08 September 2025

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

EDPS DPIA Survey 2024

Report

Contents

Table of Figures

Executive summary

Data Protection Impact Assessments (DPIAs) are an accountability tool introduced by Article 39 EUDPR. DPIAs are meant to help EU institutions, bodies, offices and agencies (EUIs) as controllers to ensure compliance with data protection principles in practice – and to demonstrate such compliance to external stakeholders, including supervisory authorities. The EDPS has issued guidance in the form of a non-exhaustive positive list of processing operations *prima facie* requiring a DPIA under Article 39 EUDPR, as well as a negative list of those that do not[1].

Under Article 40 EUDPR, the controller – after consulting the Data Protection Officer (DPO) – has to **consult the EDPS under certain circumstances** prior to the start of processing operations[2]. In line with the EDPB DPIA Guidelines[3], not all processing operations requiring DPIAs will also require such a prior consultation, though:

- There are cases in which following a DPIA and the (additional) controls implemented, risks will be appropriately mitigated to an acceptable level. Such cases do not require prior consultation;

- There may also be cases where, following the DPIA, the controller realises that risks cannot be mitigated to an acceptable level. In such cases, the project should be abandoned if it proves impossible to implement the processing in a compliant way;

- However, under Article 40 EUDPR, the **controller has to consult the EDPS** prior to the start of processing operations in cases where, despite reasonable measures to mitigate risks, **"high residual risks" remain.**

The aim of this EDPS survey was to gather information about how EUIs are conducting DPIAs and to compare the results with the previous survey on this topic, now that EUIs have acquired more experience. A 2020 survey on the topic[4] showed that, at the time, only 17 DPIAs had been finalized and the majority of EUIs had not conducted a DPIA yet. Now, four years on, the EDPS seems to have received **fewer prior consultations** under Article 40 EUDPR **than would be expected** in the light of how much the data processing landscape on the ground is changing, including the rising use of AI technologies and tools. Since the entry into force of the EUDPR end 2018, the EDPS has been consulted under Article 40 EDPR on **less than 40 DPIAs**.

DPIAs should be amongst the most valuable sources to understand such changes to the data processing landscape and the DPO has a unique horizontal view of what the challenges are in their EUI regarding DPIAs. This is why, on the basis of Article 32 EUDPR, the EDPS decided to launch an **EDPS Survey** on DPIAs addressed to all DPOs of EUIs using the EU Survey tool. In addition, he requested from each EUI concerned the **last two[5] DPIAs conducted** for which the controller

[1] The decision is also reproduced in Annex 5 to part 1 of the Accountability on the ground toolkit. If in doubt, EUIs should do a threshold assessment.
[2] Whilst an obligation to consult the EDPS also exists under Article 90 EUDPR for EUIs when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU and the respective DPIAs under Article 89 EUDPR follow the same structure, this exercise does not cover DPIAs on processing operations involving operational data.
[3] Available under https://ec.europa.eu/newsroom/article29/items/611236.
[4] Available on the EDPS website: https://edps.europa.eu/data-protection/our-work/publications/reports/edps-survey-data-protection-impact-assessments-under_en.
[5] The last ten for the European Commission, the European Parliament as well as the Council of the European Union.

decided not to consult the EDPS under Article 40(1) EUDPR, including a reference to the advice provided by the DPO under the last sentence of the said article.

Due to the volume and complexity of the expected submissions, the EDPS did not provide detailed, individual feedback to each EUI on the DPIAs received. Instead, the focus was on reviewing them to **identify overarching patterns and notable exceptions**. This approach allowed this report to analyse effectively the collective data, ensuring that it captures significant trends and anomalies that emerge from the broader set of submissions. This will feed into improving the EDPS' guidance on DPIAs.

As its 2020 predecessor, this exercise is exploratory in nature and is decidedly **not about naming and shaming** – this Report does not refer to EUIs by name.

Our main findings are:

1. **The DPIAs' landscape has changed since the last EDPS DPIA Survey in 2020.** Now the **majority of the EUIs have performed a DPIA** (compared to the only 17 DPIAs that had been finalised in 2020). **31 EUIs** stated in response to the Survey that they have **never conducted a DPIA at all** or none covered by our request.
2. Since 2018, EUIs carried out 242 DPIAs; during the same period, the EDPS received 3 prior consultations under Article 40 EUDPR.
3. 31 EUIs have performed less than 10 threshold assessments.
4. Sometimes EUIs identify the relevant risks of a processing activity in the threshold assessment - but then they fail to reflect these insights to the DPIA, e.g. the DPIA only focuses on security risks and does not reflect risks to data subjects.
5. 39 out of the 71 EUIs participating in this survey replied that they **rely on the EDPS template** when conducting their DPIAs
6. From the total of 79 DPIAs examined (two submitted were actually only a threshold assessment), **13% of the DPIAs failed to provide a systematic description of the processing activities.**
7. The majority of the DPIAs examined did not include a detailed data flow diagram (flowchart).
8. In 15 out of the 79 DPIAs examined in this survey, EUIs failed to demonstrate an assessment of the necessity and proportionality of the processing operations in relation to the purposes.
9. The involvement of the DPO in the threshold assessment, in the elaboration of the DPIA and the elaboration of the decision whether to consult the EDPS is often not documented by the controller.
10. Most EUIs adopt a numerical system to evaluate risks, some without clarifying how they end up with a specific score instead of another.
11. EUIs using threshold assessments and DPIAs that use a checklist with full text instructions including guiding examples and counterexamples, provide a more comprehensive overview for the specific outcome. This is in particular the case, where the controller is forced to explicitly reason respective box-ticking.

1. Methodology

This report is the result of a **two-prong approach**: the EDPS launch a **targeted questionnaire** (see **Annex 1**) using the EU Survey tool and, in addition, requested from each EUI concerned the **last two**[6] **DPIAs conducted** for which the controller decided not to consult the EDPS under Article 40(1) EUDPR, including a reference to the advice provided by the data protection officer.

Accountability means that it is the *controller* who is in charge of ensuring compliance and being able to demonstrate that compliance. The business owner / person responsible on behalf of the controller for a processing operation will be the main driver and the DPO (and DPCs, for those EUIs who have them) has the role to *assist* them (see EDPS Guidance, Summary, p. 3).

The structure of this report follows the generic DPIA process (see EDPS guidance *Accountability on the ground* Part II, p. 6):

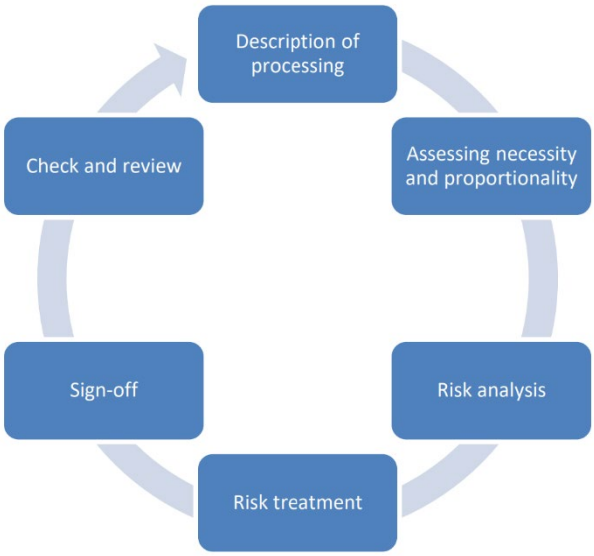


Figure 1: Generic DPIA process, EDPS Accountability on the ground Part II, p. 6

Regarding "*who does what?*", EDPS Guidance (e.g. Part I, p. 4 and Part II, Annex 1) clearly delineates what is for the controllers / business owner to do (notably draft DPIAs and analyse the need to continue to prior consultation) and what for DPOs. EDPS Guidance (Part II, Annex 1) in particular highlights that, unless otherwise indicated, the DPO:

- acts as the guardian managing the central register of records of processing operations (see Summary, p. 5);
- guides controllers through DPIA process;
- provides feedback on draft documentation/DPIAs;
- replies to consultations from controllers / business owners; and
- provides the liaison point between EUI and EDPS, including submitting prior consultations.

[6] The last ten for the European Commission, the European Parliament as well as the Council of the European Union.

Against this background, the **DPO has a unique horizontal view of what the challenges are** in their EUI regarding DPIAs. The EDPS therefore decided to address the survey's questionnaire to all EUI DPOs. To minimize the burden on DPOs, the number of questions was limited to ten and DPOs were given the possibility to let the EDPS know of any additional observations they want to share.

For this report, we analysed a **total of 79 DPIAs** for which the controller decided not to consult the EDPS. These are considerably **less DPIAs than expected**. We had contacted a total of 71 EUIs, asking for the last two DPIAs for which the controller decided not to consult the EDPS from every EUI except for the three "big" EUIs (European Commission, EP and Council, who were invited to provide the last ten such DPIAs). We could thus have ended up with a maximum of 166 DPIAs.

10 EUIs submitted one DPIA for which the controller decided not to consult the EDPS, 23 EUIs submitted two such DPIAs and three EUIs submitted more than three DPIAs. **31 EUIs** stated in response to the Survey that they have **never conducted a DPIA at all** or none covered by our request. As opposed to 2020, this is no longer the situation for the majority of EUIs[7]. However, in view of technical progress in the meantime and invasive processing operations in place during COVID-19, it could be considered somewhat surprising that still more than one third of all EUIs have not conducted any DPIA so far. One root cause for this might be the way in which some EUIs conduct a threshold assessment (if they do so at all) – see section 4 of this report.

The DPIAs covered various processing operations ranging from A like 'access control' to Z like 'Z (name of company) internet access service'. For small EUIs, the DPIAs provided were in many cases still within the realm of COVID-19 related processing of personal data (e.g. contact tracing).

Due to the volume and complexity of the submissions, we did not provide detailed, individual feedback to each EUI (this was announced in the letter to EUIs launching this exercise). Instead, our **focus was on** conducting a comprehensive review to identify **overarching patterns and notable exceptions**. This approach allowed us to analyse effectively the collective data, ensuring we capture significant trends and anomalies that emerge from the broader set of submissions.

2. Threshold assessment

EDPS guidance Accountability on the ground Part II, p. 31 defines "threshold assessment" as an "Assessment carried out by the controller, with the DPO's assistance, to find out whether a DPIA is needed".

2.1. What we asked in the questionnaire...

When assessing whether a planned processing operation triggers the obligation to conduct a DPIA under Article 39 of Regulation (EU) 2018/1725 (EUDPR), the controller shall conduct a threshold assessment.

[7] See findings p. 4 of the 2020 DPIA survey, available here: https://edps.europa.eu/data-protection/our-work/publications/reports/edps-survey-data-protection-impact-assessments-under_en.

The EDPS has published an **EDPS template** (see EDPS guidance Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, section 4.3 and Annex 5) to facilitate this task.

In response to our first question ("**How many such threshold assessments has your EUI conducted?**"), one EUI noted difficulties in replying because "There is no central register of threshold assessments and no obligation to request the advice of the DPO (even though often the DPO is consulted). This is a responsibility of the controllers."

