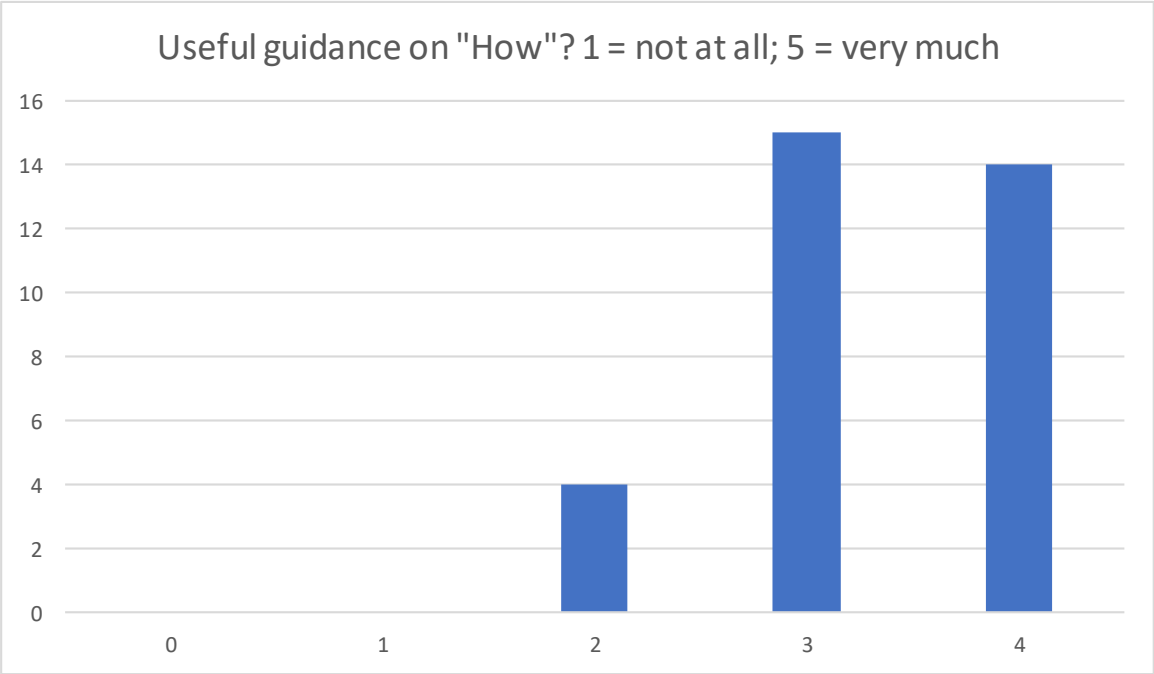
- "The section discussing the question "when" to carry out a DPIA could provide more details on dealing with **existing processing operations**, and on specific factors that may affect the decision on the need for the DPIA";
- "More potential examples in the positive list requiring DPIA."; "Annex 2 and Annex 3 on the **positive and negative list** could contain more processing operations" / "relying on super obvious examples in the positive and negative lists for DPIAs...is not helpful"; "...the negative and positive list and the threshold assessment could contain more concrete, illustrative examples and counterexamples";
- "More guidance on how to determine whether a DPIA or not in case the threshold of **two questions with yes** is reached would be appreciated with more concrete examples"; "For the cases where two "yes" are ticked, it would be very useful to have more examples and arguments as to when a DPIA must or is not necessary to be done"; "...more concrete examples of cases requiring a DPIA & cases with two or more yes in the threshold assessment not requiring a DPIA"; "It would be good to receive more guidance and arguments for the cases where two yes are ticked on which ground a DPIA must be done and on which case no DPIA is needed"; "maybe for threshold assessments with two elements ticked, more arguments and reasons could be provided why a DPIA must be conducted and in which case no DPIA is needed";
- "The guidelines could be more specific regarding the question when data processing actually takes place on **large scale** (both more guiding information and more examples/counterexamples)";
- "The **notion of vulnerable person** raises often questions. Is a staff member a vulnerable person or not? The guidance of the EDPB seems more strict in that regard and considers all staff/employees vulnerable persons. In practice, the notion is interpreted in the context of the processing operation. Especially when the processing

is based (partially) on consent of a staff member in a hierarchical relationship with the controller or involves sensitive or otherwise particular data, the staff member will be considered as vulnerable person";

- "Examples of **how to involve processors**; at what point in time to do a DPIA in case of procurement procedure";
- Where a specific DPIA needs to be conducted not only by one, but by several EUIs (e.g. Microsoft products), several EUIs suggested that there should be the **possibility of a joint / shared DPIA**: "the fact of requesting all [EUIs] to conduct individually their own DPIA without offering the possibility to share the one that has already been done could be perceived as not cost/efficient." One EUI questioned whether it makes sense and whether there is capacity for obliging "50+ EUI make their own DPIAs for each MS product (Windows, Office, Internet Explorer, SharePoint, Skype, etc.) all over again".

Usefulness of EDPS guidance on how to conduct a DPIA

Do you consider the EDPS guidance on how to conduct DPIAs useful (Accountability on the ground, part II)?



Responding to the request for suggested improvements, EUIs noted the following (summary):

Harmonise templates, checklists, tools & methodology

- "Common EUI model practical methodology and step-by-step templates with detailed instructions provided by the Supervisory authority."
- "A word format template DPIA report from the EDPS would be welcome";
- "More streamlined guidance, such as a checklist, would be advisable";
- "Useful document, but the EDPS...should make a clear EU-wide DPIA **template** available and not just a very incomplete structure/skeleton"; "It would be great if the EDPS and the other EUIs could develop together a EUI data protection **online/digital**

tool to fill in and manage records, threshold assessments and DPIAs. This would then help DPOs and responsible staff members (controllers in practice) to improve their cooperation and better monitor the level of compliance. A user friendly tool may also make DPIAs more appealing to the responsible staff members."

- On **methodologies**: "EDPS does not suggest a methodology, which I think is correct in order to reinforce the accountability of the institutions, but as practice develops, it would be good to reflect about the best methodology that could be used by EUIs"; "Annex 4 provides for a list of possible methodologies to be followed. However, deciding on one specific methodology from this list may prove difficult, and may need amendments, depending on the process itself. We are currently looking at the methodologies in the context of the future DPIA, and a centralised model for EUIs, who must lead by example, would be appreciated"; "It would be good to provide more indications/suggestions on the methodology for carrying out a DPIA".

Share examples and best practices

- "It would be good if example of best practices for DPIA (including concrete example) are shared"; "A concrete example of a completed DPIA could help to understand better the whole exercise." "Provide an example of a good DPIA"; "To the extent that it would be possible to share it, publishing one good example of a real DPIA (e.g. drafted by the EDPS) as opposed to one bad example of another DPIA would be extremely useful in order for us to see in practice how to do a DPIA". One EUI went even further: "Since the EDPS processes also personal data, it could share with us its threshold assessment & DPIA as best practice".
- "Maybe it would be useful following the template structure of a DPIA report, to have a real example of a case for which every EUI may need to perform a DPIA".
- "It might be helpful, if section 3.3 on the assessment of necessity and proportionality contained some example to illustrate these two rather abstract legal terms to non-lawyers." "The inclusion of more examples of risks that may be posed by certain processing operations and possible ways to mitigate them"; "Relation to practical examples and respective guidance".

Keep it simple

- "A shorter version/simplified of this document could be easier for controllers to follow"; "Simplification of the procedure";
- "A word format template DPIA report ...could be issued..., using a lay language understandable by data controllers"; "...guidelines are very helpful for DPOs. But controllers would probably find it difficult to assess the need of a DPIA and then conduct it by reading part III";
- "While records are quite straight forward as it is an evolution of the previous notifications, DPIAs are something newly introduced by the EUI DPR. Thus unfamiliar for several controllers. These need for more practical guidelines and clear examples on what they must do and how to do it. Too much leeway in the wording of their obligations construes a perception that details are not necessary and that the entire obligation is a mere tick box exercise to dress up compliance with data protection obligations, rather than a systematic assessment of data processes, risks and mitigating measures."

Other suggestions for improvements

Other or more general suggestions for improving our guidance on Article 39 included the following:

- "**Sharing good practices among EUIs** would facilitate our work."
- "In general, the more **real-world examples** are provided, the better. These could be examples from EUIs; they could however also be fictitious examples, or examples from outside the EU context (if the same principles apply, which they often would)."
- "It would be useful to provide a **FAQ section for controllers**, where the basic points related to DPIAs would be answered in simple way; it would also be useful that EDPS works, in co-operation with the DPOs network, on more specific examples of threshold assessment and DPIAs for "common" processing activities that are relevant to many EUIs."
- "We also see that some recommendations on the preferred tools as well as **standardisation of the evaluation criteria** from EDPS for carrying out the DPIAs would be required...We think that currently there is no consistent approach amongst EU Institutions and agencies which are following recommendations and best practices coming from national regulators and authorities, leading to very different assessments of the same processing or tool across the EU. Some clarification on the criteria to be used as well as whether we can follow these national recommendations would be appreciated";
- "The tool concerning **calculation of risk** could be more detailed"; "Provide a preference for a "risk assessment" methodology."
- "Based on the experience gathered, the guidance could be updated in the future to include tips/best practices."
- "Common model EUI **policy on publishing short versions of DPIA** provided by the Supervisory authority";
- "**Training from the EDPS** is without doubt the main suggestion and would be very much appreciated"; "A contact person at the EDPS, with expertise in DPIA, for direct consultation? A webinar on DPIAs?";
- "...some guidance on how to integrate the DPIAs, and also any privacy and data protection risk assessments, in the **procurement process** would be very helpful.
- "Guidance on how to implement the requirement of '**prior to the starting of the processing operation**' is needed...there is no clear idea amongst EUIs how to implement DPIAs in contract management (for both framework contracts and licenses purchase)."