The answers given reveal that a large number of respondents (31 EUIs) have performed less than 10 threshold assessments.

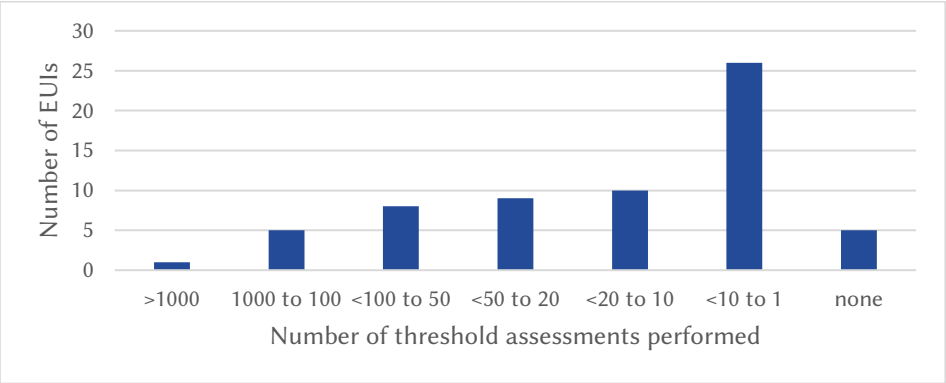


Figure 2: Aggregated data on the threshold assessments performed by EUIs

On the other hand, a considerable number of EUIs (12) state that they routinely conduct **a threshold assessment for each record** they establish.

Example: "The ... DPO has encouraged data controllers to fill in the Threshold Assessment since the entering into force of the EUDPR, as a risk assessment mechanism, even related to processes that did not appear to present risks. For that reason the number of threshold assessments is relatively high compared to the number of DPIAs conducted."

Example: "Each time (EUI) creates or updates a record we perform the threshold assessment."

Example: EUI "performs a threshold assessment for any new or updated process of personal data for which the Agency is the controller."

Example: "We conduct a threshold assessment for all data processing operations (part of our data processing record)."

Example: "Threshold assessments are part of all our records."

Example: "(EUI) would like to clarify that it uses the Data Protection Management System, as designed and implemented by the (EUI). In this system, the assessment of Art. 39 of the EUDPR and the EDPS threshold assessment are embedded and mandatory for each data protection record."

2.2. ...what we saw in the DPIAs provided

2.2.1. Was a threshold assessment conducted?

We had not explicitly asked for the threshold assessment leading to the DPIAs conducted in the context of this exercise. As some templates used by EUIs lead to the threshold assessment being an entirely separate document, those were mostly not provided.

Example: One EUI splits the DPIA process into four different modules: Threshold assessment, DPIA part I + II, Annex I Risk assessment.

This section consequently draws on the threshold assessments **only insofar as they were provided by the EUIs or are explicitly referred to in the DPIAs**.

2.2.2. Criteria identified

EDPS guidance Accountability on the ground Part I, p. 11 / section 4.3 (emphasis added): "...**In general, if you tick two or more of the criteria, you should do a DPIA**. Document this threshold assessment... However, the assessment cannot be reduced to a simple calculation of the number of criteria met. This is not an automated decision. Indeed, in some cases, a processing meeting only one of these criteria may require a DPIA. In other cases, a DPIA may not be necessary despite meeting two or more criteria. If you tick two or more criteria and do not consider that the processing would in fact cause high risks for the persons affected, explain why after consulting your EUI's DPO."

In 36 DPIAs (out of which 23 DPIAs were not related to IT aspects), no explicit reference was made to the criteria outlined in the "List of criteria for assessing whether processing operations are likely to result in high risks" provided in EDPS guidance Accountability on the ground Part I, Annex 1.

Insofar as EUIs did use those criteria (obviously, mentioning multiple criteria was possible, mentioning at least two likely), the three criteria referred to most frequently were:

- **Sensitive data** or data of a highly personal nature;
- Data processed on a **large scale**, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage;
- **Innovative use** or applying technological or organisational solutions that can involve novel forms of data collection and usage.

Data concerning vulnerable data subjects was referred to in five instances; systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting in four; Datasets matched or combined from different data processing operations also in four instances; three references were made to preventing data subjects from exercising a right or using a service or a contract and two each to automated-decision making and systematic monitoring.

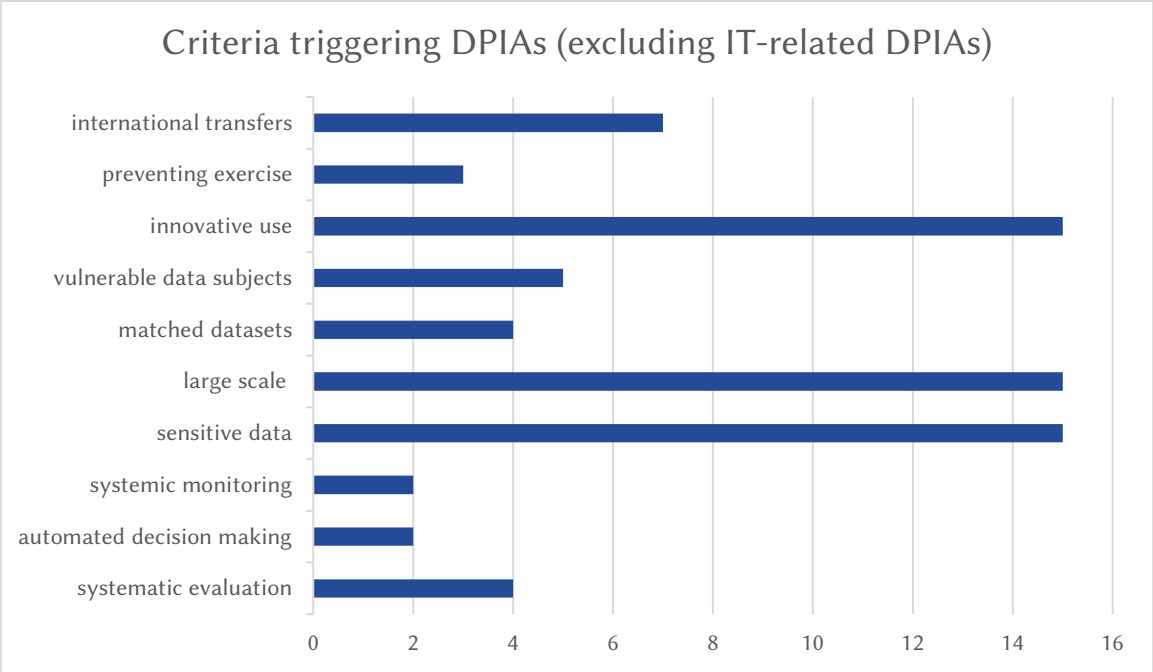


Figure 3: List of criteria triggering DPIAs (excluding IT-related DPIAs)

These findings correspond to the main criteria triggering the need for a DPIA under Article 39 EUDPR identified in the 2020 Survey.

Regarding IT-related DPIAs , the three most cited criteria are innovative use (four instances), vulnerable data subjects (four instances) and sensitive information (three instances).

2.2.2.1. Innovative use

Regarding the criterion of "**innovative use** or applying technological or organisational solutions that can involve novel forms of data collection and usage", one EUI suggested that **cloud computing** should not be considered as a high risk.

On the other hand, another EUI decided to conduct a DPIA on the very basis of cloud-based processing: "Taking into consideration that the data stored in the (tool) is not publicly available data and the (tool) will be hosted on Cloud, that therefore EUI, as would be the case in general with Cloud based infrastructure/platforms and services, will have less control on the way data are processed, the roles of the third parties in terms of accountability might also raise a certain level of uncertainty and should be assessed and defined clearly, the necessity to ensure that the physical location of data is in the EU will always be present, it was agreed to carry out a full DPIA to ensure the process, controls, risks, and mitigating measures are properly assessed, managed and documented."

2.2.2.2. International transfers

Nine DPIAs mentioned "**international transfers**" as a risk in their threshold assessment, although this criterion is not contained in the "List of criteria for assessing whether processing operations are likely to result in high risks" provided in EDPS guidance Accountability on the ground Part I, Annex 1.

One EUI explicitly suggested making international data transfers a part of the DPIA, possibly by **merging the transfer impact assessment into the DPIA**: "DPIAs need to include a part on international data transfers. There's also a requirement to carry out a TIA for international data transfers. We would appreciate guidance on how to ensure alignment of the two documents in cases where both DPIA and TIA are required - in such cases we suggest that TIAs should be part of the DPIA and there shouldn't be any need to do a separate additional assessment for TIA. Also it would be very helpful if the two documents were more aligned."

2.2.3. Criteria missed or misinterpreted?

EUIs generally referred to criteria triggering a DPIA that, in view of the information contained in the documents provided, seemed plausible in the light of the processing operation intended. This suggests that **there is no structural issue in recognising risks or interpreting them** and that the examples given in the "List of criteria for assessing whether processing operations are likely to result in high risks" provided in EDPS guidance Accountability on the ground Part I, Annex 1 are helpful in practice.

Example: One EUI dealing with 1:1 biometric access control using fingerprints (criterion 'Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage') explicitly noted in their assessment that this was listed as example for this criterion.

We only came across 11 instances for all criteria in which would it seem that an EUI may have missed or misinterpreted a criterion. Obviously, in all of these instances, a DPIA was actually conducted nonetheless - otherwise, the respective DPIAs would not have been submitted in the context of this exercise.

Example: 'Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting' was missed for a teambuilding involving profiling. In the same context, the EUI failed to examine 'data concerning vulnerable data subjects'. Staff members could be considered vulnerable data subjects where a power imbalance means they may not be able to easily object to the processing of their data by an employer (the latter was plausible according to the DPO comments contained in the DPIA).

Example: 'Sensitive data or data of a highly personal nature' as well as 'data concerning vulnerable data subjects' were both not addressed for e-recruitment.

Example: 'Data concerning vulnerable data subjects' was denied for a case involving an internal competition - although data subjects will mostly have been EUI staff, thus in an employer-employee relationship. The reasoning provided was "Internal competitions represent a career opportunity - they are not an obligation of the employee to participate in, but an option/choice. To achieve similar results in their career, potential candidates have also other options - participating in external competitions...". These other options obviously do not change the nature of the data processed - or make employees less vulnerable once they joined an internal competition.

2.2.4. Advice of the DPO on the need to conduct a DPIA

In many cases, the involvement of the DPO in the threshold assessment (or the resulting need to conduct a DPIA) **was not documented**, making it difficult to conclude whether controllers saw a need to consult the DPO when applying the "List of criteria for assessing whether processing

operations are likely to result in high risks" provided in EDPS guidance Accountability on the ground Part I, Annex 1.