Annex I : EDPS questionnaire on Article 39 of Regulation 2018/1725

1. General questions

1.1 How many DPIAs has your EUI carried out since the Regulation became applicable?

1.1.1 Please list the names of processing operations for which your EUI has carried out a

1.1.2 DPIA;

1.1.3 For each DPIA your EUI has carried out, please list the criteria triggering Article 39[6];

Name	Criteria

1.2 Please provide the full text of your EUI's two latest DPIA reports;

Attachment please

2. Deciding on whether to do a DPIA

2.1 Out of those DPIAs listed in 1.1.2, which were done following a threshold assessment[7]?

2.2 How many DPIAs were done for other reasons (e.g. management decision) and what were those reasons?

2.3 Please list the names of processing operations for which your EUI has, following the threshold assessment, decided not to carry out a DPIA;

2.4 Provide the full text of your EUI's two latest threshold assessments[8];

Attachment please

[6] Criteria as further explained in Accountability on the ground, part I, chapter 4.3 and annex 5.
[7] See Accountability on the ground, part I, chapter 4.3 and annex 5.
[8] See Accountability on the ground, part I, annex 5.

3. DPIA process

3.1 Which methodology/methodologies did you use for your DPIAs?

3.1.1 If externally developed, please share what you can (incl. publicly available information);

3.1.2 If internally developed, please provide (a reference to) the methodology;

3.2 Did you rely on external consultants for drafting (parts of) your DPIAs? If so, please explain for which parts and any experience you may want to share;

3.3 What is your policy on publishing (summaries of) DPIAs?

4. DPO involvement

4.1 How do you as DPO get involved in the DPIA process (consultation on drafts, providing guidance, drafting yourself etc.)?

4.2 How satisfied are you with the level of your involvement as DPO in the DPIA process?

Not at all - 1 o 2 o 3 o 4 o 5 o - Very much

What could be improved, if anything?

5. Lessons learned

5.1 Do you have any lessons learned to share on the *process* of doing a DPIA (timelines, stakeholder involvement, etc.)?

5.2 Do you have any lessons learned to share on the *substance* of the DPIAs you EUI has done (usefulness for the controller, additional issues discovered, etc.)?

6. Feedback on EDPS guidance and suggestions for improvement

6.1 Do you consider the EDPS Guidance on when to conduct DPIAs useful (Accountability on the ground, part I)?

Not at all - 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ - Very much

What could be improved?

6.2 Do you consider the EDPS guidance on how to conduct DPIAs useful (Accountability on the ground, part II)?

Not at all - 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ - Very much

What could be improved?

6.3 Do you have other suggestions for improving our guidance on Article 39?

Annex II: Some additional DPIA guidance

The ultimate goal of a DPIA is to make sure that controllers are able to understand and ensure that the processing operations are the least intrusive possible and that they comply with data protection rules. They will also be able to demonstrate this, in accordance with the accountability principle. Additionally, a good DPIA substantially contributes to fulfilling the controllers' obligation of implementing data protection by design, in addition to offering a methodological approach for it[9].

1. Systematic description of the envisaged processing operations and purposes

Establishing the context and describing processing operations is the foundation of a solid DPIA process. In short, you have to describe what you plan to and how you plan to do it. This documentation should allow the reader – be it those affected by the processing, your own top management, who will have to sign off on the DPIA report, the EDPS or other stakeholders – to understand what the processing is about and why you are doing it.