The accountability principle under Article 4(2) EUDPR means that verifying whether a DPIA needs to be conducted is the task of the controller. The respective ***advisory* role of the DPO** is stipulated in Article 45(1)(e) and (f) EUDPR: "*The data protection officer shall have the following tasks: …*

(e) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 and to consult the European Data Protection Supervisor in case of doubt as to the need for a data protection impact assessment; …"

(f) to provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40; to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation."

In one case, however, it seems that it was the **DPO who actually *conducted* the threshold assessment** and the DPIA: "The assessment and recommendations fall in the scope of the DPO tasks as provided for in Article 45 of the EUDPR, and further defined in the … implementing rules on data protection and on the tasks, duties and powers of the data protection officer"; "The review was performed on the basis of the information provided by the delegated/controller for this processing operation and by the Processor within the scope of data privacy and shall not be considered as a data security assessment. The implementation of the actions and safeguards as recommended are responsibility of the controller."

However, EDPS guidance clearly highlights that checking whether a DPIA needs to be conducted is the task of the business owner:

> EDPS guidance Accountability on the ground Part I, p. 4: "…checking whether you need to do a DPIA is your job as the business owner – your DPO can help you with this, but it is your task to get it done."

3. Conducting a DPIA

Under **Article 39(1) EUDPR**, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

EUROPEAN DATA PROTECTION SUPERVISOR

Annex 2
Non-exhaustive list of some common processing operations and prima-facie indications of their risks

Positive list of processing operations prima facie requiring a DPIA (the numbers inside the brackets refer to the criteria in the template threshold assessment in Annex 1 such processing operations will likely trigger):

- Exclusion databases (2, 4, 9);
- large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) (1, 4, 5, 8);
- internet traffic analysis breaking encryption (data loss prevention tools) (1, 3, 8);
- e-recruitment tools automatically pre-selecting/excluding candidates without human intervention (1, 2, 8).

Figure 4: EDPS positive list of processing operations prima facie requiring a DPIA

Annex 3
Non-exhaustive list of some common processing operations not requiring a DPIA

Indicative list of processing operations prima facie not requiring a DPIA when carried out by Union institutions, bodies, offices and agencies acting as sole or joint controllers:

- Management of personal files under Article 26 of the Staff Regulations *as such*[6];
- Standard staff evaluation procedures under the Staff Regulations (annual appraisal);
- Standard 360° evaluations for helping staff members develop training plans;
- Standard staff selection procedures;
- Establishment of rights upon entry into service;
- Management of leave, flexitime and telework;
- Standard access control systems (non-biometric)[7];
- Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in public space).

Figure 5: EDPS negative list of processing operations prima facie not requiring a DPIA

Respective EDPS guidance includes a **positive list** of processing operations *prima facie* requiring such a DPIA under Article 39(4) EUDPR as well as a **negative list** of processing operations *prima facie* not requiring a DPIA under Article 39(5) EUDPR.

These lists contained in EDPS Decision of 16 July 2019 are also reproduced in Annex 5 to Part 1 of the Accountability on the ground toolkit, which also provides explanations on how to carry out a DPIA.

3.1. Number of DPIAs conducted by EUIs since 2018

A **total of 242 DPIAs** have been conducted under Article 39 EUDPR by EUIs since the entry into force of the EUDPR. This is a **significant increase since 2020**, when the last survey on the topic[8] showed that, at the time, only 17 DPIAs had been finalized.

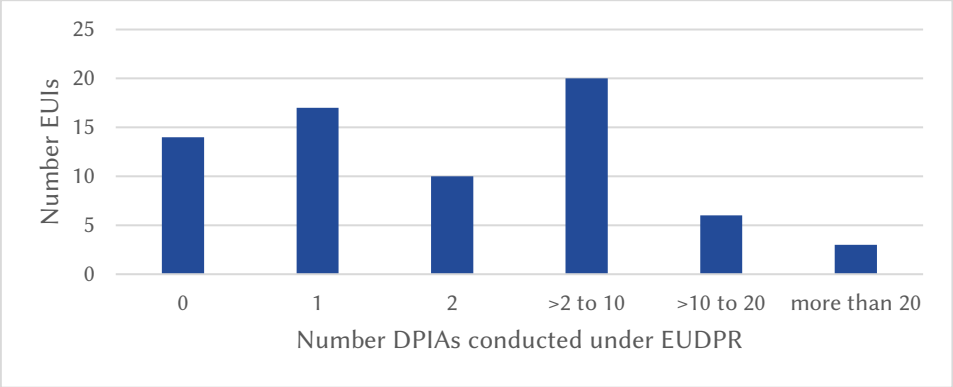


Figure 6: Aggregated DPIA count data

Only three EUIs have performed more than 20 DPIAs, though.

In contrast, a large number of respondents (**41 EUIs) have performed either none or only one DPIA**, i.e. less than the (last) two[9] DPIAs we had initially requested. Two EUI provided only a threshold assessment, not a DPIA.

One EUI noted their experience so far has been that "sometimes a data controller decides to carry out a DPIA (even if the threshold assessment criteria are not met) in order to gain insight of the process/project and see how a process/project can be designed in an even more privacy-friendly manner."

3.2. Publication of DPIAs

Under Article 4(2) EUDPR, EUIs as controllers are accountable for being compliant, but also for being able to demonstrate it - to all stakeholders, not just the EDPS. DPIAs under Article 39 EUDPR are an **accountability tool** to achieve this. According to EDPS guidance (Accountability on the ground Part II, section 3.9), the publication of DPIA reports is a **good practice** and EUIs should strive to at least publish a summary of the report (i.e. parts of the reports that should not be disclosed to the public, e.g. details on security measures, can be removed where appropriate).

However, in reply to our third question ("Do you have a policy to publish DPIAs?"), **only 8 EUIs indicated that they actually have a policy to publish DPIAs**, some of which publish at least a summary of the DPIA.

[8] Available on the EDPS website: https://edps.europa.eu/data-protection/our-work/publications/reports/edps-survey-data-protection-impact-assessments-under_en.
[9] The last ten for the European Commission, the European Parliament as well as the Council of the European Union.

- "Regarding the publication of DPIAs, the (EUI) DPO guidelines on DPIAs recommend publishing the summary of the DPIA's main findings to build trust in the Agency's processing operations, as well as to demonstrate accountability and transparency."
- "(EUI) has a policy in place: Annex III internal guidance on data protection, where the decision to publish a DPIA lies with the business owner (step 7 of the DPIA process)."

Three EUIs mentioned their intention or **ongoing work to adopt a policy** to publish DPIAs or summaries of DPIAs in the future:

- "(EUI) is finalising its first DPIA and aims at building a written procedure on the basis of this first case exercise; and at publishing some parts of the DPIA, thereby setting a policy for publishing DPIA";
- "...we intend to adopt a policy to publish DPIAs and a written procedure for applying Article 39 EUDPR, making use of what already exist at the level of other Joint Undertakings, which would allow us to gain time and efficiency with the objective to achieve full compliance.";
- "(EUI's) DPO is currently drafting working instructions on data protection that will also cover the procedure to be followed when conducting DPIAs / threshold assessments, as well as the publication of the summary of DPIA reports."

Thus the **majority of EUIs currently foregoes the potential of their DPIAs as accountability tool** vis-à-vis the general public.

4. DPIA methodology / template

EDPS guidance Accountability on the ground Part II, p. 5: "The DPIA process aims at providing assurance that controllers ... adequately address privacy and data protection risks of 'risky' processing operations. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of 'data protection by design' where it is needed the most, i.e. for 'risky' processing operations."

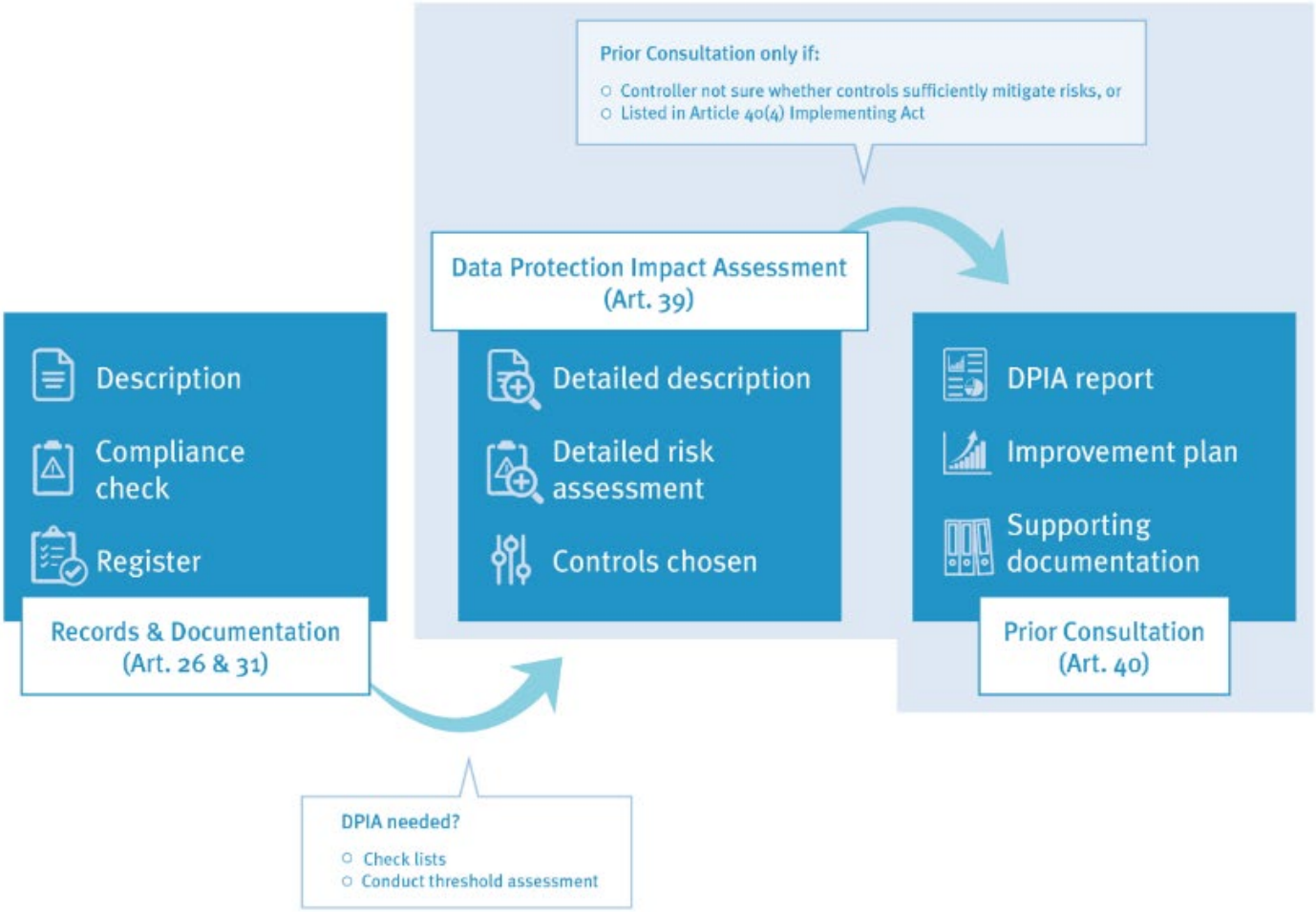


Figure 7: Overview of documentation obligation, EDPS guidance Accountability on the ground Part II, p.3

4.1. Use of EDPS guidance documents

The EDPS has issued guidance for controllers and DPOs in the EUIs on how to generate records for their processing operations, how to decide whether they need to carry out data protection impact assessments (DPIAs) and how to do DPIAs and when to do prior consultations to the EDPS (Articles 31, 39 and 40 EUDPR). The current version was published in July 2019.