As set out in the Accountability on the Ground Guidelines (p.7), the description of the processing operations should allow the reader to understand what each of the processes is about and what the reason behind it is. The following elements have been identified in the guidelines as crucial in order to be able to provide an accurate description:

- a description of the **purpose(s)** of the processing: as with the other elements, this explanation should be carried out step-by-step, distinguishing between purposes where necessary[10];
- a **data flow** diagram of the process (flowchart): what is collected from where/whom, what is done with it, where is it kept and for how long, who is it given to? The EDPS expects EUIs to provide a detailed account of the different steps of the personal data processing operation in a connected matter, so that the lifecycle of the personal data can be more clearly understood. In addition, wherever the data stored in the same repository is used for different purposes, there should be one data flow per purpose;

  Example of a flowchart (high level data flow only): Arachne (EDPS prior-checking Opinion in case 2013-0340)
- a description of its **interactions with other processes** - does this process rely on personal data being fed in from other systems? Are personal data from this process re-used in other processes? etc.;
- a description of the **supporting infrastructure**: databases, incorporation of new technologies etc.

[9] EDPS, Preliminary Opinion on Privacy by Design, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[10] As part of this description, a brief explanation should be provided on why the organisations needs to carry out this processing operation and how it limits itself to what is necessary for the aim of the processing (necessity and proportionality).

As a starting point for its process description, EUIs could use existing documentation of the process development. A lot of the information required most likely already exists as part of project or process documentation kept for other reasons. EUIs may want to re-use this documentation as far as practicable and expand wherever necessary to entail the above information.

2. Understanding the risks to data subjects' rights and freedoms

A DPIA should identify and propose measures to mitigate the risks to the rights and freedoms of natural persons. These may result from personal data processing that could lead to physical, material or non-material damage. For instance, where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage or where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data[11].

Example: Personal data processing activities taking place in ETIAS are meant to support the decision of Member States to authorise or deny the entry of an individual to the EU territory, wherever this individual is exempted from the visa requirement. It is more specifically aimed at supporting the decision of whether the presence of this individual on the territory of the MS does not pose or will not pose a security, illegal immigration or a high epidemic risk[12]. A travel authorisation therefore "constitutes a decision indicating that there are no factual indications or reasonable grounds to consider that the presence of a person on the territory of the Member States poses such risks"[13].

Denial of entry may create a series of negative consequences for individuals: a restriction on the enjoyment of their freedom of movement, a financial impact if they travel to the EU for business purposes, impact on their health if they travel to the EU to get a medical treatment they cannot obtain in their own country[14]. Admission to the EU territory may be subject to additional checks at the border, thus interfering into this individual's privacy.

For these reasons, Article 14 of the ETIAS Regulation, entitled "Non discrimination and fundamental rights" puts the emphasis on a series of rights to which the data controllers should pay specific attention when implementing ETIAS system, namely:

- **Ensuring Non-Discrimination**. "Processing of personal data within the ETIAS Information System by any user shall not result in discrimination against third-country nationals on the grounds of sex, race, colour, ethnic or social origin, genetic features,

[11] Recital 46 Regulation 2018/1725.

[12] Recital 9 ETIAS Regulation. Article 3 (1)(6), (7), (8) define the terms "**security risk**" as the threat to public policy, internal security or international relations for any of the Member States, "**illegal immigration risk**" as the risk of a third-country national not fulfilling the conditions of entry and stay as set out in article 6 of Regulation (EU) 2016/399, and "**high epidemic risk**" as any disease with epidemic potential as defined by the International Health regulations of the WHO or the ECDC and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States.

[13] Recital 9 ETIAS Regulation

[14] For instance, there are cooperation agreements between Portugal and the Portuguese-speaking African countries (PALOP) regarding access to health care services to be provided to citizens of the latter in the territory of the first.

language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation". The right to non-discrimination is a fundamental right recognised by Article 21(1) EU Charter;

- **Protecting Human dignity**. The right to Human Dignity is protected by Article 1 EU Charter which says that "Human Dignity is inviolable". In the context of border management, this right is interpreted as an obligation for border controls to be carried out in a professional and respectful manner and be proportionate to the objectives pursued.[15] This also means that all travelers have the right to be informed on the nature of the control and to a professional, friendly and courteous treatment, in accordance with applicable international, Union and national law[16];
- **Protecting the rights to Privacy and Data Protection** (Articles 7 and 8 EU Charter);
- **Protecting more vulnerable groups of individuals**, in particular children[17], elderly and persons with a disability.

3. Adopting a systematic process for risk assessment

To allow for systematic assessment of risks, a DPIA methodology should be adopted. The goal of such a methodology would be:

- to allow for the definition of and justification for mitigating measures for the risks to data subjects;
- to estimate the residual risks to data subjects in order for the controllers' management to take an informed decision as to whether risks are adequately mitigated and proceed with the processing operation.