One of the possible outcomes of this exercise is the need to update our existing guidance on DPIAs.

Figure 8: Cover pages of the EDPS guidance on DPIAs

We therefore explicitly asked whether EUIs **apply this EDPS guidance** when conducting threshold assessments and DPIAs. 70 EUIs, thus **all but one respondent**, noted that they do. One EUI noted that they had issued their own "DPIA guide".

A number of EUIs used the free text section to include suggestions regarding an **update** or future additions to existing EDPS guidance. For an overview, please see section 13.3. below.

4.2. Written procedure for applying Article 39 EUDPR

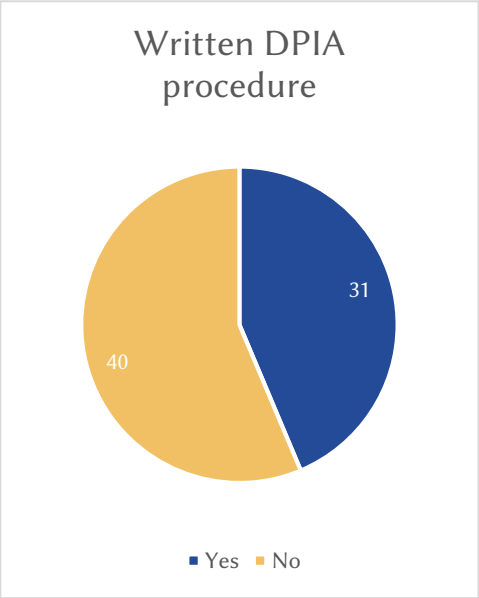
Under Article 27 EUDPR, EUIs as controllers are under the obligation to organise their systems' development processes in such a way that data protection considerations are taken into account at each step ('**data protection by design**').

As noted in EDPS guidance (Accountability on the ground Part II, section 3.1), by providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs under Article 39 EUDPR help organisations to comply with the requirement of 'data protection by design' where it is needed the most, i.e. for 'risky' processing operations. Some EUIs have developed written procedures to guide their structured thinking such as DPIA frameworks.

4.2.1. Absence of a written procedure for applying Article 39 EUDPR

When asked whether they have established a **written procedure** for applying Article 39 EUDPR, the majority of EUIs (40) replied that they have not laid out the procedure in writing. 31 EUIs, however, have a written procedure in place.

One EUI noted their intention to "adopt … a written procedure for applying Article 39 EUDPR, making use of what already exist at the level of other Joint Undertakings, which would allow us to gain time and efficiency with the objective to achieve full compliance."



Another EUI noted that there was no need to adopt any written procedure for applying Article 39 EUDPR "as the (EUI) DPO is consulted on all processing activities and is participating as observer in the (EUI)'s IT management board which is consulted and informed about all major IT projects of the EUI".

One EUI noted that "The question is unclear... In the (EUI), a threshold assessment is integrated in the record management tool... This means that delegated controllers always have to address the threshold assessment when addressing the legal obligation to have a record. Answering y/n to whether there are "written instructions specifically on DPIA" is therefore misleading as there is a general obligation (in law and in our guidelines) to have a record and the delegated controllers will need to address this aspect when meeting obligation to have a record."

Figure 9: Number of EUIs with a written DPIA procedure

4.2.2. How does this compare to best practice examples?

When compared to those EUIs identified as representing at least partially a best practice example in the context of the DPIAs provided for this exercise (see below), only half of the best practice EUIS have a written procedure in place. There is **thus not necessarily a correlation** between having a written procedure and the quality of the DPIAs performed. However, a written procedure might inform staff responsible for designing processing operations of DPIAs and thus should contribute to ensuring that a DPIA is actually conducted when it should be.

4.3. DPIA template

Article 39(7) EUDPR defines the minimum content of a DPIA, but the EUDPR does not contain a standard methodology for doing DPIAs. However, any methodology used has to comply with the EUDPR's requirements.

EDPS guidance Accountability on the ground Part II, pp. 6/7: "The EDPS does not impose a specific DPIA methodology on EUIs. You can use any methodology that complies with the rules, the EDPS example provided in this document or another methodology compliant with the WP29/EDPB guidelines."; "Annex 3 provides a template structure for such a DPIA report".

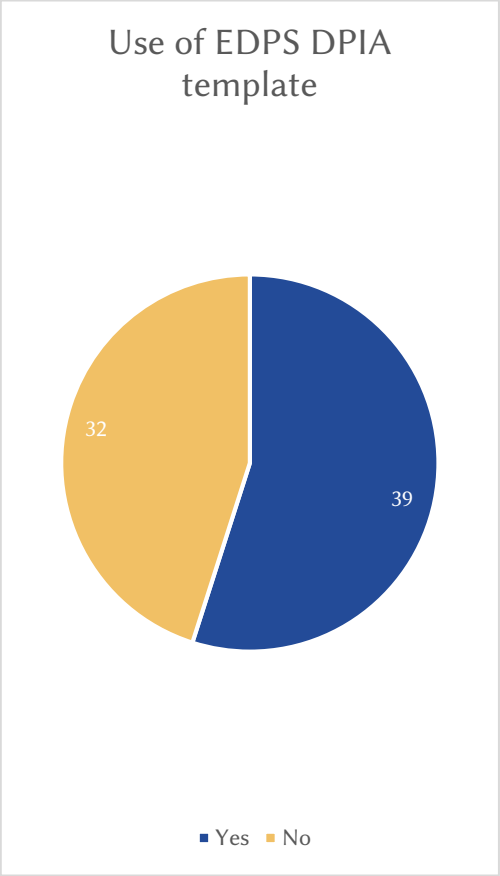
As outlined in EDPS guidance (Accountability on the ground Part II, pp. 6/7), EUIs are free to use any compliant methodology.

For ease of reference, the EDPS provides an example for the generic principles for DPIA processes, including a template structure for a report in Annex 3 and refers to other existing methodologies in Annex 4, first part.

4.3.1. What we asked in the Survey

We asked whether EUIs are using the **EDPS DPIA template** / **model DPIA** outlined in EDPS guidance (Accountability on the ground Part II, Annex 3) for advice on the elements listed in Article 39(7) EUDPR.

4.3.1.1. EDPS DPIA template / Model DPIA



From the 71 EUIs replying, the **majority** (39) replied that they **rely on the EDPS template** when conducting their DPIAs.

Three EUIs announced that, **for the future**, they intend to rely on the EDPS template rather than the one offered by another EUI:

Example: "The Agency will start using the EDPS DPIA template for next assessments, instead of the template provided by the (another EUI)."

Example: "(EUI) uses the template of (another EUI) ... (EUI) is considering replacing its DPIA template by the one published in the EDPS Guidelines to avoid repetition and duplication of information, which is available in the record and to focus only on the risk assessment since the DPIA is annexed to the record."

Example: "(EUI) is currently using the DPIA model template of (another EUI)... but (EUI) will reflect if it would be more appropriate to use a less repetitive and more focused DPIA template, like the one proposed by the EDPS."

Figure 10: Number of EUIs that use the EDPS DPIA template

4.3.1.2. Other templates used

For those EUIs not using the EDPS template, we asked whether they are using any other DPIA template / model DPIA. **32 EUIs either rely on a different template or they use their own** template.

4.3.1.2.1. Model inspired by the EDPS template

In designing their own template, some EUIs took inspiration from the EDPS template:

Example: "The (EUI) has developed its own template for DPIAs, which incorporates the EDPS guidance of 2019 'Accountability on the ground'. ...The (EUI) DPIA template guides controllers and their staff on what should be considered when carrying out a DPIA."

Example: "EDPS guidance was mainly used to build (EUI)'s DPIA template."

Example: "The (EUI) in its DPIA Guidance has taken into account and used specific elements, including Guiding Questions from the EDPS Guidance document and the (EUI) used own template versions based on the EDPS template. In one case, the (EUI) used an external contractor to assist in conducting the DPIA. Thus, the (EUI) has used both methods of conducting the DPIA on its own as well as the one time involvement of an external contractor…"

However, one EUI noted that: "The EDPS Guidelines/template on Accountability on the ground is not really fitting as guidelines or template for DPIAs. It would be very welcome to have a template, particularly in relation to the description of the processing operation, as we have observed that on occasions the expectation is higher. Equally, it would be also welcome to see what is the criteria used by the EDPS to consider the **acceptance of the EUI of the risks** after mitigation measures, as in principle that would belong to the **risk appetite of the EUI**."

In this context, the EDPS noted in its EDPS guidance Accountability on the ground Part II (p. 16) that "When selecting the controls/mitigating measures, **compliance with the Regulation is the minimum standard** you cannot go below." In addition, the EDPS explained that "…while the shift towards a 'risk-based approach' in the GDPR and the Regulation is one important feature of the new rules, there is still a certain floor of specific requirements to ensure compliance, which your organisation cannot fall below without exposing itself to regulatory action. Put differently: there are risks that your organisations must not simply accept, but will have to mitigate or avoid. Think of these as mandatory controls included by the legislator because they are always a good idea. This concerns especially the protection target fairness. Your EUI cannot say 'we won't provide access, it's too much of a hassle', but your EUI may be able to say –when appropriate– that 'given the few requests we expect in this new system, we will not invest in an automated self-service system for people to obtain access, but will only provide a contact point and deal with requests manually when they come in'…".

4.3.1.2.2. European Commission model

Most respondents not using the EDPS template replied that they rely on an alternative model conceived by the **European Commission**.

Example: "The processing operations carried out by (EUI) which require a DPIA are linked to systems managed by the European Commission (…). Considering the link, the DPIA of (another EUI) is used as basis for preparing the internal one."

Example: "Model templates used based on (another EUI) template (part I and part II). (Another EUI's) on-line tool for evaluating the level of risk for a personal data processing operation has been also used as complement of the DPIA to test the impact of the measures proposed."

Example: "(EUI)'s DPIA follows all the content indicated for DPIAs by the EDPS, however we used in our first DPIA (another EUI)'s template. When another EUIAB has carried out a DPIA, and with a view to maximise synergies, we consider that (EUI) should by default aim at building its own assessment on that, while ensuring that variations in processing (liabilities) are duly assessed for impact and duly documented. In particular, this is in particular challenging when (EUI) uses a service provider of (another EUI) and has not been involved in the negotiation of the terms of the contract, but still (EUI) is the controller and liable for the processing."

4.3.1.2.3. Templates issued by national data protection authorities

Other EUIs rely on templates issued by **national data protection authorities**:

Example: "The methodology used draws on guidance issued by the EU Data Protection Supervisor (EDPS) and the UK Information Commissioner's Office (ICO)".

Example: "(EUI) uses the EDPS DPIA template but included additional provisions based on the DPIA template of the CNIL. (EUI) uses the template developed by the French Health Data Hub for activities for which the DPIA requires submission to the CNIL."

The ICO model is available here; the CNIL model here.

4.3.1.3. How does this compare to best practice examples?

Whilst the majority of best performers use the EDPS template, some of the EUIs providing us with best practice examples in reply to our exercise have come up with their very own template.

4.3.2. ...what we saw in the DPIAs provided

Some DPIAs were partially blackened out; one EUI found it impossible to share a particular DPIA for security reasons.

Since there is no single mandatory DPIA template, (almost) all DPIAs provided looked different.

- As for the 2020 Survey (p. 6), there is a **remarkable spread regarding the length** of the DPIAs provided, which ranges from four to several dozen pages. And as for the 2020 predecessor exercise, given the variety of topics and the very different formatting options used (anything from full text to excel tables in fine print), this represents admittedly a presumably weak indicator, as illustrated by a DPIA conducted on COVID 19 contact tracing on only seven pages. However, given the comprehensive analysis and the weighing of different risks needed to produce a meaningful DPIA, a five page DPIA still remains at any rate less than required.

- **Joint DPIAs**: As noted in EDPS guidance Accountability on the ground Part II, p. 3: "According to Article 39(1) of the Regulation, 'a single assessment may address a set of similar processing operations that present similar high risks'. Such 'joint' DPIAs may be appropriate when several EUIs implement processing operations in the same way, e.g. because they have identical rules for specific procedures or because they use the same product in the same way." Not many EUIs provided a DPIA jointly established with another EUI.

- In the 2020 Survey (p. 9), we noted in the context of threshold assessments that "Those EUI using a checklist with **full text instructions (rather than Excel sheets)** including guiding examples and counterexamples, are clearer. This is in particular the case, where the controller is forced to **explicitly reason respective box-ticking**". The same is true for DPIAs.

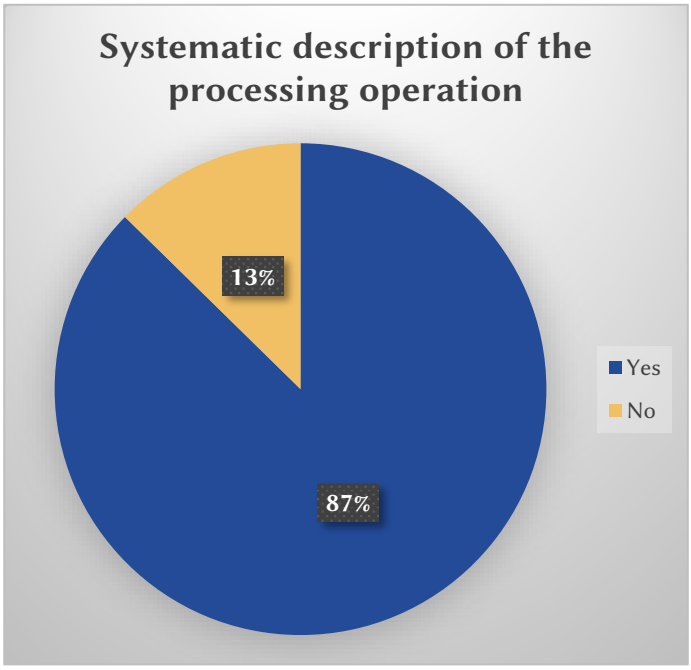
- And whilst **good templates do not necessarily guarantee good DPIA, bad templates invariably make for bad DPIAs**. In one example, a case of a switch from a medical paper files to an e-file system with external access based on consent, the template used relies mostly on mere box-ticking and Y/N replies and led to an examination limited to data security issues (see below section 8 on why this is not broad enough).

5. Description of processing

Article 39(7) EUDPR defines the minimum content ("shall contain at least") of a DPIA. Under Article 39(7)(a) EUDPR, this includes "a systematic description of the envisaged processing operations and the purposes of the processing".

As noted in the 2020 Survey (p. 27), "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."

5.1. Systematic description



From the total of 79 DPIAs examined (two submitted were actually only a threshold assessment), **less than 15% of the DPIAs failed to provide this minimum content**. This was partially due to a lack of ticking boxes, filling in free text fields or because preliminary statements had been inserted, but had not been replaced by definite assessments by the time the DPIA was "finalized".

Example: In one case, no actual description of the processing or the tool was provided, as the DPIA only referred to the purpose of the processing (whistleblowing - "a facility for external persons to report alleged breaches of Union law within the (EUI)'s competence to examine and act upon").

Figure 11: Percentage of DPIAs submitted to the EDPS' survey that included a systematic description of the processing operation

In other cases, the DPIA remained unclear on which (categories of) personal data will be processed.

Example: "Other Relevant Data: Any other data that is directly or indirectly related to the security inquiry and deemed necessary for its investigation and resolution."

Example: "...what is the nature of the data, and does it include special category or criminal offence data? Data have to do about a person's preferences e.g. in communication and team work...".

5.2. Data flow diagram

EDPS guidance Accountability on the ground Part II, p. 7: "The descriptive part of a DPIA starts from the information in the record, going into more detail and including a detailed data flow diagram."

As explained in the 2020 Survey (p. 27), a data flow diagram of the process (flowchart) illustrates "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".

In response to this exercise, we were provided with very few DPIAs containing detailed data flow diagrams. Of the very few provided, most seem to rely on data flow diagrams made available by their providers.

6. Assessment of necessity and proportionality

Article 39(7) EUDPR defines the minimum content ("shall contain at least") of a DPIA. Under Article 39(7)(b) EUDPR, this includes "an assessment of the necessity and proportionality of the processing operations in relation to the purposes".

EDPS guidance Accountability on the ground Part II, pp. 7/8: "...explain why you plan to do the processing. Be sure to explain that there is a real need for the processing in order to achieve the aims of the legal basis; the processing effectively addresses this need; and that the processing is the least intrusive alternative (from the perspective of fundamental rights) to achieve this aim (necessity). In addition, you must ensure that the advantages resulting from the processing should not be outweighed by the disadvantages that the processing causes with respect to fundamental rights (proportionality)."

From the total of 79 DPIAs examined, **fifteen DPIAs** (from nine EUIs, including one big EUI) **failed to provide this minimum content**.

The most frequent problem was that the examination was limited to arguing the processing operations *necessity*, thus without examining the *proportionality* of the processing operation *in relation to the purpose*.

Examples: In one case, regarding the use of a particular occupational health and safety *software*, the necessity assessment focussed on the EUI's need to have a medical service *per se*.

Example: One EUI merged the assessment of the necessity and proportionality of the processing operations in relation to the purposes with an assessment of the risks to the rights and freedoms of data subjects - in *under one page*.

Example: In one case, even guiding questions provided by the DPIA template used did not help: "Does the processing actually achieve your purpose? Is there another way to achieve the same outcome?" - "This is the only way to identify people's profile before the workshop, in order to attain the goals of the exercise". The goal of the exercise was teambuilding.

In other cases, the template used to conduct the DPIA led to shortcomings:

Example: The structure of the template used focusses primarily on data protection principles and information security issues - thus neglecting whether the processing is the least intrusive

alternative (from the **perspective of fundamental rights**) to achieve this aim (necessity) or, subsequently, proportionality aspects of the processing.

Example: On one case regarding the use of AI, the template used limits the assessment under the DPIA to lawfulness, the exercise of data subject rights, processor issues and transfer considerations, thus also not covering the broader necessity and proportionality of the processing operation in relation to the purpose.

7. Risk analysis: identifying and evaluating

Article 39(7) EUDPR defines the minimum content ("shall contain at least") of a DPIA. Under Article 39(7)(c) EUDPR, this includes "an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1".

EDPS guidance Accountability on the ground Part II, p. 8: "In a DPIA, you assess primarily risks to the rights and freedoms of data subjects. At the same time, you should analyse the compliance risks for your organisation. These are related, but not necessarily identical."

From the total of 79 DPIAs examined, **37 of the DPIAs fell short of providing such an assessment**. In one instance, this was missing altogether, as the template had not been filled in. In two other cases, this "risk assessment" took less than a page.

Example: One frequently used template does not allow for identification of risks in its second (DPIA) part, but moves directly to measures, which are understood to be information security risk management (ISRM) related ones: "MEASURES ENVISAGED TO ADDRESS THE RISKS: Describe security measures put in place for securing the processing operations on personal data and any data system used. Please describe also measure adopted by the processor, if you are using one. Please refer to particular parts of your contract with the processor or attach additional documents, if necessary". Whilst the same template's first part (threshold assessment) allows for risk identification, these identified risks then cannot be properly assessed in part 2, as there is no room to examine them.

7.1. Risk identification

As noted in the 2020 Survey (p. 28) with reference to Recital 46 EUDPR, "A DPIA should identify ...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."

EDPS guidance Accountability on the ground Part II, p. 8 (emphasis added): "The term 'rights and freedoms' of the persons affected refers in the **first place to the rights to privacy and data protection** (Articles 7 and 8 of the Charter), but also covers **related rights that may be impacted** as well – e.g. chilling effects on freedom of speech or freedom of assembly due to surveillance measures."

As noted in the 2020 Survey (p. 7), "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." (emphasis added).

In some cases, however, the structure of the DPIA template does not allow to integrate the result of the prior threshold assessment (see also below, section 8.1.3).

In an example involving profiling for a teambuilding event, the systematic layout of the template did not provide for any place to examine the risk of profiling identified in the threshold assessment triggering the DPIA. The threshold assessment had correctly noted that "During the workshop evaluation of individual characteristics and behaviour patterns will take place, which is considered as profiling. The workshop activities will allow individual's personality or behaviour to be determined. Consequentially, in some cases profiling can lead to inaccurate predictions, as well as, perpetuation of existing stereotypes". The subsequent DPIA only refers to the following: "The novelty of processing is based on profiling: a profile on the data subject will be elaborated by an automated means only, using an algorithm", but mentions no respective risk to the rights and freedoms of data subjects, i.e. the EUI's employees concerned.

In another example, a processing operation regarding biometric access control was identified as a risk triggering the need for a DPIA in the threshold assessment - but the DPIA then failed to take into account e.g. risk of identity theft given that this involves the reading of the data points from the fingerprint, face and palm.

In other cases, an assessment of several risks is done - but not of *risks to the rights and freedoms of data subjects*, as the **template used only refers to a different and limited set of risks**.