While you are free to select one of the existing DPIA methodologies[18] or create your own, for it to be of maximum effectiveness it should at least contain:

- a description of the roles and responsibilities of the different actors in the DPIAs exercises (e.g. who within the controllers will assess risks, who will select mitigating controls, who will sign-off the report). In case contractors are involved, explain their role and the relationships with key stakeholders of the system;
- a way to describe the business processes and data flows;
- a way to determine what events could create risks to data subjects ;
- a method to estimate the likelihood and impact of these events;
- a method to calculate the risks to data subjects based on the events, their likelihood and their impact;
- information on how the controllers' management will decide on which risks to data subject to mitigate, and the options they have for taking such a decision;
- a method for the risk analysis to propose the implementation of mitigating measures to reduce the risks to data subjects;
- a method to calculate the residual risks to data subjects;

[15] Recital 7 of the Schengen Borders Code

[16] Section 1.2 of the Practical Handbook for Border Guards (Schengen Handbook)

[17] The rights of the child are protected under Article 24 EU Charter which mandates public authorities to take childrens' best interest as primary consideration in all actions relating to children.

[18] refer to the EPDS and WP29 guidelines for DPIA

- information on how the controllers' management will decide on any residual risks to data subjects, and the options they have for taking such a decision.

Usually, the analysis of the risks to data subjects is qualitative *i.e.* estimated on scales (one for likelihoods, one for impacts and one for the risks).

While there is a clear information security risk management (ISRM) aspect to this (not least since keeping data securely is one of the data protection principles), ISRM is far from all there is to this exercise. ISRM tends to focus on risks that stem from unauthorised system behaviour (e.g. unauthorised disclosure of personal data), while parts of the risks to data subjects and compliance risks stem from the authorised system behaviour for which you do the DPIA.

Processes working exactly as planned may have impacts on data subjects. These risks have to be assessed as well, not only the risks of 'things going wrong'. To do so, use the data protection principles as a reference.

The "what-if" scenarios (events) rely on the knowledge of the operational staff as to what happens in the real world and their knowledge of the business processes and data flows. The key is to have a justified reasonable analysis. In case you involve a contractor in the DPIA, ensure you have identified the key stakeholders of the project to provide input (and feedback at the end) and establish a plan of their involvement/consultation in the process.

Furthermore, a justified reasonable **analysis of the business processes and data flows** will enable all stakeholders to better understand their roles and responsibilities.
As the processing operations become more detailed, the evaluation of the risks will need to be revised to ensure that

- the risks already defined are reasonably well evaluated;
- new risks are defined and properly analysed.

In the risk analysis, every step should be documented to be able to trace back why a mitigating measure was implemented vis-à-vis a specific risk to data subjects. In case of different opinions on the selection of mitigation measures, such opinions should be documented as well.

Annex III: Example: Workflow DPIA

Overview of the DPIA process

1. Identifying the need for a DPIA

The need for a DPIA can be identified by the following: EDPS list in Annex2; or two or more criteria of the EDPS list in Annex 1 are fulfilled ; or processing is likely to result in high risks to rights of the individuals in line with Article 39 of the Regulation (EU) 2018/1725.

DPO to draft part one of the DPIA

2. Consultation process

All relevant internal stakeholders should be consulted , e.g. DPO, information security etc.

Business Area (BA) to draft part two of the DPIA

3. Describing the information flows

Describe the data flows of the project.
Explain what personal data is used, for what purpose, who it is obtained from and disclosed to, who will have access, the supporting infrastructure and any other necessary information.

BA to draft part three of the DPIA

4. Assessment of necessity and proportionality as well as of compliance with the data protection principles

You should assess whether the processing activity is necessary and proportionate: Do your plans help to achieve your purpose? Is there any other reasonable way to achieve the same result? Do your processing activities comply with the data protection principles?

DPO to draft part four of the DPIA

5. Identifying the privacy risks for the data subjects

Risks to individuals: e.g. damage caused by inaccurate data, security breach, upset caused by an unnecessary intrusion on privacy.

BA to draft this part of the DPIA

6. Identifying and evaluating privacy solutions

Explain how you could address each risk (e.g. data protection audits, deletion rules in place, awareness trainings for staff, anonymising or pseudonymising data where possible, etc.). Some risks might be eliminated altogether. Others might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

BA to draft this part of the DPIA

7. Conclusion of DPIA

You should then record:

- whether each risk has been eliminated, reduced, or accepted;
- the overall level of 'residual risk' after taking additional measures; and
- whether you need to consult the EDPS.

DPO to draft the conclusion of the DPIA

8. Integrating DPIA outcomes

Integrating the outcomes of the DPIA into the project plans:

- You should identify any action points and who is responsible for implementing them.
- You need to keep your DPIA under review.
- You may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

BA to follow the integration of the DPIA results