One example regards an engagement platform involving consent-based tracking, "aiming to reach people and raise awareness on the necessity to support the project of the European Union", i.e. data processing potentially revealing political opinions. The template used to conduct the respective DPIA limits the risks to be considered to data protection principles ("Assessment fundamental principles"), data subject rights ("Rights protection controls") and "Security controls". This in turn leads to a limited consideration of risks related to "Spoofing of an internal user (formerly named "Data subject / (EUI) user"); The data subject is not aware of which information is collected and why; Request for deletion of the account (formerly named "Contributions - manual deletion"); Deletion of personal data of external users; ...".

In another example, the DPIA notes that a "...risk assessment has been done for the confidentiality, integrity and availability domains...".

While there is a clear aspect of **information security risk management** (ISRM) in identifying the risks to the rights and freedoms of natural persons (not least since keeping data securely is one of the data protection principles), ISRM **is far from all there is to this exercise** (see EDPS guidance Accountability on the ground Part II, p. 9).

As already noted in the EDPS guidance Accountability on the ground Part II, p. 9: "Processes working exactly as planned may have impacts on data subjects (e.g. employee monitoring). These risks have to be assessed as well, not only the risks of 'things going wrong'"; "...a classical ISRM approach would likely not address these aspects. While there is a close link to ISRM, since you cannot have good data protection without good information security, the risks to consider here are more than the ones affecting the classic ISRM targets of confidentiality, integrity and availability."

7.2. Risk analysis / evaluation

EDPS guidance Accountability on the ground Part II, p. 8: "A 'risk' in this sense is a possible event that could cause harm or loss or affect the ability to achieve objectives. Risks have an impact – 'how bad would this be?' and a likelihood – 'how likely is this to happen?'."

Under Recital 47 EUDPR, "The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."

7.2.1. Number crunching

Often EUIs adopt a numerical system to evaluate risks. As noted in the 2020 Survey (p. 30): "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)."

Risk likelihood	**Risk severity**
1: Rare	*1. Very low*
2: Unlikely	*2. Low*
3: Possible	*3. Medium*
4. Likely	*4. High*
5. Almost certain	*5. Very high*

Figure 12: Example of numerical risk assessment

Many such DPIAs, however, do not give any clarifications on how they end up with a specific numerical score.

Domain area	Average inherent risk score	Average residual risk score
Third party governance	13.6	8.4

Figure 13: Example from one EUI, which strives to evaluate risks up to a decimal point

Example (in a case regarding AI and IP rights) under the heading "Assessment of the risk": "Severity of the impact ☐1☒2 ☐3 ☐4 Likelihood ☐1☐2 ☒3 ☐4; Assessment of the risk (severity x likelihood) = 6". No further explanation is provided.

Example (in a case regarding the use of an AI tool): "Risk 10: Reliability (source information) When AI technologies neglect the reliability of their sources, several risks emerge: • Misinformation Propagation: AI models learn from data, including unreliable sources. If these sources contain false or biased information, the AI may perpetuate inaccuracies. • Bias Amplification: AI can inadvertently amplify these biases, affecting decision-making and fairness. • Malicious actors can

manipulate AI by injecting false data. Without source reliability checks, AI systems become vulnerable to adversarial attacks. • Trust Erosion: People lose confidence in AI systems when they produce inaccurate or harmful results. • Using unreliable sources may violate privacy, copyright, or ethical norms with possibly creation of legal repercussions and reputational damage can follow. Prioritizing source reliability is crucial for building trustworthy and effective AI systems.
Assessment of the risk
Severity of the impact ☐1☒2 ☐3 ☐4
Likelihood ☐1☒2 ☐3 ☐4
Assessment of the risk (severity x likelihood) = 4"
No further information on this scoring in the light of the above risks is given.

Same example: "Risk 13: Hallucination/Misinfinformation/Disinformation AI-generated content, such as deepfakes, contributes to the spread of false information and the manipulation of public opinion. Efforts to detect and combat AI-generated misinformation are critical in preserving the integrity of information in the digital age. It has been highlight that AI systems are being used in the service of disinformation on the internet, giving them the potential to become a threat to democracy. From deepfake videos to online bots manipulating public discourse by feigning consensus and spreading fake news, there is the danger of AI systems undermining social trust. The technology can be co-opted by criminals, rogue states, ideological extremists, or simply special interest groups, to manipulate people for economic gain or political advantage.
Severity of the impact ☐1☐2 ☒3 ☐4
Likelihood ☐1☐2 ☒3 ☐4
Assessment of the risk (severity x likelihood) = 9
Again, no further information on this scoring in the light of the above risks is given.

This is regrettable, because transparency can be achieved, as illustrated by the following examples, which all **go beyond box-ticking and include reasoned attribution of numeric scores**:

Example: "The risk scores that are mapped for each of the above-mentioned processing activities represent the outcome of the risk assessment. Risk is the product of multiplication two numeric parameters: likelihood and impact (both scale 1 to 5). The descriptions provided in square brackets for Likelihood and Impact as well risk equation presented the consecutive tables are harmonized with (EUI) Risk Management Manual."

Example explaining connection between risk, measure and resulting risk score (numbering): "Scale from 0 to 5, 0 being not severe/likely at all and 5 being extremely severe/likely"... "Singling-out: (The) app only collects the following user information: age, gender, location and risk level. In "gross terms" the use of precise location data at mobile phone level could generate a potentially high risk (estimated at the level of 4) of singling out. The likelihood is however lower, estimated at the level of 2, because the singling out would require hacking into the user's phone. In the developed solution ("residual terms") the location data are collected every 30 minutes and deleted every day... The dataset uploaded to the database does not contain any element which would allow the association of the dataset with a concrete person... Moreover, the anonymised user data are aggregated in such a way that... This set of information does not reasonably allow to identify any individual and therefore the residual risk and likelihood are very low, estimated at the level of 0.5; ..."

7.2.2. Deficiencies in dealing with risks identified

Once a potential risk has been identified, it should be analysed and evaluated (qualified and quantified). Some DPIAs fail to demonstrate this process:

Example: In a case involving an exclusion database, whilst discrimination had been explicitly mentioned in the section entitled "description of the risk", the section on "fairness" does not actually analyse or evaluate the situation.

Example: In a case where the DPO had, as documented in the DPIA, identified a risk of "lack of legal basis" and disregard for the principle of purpose limitation, these risks identified were simply ignored by the controller in the respective sections of the DPIA.

In other cases, this failure to demonstrate that risks identified are actually examined, could be down to structural issues of the DPIA template used.

Example: In a case involving whistleblowing, the risk likelihood was simply not filled in and the risk severity was valued at "4" ("high") without further explanation:

"Where an unsubstantiated allegation is made against a data subject there is a risk that if this data remains on file, it could have a detrimental impact to the concerned data subject.	Mitigation measures already in place.
Risk likelihood: not filled in; Risk severity "4" ("high")"	

7.2.3. Linking risks identified in the threshold assessment to the DPIA

Although this would seem like a straightforward 'cut and paste' exercise, several DPIAs fall short of referring to **risks that had previously been identified in the threshold assessment**. This is somewhat surprising, especially as making that obvious link could be easily facilitated by a template nudging users to do so.

Some EUIs did not provide their threshold assessment and there was no reference in the DPIA submitted to a threshold assessment preceding the DPIA, which means that there was also **no documented link** between the risks identified in a possible threshold assessment and the risks subsequently examined in the DPIA.

Documented mismatch between risks identified in threshold assessment and the DPIA: For other EUIs, the threshold assessment was provided and it identified the relevant risks of a processing activity - but then, these risks were not mentioned or addressed in the DPIA.

Example: The threshold assessment notes that "Although (EUI) does not intend to use (tool) to monitor its employees (i.e., data subjects), the scale of processing is substantial, including IP addresses, device IDs, metadata and content which can take place all over the world (depending on how the system is configured). For these reasons, a decision was made to perform a DPIA". However, the subsequent DPIA does not refer to this risk.

Sometimes, this is the direct result of the DPIA template not giving room to refer to such risks or to address them with respective measures, e.g. by only focussing on aspects of information security risk management (see above, section 8.1.1).

However, as stated in the 2020 Survey (p. 30) and already referred to above (section 8.1.1), "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." (emphasis added).

8. Risk treatment: measures to address the risk

Article 39(7) EUDPR defines the minimum content ("shall contain at least") of a DPIA. Under Article 39(7)(d) EUDPR, this includes "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".

EDPS guidance Accountability on the ground Part II, p. 16: "Once you have established the risks, you have to choose appropriate mitigating measures (controls)"; "When selecting the controls/mitigating measures, compliance with the Regulation is the minimum standard you cannot go below".

In two cases, this section encompassed less than a page; in one instance, the DPIA only referred to "possible measures" without identifying any *actual* measures.

In one case regarding an exclusion database, the *purpose* of the measure (protecting the EU budget) was wrongly identified as a *mitigating measure*:

Example: "The registration of a natural person (falling under the scope of (an exclusion database), in line with Article 135(2)FR) in the (exclusion database) ... may be considered as a high risk for the natural person. However, the exclusion is a way to protect the Union's budget from unreliable persons who would have committed fraud, corruption, grave professional misconduct of other wrongdoings in line with Article 136(1)FR. ...
Assessment of the risk
Severity of the impact
☐1 ☐2 ☒3 ☐4
Likelihood
☐1 ☒2 ☐3 ☐4"

As is also the case in the above example, the **criteria to attribute values to severity, likelihood and impact** often remain unclear:

Example: In one case (involving the use of AI), although 24 risks had been identified, the risk assessment was never above "8" (without further explanation given).

Example: "MEASURES ENVISAGED TO ADDRESS THE RISKS" only invites the description of information security measures, followed by a somewhat apodictic attribution of "severity" and "impact" leading to score of "six" (notification EDPS only if higher than "eight").

It will be even more difficult to express the risk reduction achieved by envisaged measures referring to future (expected) safeguards:

Example regarding international transfers (for which the risk was identified as "*EU Data boundary*"): "... (a particular tool) will be added as a covered workload in the data residency commitments in (a provider's) Product Terms later in 2024. ... (A provider's) Advanced Data Residency (ADR) and Multi-Geo Capabilities offerings will include data residency commitments for (a particular tool) for (a provider's) customers later in 2024."

As in the above examples, templates often **focus on information security measures** for risk mitigation, which makes it difficult (and, as a result, unlikely) for controllers to deal with any risk that is not information security related (see above section 8 on why this is an inappropriately limited coverage for a DPIA).

When identifying mitigation measures, controllers need to **be wary of simply copying documentation provided by service providers** selected as service providers:

Example: In one case, the risk identified was the "Lack of accountability – the controller is unable to explain the functioning of the tool (e.g., its training and bias-prevention techniques)". The EUI suggested as safeguard inter alia "Reference to details from the documentation from (big IT provider)."

In addition, under Article 39(7)(d) EUDPR, controllers need to take into account the rights and legitimate interests of data subjects and other persons concerned, **not just safeguard the EUI against liability** resulting from infringing those individuals' rights.

The measures should actually target the risk, i.e. the **mitigation measure selected should match the risk identified** and this should be clearly documented.

Example where there is a mismatch: The EUI in question identified "Data processed on a large scale" as a risk (also in the DPIA), but then noted "The following measures will be implemented by the (EUI) to mitigate the identified risks: Joint Controllership Agreement between the (EUI) and (XXX) in order to regulate the respective roles and responsibilities in relation to the collection and transmission of ...IP addresses... Consent management form in order to collect ... users' consent to (XXX) analytics".

Example for the connection between the risk(s) identified and the measures taken is not documented: In a case involving remote testing, some mitigation measures seem to target a risk explicitly identified in the threshold assessment - but this connection between risk threshold assessment and the presumably respective mitigation measure in the DPIA is not clearly documented.

9. Sign-off

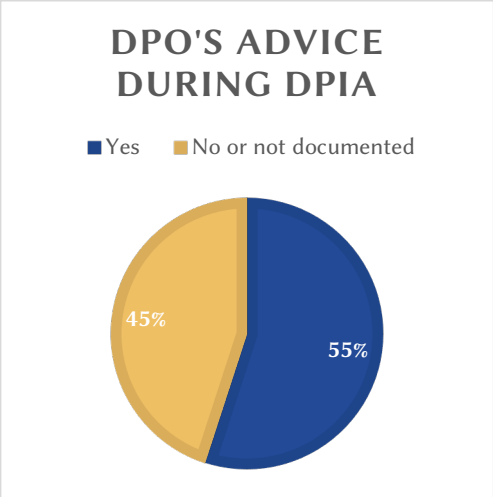
9.1. Advice from DPO during the DPIA

EDPS guidance Accountability on the ground Part II, p. 5: "**DPO can serve as a facilitator**, keeping in mind that responsibility and accountability finally lie on the controller's side – DPOs should help controllers to do their job, but should not do it for them... While carrying out the DPIA is your responsibility as business owner of the assessed process, your EUI's DPO can be of help throughout the process - if you need guidance at any stage during the process your EUI's DPO is your first contact point. Also consult your EUI's DPO on each step of the DPIA process."

From the total of 79 DPIAs examined, only a little more than half (45) contained some **documentation of input by the DPO** to the process.

Example: "The DPO agrees with the assessment of the data controller below".

For all others, any involvement of the DPO went undocumented. In two cases regarding the same EUI, the respective section was blackened out.



Example: One template (under the heading "DPO comments") asks the controller to explicitly document "What were DPO's comments and concerns? How did you integrate them (e.g. by adding additional risks in section 5 above)?"

In several cases, the field available in the DPIA template to document such involvement was simply left empty.

In one case, the opinion by the DPO was properly documented, but later "overruled" by the controller ("*advice overruled as not possible to implement due to time restrictions*").

Figure 14: Percentage of DPIAs which included the DPOs advice and/or consultation

On the other hand, several examples illustrate that the involvement of the DPO was fruitful - and this was also properly documented as part of the template.

Example: "On the basis of the analysis presented in the present document, any data protection concerns were effectively addressed. Additionally, the current privacy statement pertaining to recruitment has been fully updated in order to accurately inform data subjects of the modalities of the processing of their personal data."

Example: "The DPO would like to emphasize the need to update and sign without delay the SLA/MoU with (XXX) regarding (YYY) (with clearly defined responsibilities in DP matters). The DPO would like to be updated about this process and, where necessary, consulted on this matter."

Example: "The DPO was consulted for the impact assessment and her comments were taken on board for the finalization of the text."

In other cases, the involvement of the **DPO went well beyond the role of facilitator**:

Example: In one case, the assessment of safeguards, security measures and mechanisms to mitigate the risk or any reason leading to non-consultation of the EDPS was done by the DPO, on the basis of a template noting explicitly: "To be completed by the DPO or DPO representative".

Example: In another case, the assessment of safeguards, security measures and mechanisms to mitigate the risk or any reason leading to non-consultation of the EDPS was equally left to the DPO - but the not taken fully on board.

Example: In one case, the template used seems to be an amalgam of threshold assessment and DPIA and its explicitly states that "The assessment and recommendations fall in the scope of the DPO tasks as provided for in Article 45 of the EUDPR, and further defined in the ... implementing rules.". As a result, the examination conducted concludes that "The review was performed on the basis of the information provided by the delegated/controller for this processing operation and by the Processor within the scope of data privacy and shall not be considered as a data security assessment. The implementation of the actions and safeguards as recommended are responsibility of the controller."

9.2. Views of data subjects or their representatives

EDPS guidance Accountability on the ground Part II, p. 5: "Where appropriate, you also have to consult data subject representatives. Where the processing targets staff members in the EUIs this often means the Staff Committee. Where persons outside your EUI are affected, the controller may need to find solutions to obtain their views as well, where appropriate. This does not necessarily mean public consultation of all interested parties."

From the total of 79 DPIAs examined, only three DPIAs actually documented that data subject representatives had been consulted.

Example: The involvement of a "*Commission paritaire*" for a processing operation regarding **e-recruitment** / internal competitions.

However, no such consultation took place in many other cases that may have lend themselves by the nature of those concerned by the processing to such consultation. In two cases regarding the same EUI, the respective section was blackened out.

Example: In one case concerning **COVID access control** ("A temperature check performed on any person entering the EUI's buildings in the ... work places to deny access to anyone presenting a body temperature above 37,7° Celsius and; The presentation of a valid EU Digital COVID Certificate by everybody who intends to access the EUI's buildings.").

Another case where no such consultation took place, but may have been considered a good reflex concerns the **election of a Staff Committee**.

Example: In one case regarding teambuilding, for which the controller had argued that the processing was voluntary ("Each participant needs to agree with the terms & conditions in order to fill in his/her profile and has the right not to do so, in case he/she does not want to fulfil this activity.") and that "The staff has not expressed any concerns related to this activity", the DPO explicitly recommended "Consulting the Staff Committee to collect the views of the participants...

The activity is carried out in the work environment and data subjects may not feel comfortable or confident enough to truly express their concerns directly to their superiors." However, this was "overruled" by the controller as a next step ("advice overruled as not possible to implement due to time restrictions").

Example: In another case regarding whistleblowing, the template used explicitly referred to such consultation ("Will any stakeholders be consulted during the project or initiative? If so, how? If not, why not?), triggering the following explanation by the controller: "No. There is a legal framework already in place, which envisages whistleblowing arrangements of the present kind, in particular the (EUI) Regulation... This framework establishes the responsibilities of the (EUI) to operate whistleblowing arrangements in a manner that is consistent with the rights and freedoms of data subjects. While it leaves discretion to the (EUI) on the particularities of the external whistleblowing arrangements, this is not to an extent that would require external consultation."

9.3. Involvement other third parties

In some instances, the DPIA clearly stated that other third parties had been involved in drafting the DPIA.

Example: In one case, an EUI decided to get "assistance" from their provider of a particular tool: "In line with their obligation as processor under Article 29(3)(f) of the EUDPR, (XXX) has assisted the HR Family to ensure compliance with its obligation to carry out a DPIA under Article 39 of the EUDPR."

Example: Four EUIs outsourced the drafting of a DPIA to a consultancy / law firm.

As noted in the 2020 Survey (p. 12), it would seem safe to say that the involvement of external consultants is **not a silver bullet**. All best practice examples identified were *not* the result of outsourced DPIAs.

10. Check and review

EDPS guidance Accountability on the ground Part II, p. 18: "Review DPIA reports on a regular basis (suggested: every two years) and prepare for extraordinary reviews where needed."

There are several examples that EUIs regard **DPIAs as living documents**:

Example for the DPIA as a living document in the light of the evolution of risks: "During the revision of this version of the DPIA, we reassessed the risks as the platform had evolved. The changes to the answers of the ... template increased the overall risk assessment from Low to High."

Example of a DPO drawing the attention of the controller to the DPIA being a living document: "The DPIA is a living instrument that requires ongoing update. As a result, in the event the controller wishes to incorporate new functionalities to (a particular tool), those will need to be assessed from a data protection perspective to make sure any resulting risks for the data subjects are identified and mitigated."

Example : « ...compte tenu du dynamisme des scénarios du cloud, une DPIA a été préparée et sera mise à jour chaque fois que le scénario et les données traitées changeront pour mieux évaluer les nouveaux risques potentiels pour les personnes concernées... »

Example: In a case regarding storage limitation, the DPIA states: "pending update – the rules to enforce retention periods had to be changed for technical reasons. A provisional measure is now reflected in the current version of the Data Protection Record, and a definitive measure is being studied with the DPO. The DPIA will need to be adjusted afterwards".

Example: In a case regarding security inquiries, the respective DPO observation reads: "... ongoing monitoring and periodic reassessment of the implemented measures are recommended to ensure their continued effectiveness. Regular reviews will help address any emerging risks and maintain compliance with evolving data protection standards."

11. Consultation EDPS

11.1. Prior consultation of the EDPS

Under Article 40 EUDPR, the controller – after consulting the DPO – has to consult the EDPS under certain circumstances prior to the start of processing operations. The EDPS seems to have received fewer prior consultations on the basis of DPIAs under Article 40 EUDPR than would be expected considering how much the data processing landscape is changing, including the rising use of AI technologies and tools. This was one of the reasons for launching this exercise.

- In line with the EDPB DPIA Guidelines, **not all processing operations requiring DPIAs will also require such a prior consultation**. This is the case where, following a DPIA and the additional controls implemented, risks have been appropriately mitigated to an acceptable level and in cases where, following the DPIA, risks cannot be mitigated to an acceptable level, which leads the EUI to abandon the project.

- However, there will be cases in which there are **"high residual risks"** and improvements are necessary to mitigate these risks to an acceptable level. These cases are what prior consultations under **Article 40 EUDPR** are there for.

11.2. What we asked in the Survey...

EDPS guidance Accountability on the ground Part II, p. 22: "For particularly difficult cases, you proceed to prior consultation to the EDPS; when replying, the EDPS will give further guidance on how to ensure compliance with data protection rules. In keeping with the 'accountability' spirit of the Regulation, we do not expect that there will be many prior consultations..."

Whilst the EDPS was thus not expecting that "there will be many prior consultations", the EDPS was expecting at least some - and definitely more than the ones received.

Accordingly, we asked **how many times**, after conducting a DPIA and after seeking the advice of the DPO, the **controller decided *not* to consult the EDPS** under Article 40(1) EUDPR?

Several EUIs noted that they never consulted the EDPS under such circumstances, because risk mitigation always addressed risks to an acceptable level which did not require any EDPS consultation (which, according to one EUI, "appears to underline the usefulness of DPIAs as a means to mitigate risks to data subjects"):

- "The controllers have consistently ensured that adequate safeguards are in place to mitigate potential risks associated with processing operations. As a result, there hasn't been a necessity to consult the EDPS under Article 40(1) EUDPR after conducting DPIAs and seeking advice from the DPO."
- "Zero - In no case has the delegated controller concluded that the identified risks could not be mitigated."; "In the (EUI), the delegated controllers have always been able to identify and mitigate the risks as a consequence of which prior consultation of the EDPS was not legally required.
- "6 as the outcome of the DPIA has been that there is no high risk/risks are mitigated."

Under such circumstances, other EUIs referred to their choice to nonetheless informally consult the EDPS:

- "5 DPIAs have been conducted without a formal consultation under Article 40(1) EUDPR. However, the DPO Team proactively informed the EDPS and sought for informal advice by the EDPS e.g. on the DPIA on the System for the exchange of information relevant to the assessment of the fitness and propriety by the competent authorities (currently subject to a second round of informal consultation with the EDPS)."
- EUI: "2 out of 3 DPIAs (which – to date – have been completed and finalised by (EUI)). In relation to 1 DPIA, (EUI) has received from the EDPS an informal supervisory opinion under Article 57(1)(g) and (p) of Reg. 2018/1725."
- EUI (7 = total): "5 - decided not to consult; 2 - decided to consult informally".

Two EUIs refer to relying on DPIAs conducted by other EUIs as a reason for not separately consulting the EDPS:

- "(EUI) controller has not consulted the EDPS on its 3 DPIAs as they are based entirely on the assessment of the DPIAs of (another EUI) as service provider; the processing is used in the same technical configurations, based on the DPIA conducted by (another EUI's) services; the DPIAs are applied mutatis mutandis by the (EUI)."
- "The processing operation is similar to the one used by the (another EUI) and therefore (EUI) could take advantage of (another EUI) DPIA."

11.3. What we saw in the DPIAs...

In one case, the **DPIA did not document any conclusion** as to whether or not the EDPS should be consulted: "After carrying out the data protection impact assessment, the controller is of the opinion that the necessary use of the EUI of RFID technology for vehicle access management to EUI car parking facilities outweighs the minimal residual risks to the rights and freedoms of natural persons".

In other cases, the non-consultation of the EDPS might be due to **confusing instructions included in the EUIs' template** on the need to consult the EDPS.

Several examples illustrate that it can pay to consult the EDPS:

Example: In one case, a DPIA was revised after recommendations received from the EDPS and the second version of the DPIA corresponds to best practice examples.

Example: Another EUI noted that "...even in cases where the threshold was not formally met we have taken the advantage to reach out informally to EDPS staff for informal advice and are very grateful for that possibility, which helped establish the DPO function within the Agency."

11.4. Documented DPO advice on need for prior consultation

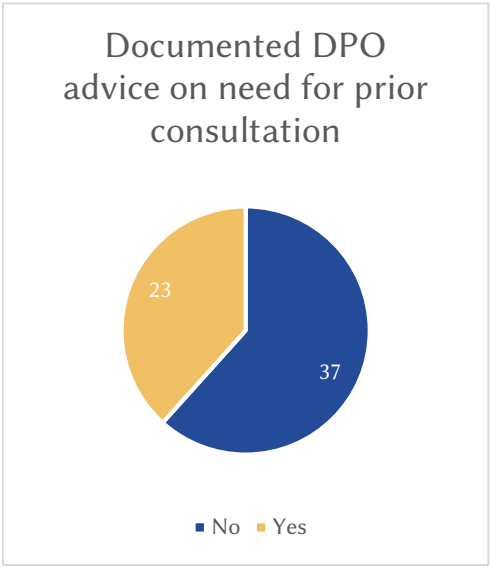
From the total of 79 DPIAs examined, the **involvement of the DPO** in advising on the need for a prior consultation of the EDPS **was documented in only 26 DPIAs**.

Example: In one case, the DPO advised on the need for prior consultation of the EDPS following two revisions of the DPIA.

Example: Under the heading of "The DPO recommends" the DPIA reads: "No prior consultation of the EDPS is needed. Reasons: The DPO would like to emphasize the need to update and sign without delay ... (with clearly defined responsibilities in DP matters). The DPO would like to be updated about this process and, where necessary, consulted on this matter."

Example: In another case, the DPO provided the following observation: "On the basis of the analysis presented in the present document, any data protection concerns were effectively addressed. Additionally, the current privacy statement pertaining to recruitment has been fully updated in order to accurately inform data subjects of the modalities of the processing of their personal data".

In one case, this section was blackened out. In another case, the section of the template was left empty. In the rest of the cases, no involvement by the DPO was documented.



Example: In one case regarding the use of an AI system, the DPO advised on the need for prior consultation, but the controller decided to "downgrade": "After carrying out the data protection impact assessment and after seeking advice of the Data Protection Officer, the controller is of the opinion that: ☒ Taking into account the safeguards, security measures and mechanisms to mitigate the risk, the processing of personal data does not represent a high risk to the rights and freedoms of natural persons and the processing of personal data will be carried out". The DPIA contains no further respective reasoning), although no less than 24 risks had been identified. The respective risk assessment - without explaining the numeric value - never exceeds "8" (whereas a consultation of the EDPS would have required "9").

Figure 15: Number of DPIAs that documented the DPO's advice on the need for an EDPS prior consultation under Article 40 EUDPR

12. Outlook

12.1. Artificial intelligence systems, including generative AI

When the use of AI systems, including generative AI, involves the processing of personal data, data protection rules, including the EUDPR, apply in full. The EDPS has published its Orientations on "generative Artificial Intelligence and personal data protection" to provide EUIs with practical advice and instructions on the processing of personal data when using generative AI systems, to facilitate their compliance with the requirements of the data protection legal framework.

Without appropriate safeguards, the use of AI, with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomy), presents significant risks to privacy and the protection of personal data.

All stages of an AI system life cycle should operate in accordance with EU data protection law. This means considering the unintended consequences of the use of AI systems and the need to follow a risk-based approach covering all the stages of the life cycle of the system. It also entails full transparency regarding the use of training data and its sources, on how algorithms are designed and implemented, what kind of biases might be present in the system and how are tackled possible impacts on individual's fundamental rights and freedoms. In this context, AI systems, in particular generative AI systems, must be transparent, explainable, consistent, auditable and accessible, as a way to ensure fair processing of personal data.

Against this background, **14 EUI replied to the affirmative** to our question whether **they carry out processing activities involving the use of AI systems**, including generative AI.

Example: In one case, an EUI replied that "It can currently not be excluded that Agency staff, beneficiaries, service providers etc. are using AI, including generative AI, by using either publicly

available AI (...) or (EUI) corporate tools which may including the use of AI, thus a further risk analysis for the protection of personal data may be required."

Example: Another EUI noted that its "services, in the absence of any specific definition of AI systems included in the survey, based their replies on the following definition of AI systems included in the draft AI Act. The (EUI) does not use AI systems to carry out processing of personal data. The (EUI) services are however considering using AI systems (...), which are likely to result in processing of personal data. For those cases, controllers are carrying out DPIAs prior to any potential deployment and use of such AI systems. The final advice of the DPO has not been provided yet."

At the same time, the same EUI noted that two of its services reported to the DPO that they were using AI systems - *but not for the processing of personal data*. In one instance, this regards an AI system for neural machine translation, which is an integral part of the translation process. The other instance is the IT department, which "engages in small-scale testing experiments aiming to understand the possibilities which AI may present". According to the EUI concerned, "These activities avoid any use of personal data and non-public information".

In one case, an EUI identified a particular **future AI use case**: "Some processing operations in scope can be supported by (a particular product) via semi-automated workflows, i.e. workflows where at least one gate requires an explicit human intervention. With the introduction of Generative AI (Artificial Intelligence) algorithms, (that product) can analyse historical data, patterns, and hence make some predictions. However, it will require the analysis of large amounts of data before proposing an option. This feature needs to be technically enabled and it will be only done at the request of the (EUI). Even in the case the purpose of the system in scope is to support processing activities that could entail profiling or assist in decision-making with a legal or similar effect on data subjects, the final decision will be taken by a human being, not an algorithm, in accordance with articles 24 and 33 of the EUDPR (see dedicated section below on IT security). (The product) is used for support, not decisions."

One EUI noted that it had issued own "guidance on third party Generative AI tools."

12.2. DPIA on the use of AI systems, including generative AI

The EUDPR requires that a DPIA has to be carried out when the personal data processing is likely to result in a high risk to fundamental rights and freedoms of natural persons, and always before the start of the processing. The EUDPR points out the importance of carrying out such analyses where new technologies are to be used or are a new kind in relation of which no assessment has been carried out before by the controller, such as in the case of generative AI systems. As a result of the assessment, appropriate technical and organizational measures must be taken to reduce the identified risks.

In that regard, the processing of personal data in generative AI systems presents particular risks stemming from systematic and large scale processing, in several cases without the awareness of the individuals affected, carried out in the context of processing activities linked to model training activities (e.g. personal data is obtained from publicly available sources in the Internet or collected from third parties). Personal data in this context is also obtained from the final users of the system, via the normal use of the system or through inference.

No less than **seven EUIs replied "Yes" to our question "Have you conducted a DPIA on your EUI's use of AI systems**, including generative AI, to address data protection risks?" That

corresponds to half of the 14 EUIs confirming that they carry out processing activities involving the use of AI systems, including generative AI.

One EUI clarified that "The determining element is not whether the processing operation includes "AI" but rather whether the processing operation (which may include AI) involves processing of personal data. If so, it will need to be assessed whether a DPIA is required or not" and gave a concrete example.

Another EUI informed that "The use of artificial intelligence, as a new technology, requires a DPIA if it generates a high risk for the data subjects. However, a high risk is not necessarily present in view of the envisaged use and other measures taken. The (EUI) has adopted guidelines on the use of artificial intelligence. Only approved tools should be used, such as (X) and (Y) (speech recognition, locally installed). While these tools could potentially (or accidentally) also process personal data, this is not their main purpose and there appears to be no high risk for the data subjects in view of the functioning and the use of these tools. No DPIA has therefore been made."

Another EUI noted that it had "developed a dedicated AI DPIA template based on guidance issued by the CNIL and the UK ICO (currently being tested)", that "the use of generative AI is at an experimental stage, (Z) was recently launched in production" and that it has "initiated the AI DPIA process for the DAP which includes (Z)."

Other EUIs expect the need to conduct a DPIA on the use of AI system for the future:

One EUI noted that: "In the next future, we could expect the need of DPIA on the use of AI systems, including generative AI."

For another EUI, "AI use is in piloting and testing phase" and a "DPIA on general use of AI is currently being developed."

Yet another EUI highlighted challenges in the context of draft legislation: "... as most EUIs, (EUI) is currently exploring AI tools and in this prospection and experimenting we try to address risks incl. those related to rights & freedoms of DS. Inter alia we created ad hoc 'Sandboxing' principles reflecting principles & rules of draft AI Act. But how can we do complete and integrated RA when AI legal framework is still in draft?"

Several EUIs request EDPS guidance on DPIAs related to AI:

One EUI noted that "EDPS guidance on DPIAs related to Artificial Intelligence would be welcome and very much appreciated"; another EUI believes that "Many DPIAs on generative AI will be needed in the future, it would be very useful to receive guidance from the EDPS".

One EUI highlighted the need for guidance on the articulation of the requirements related to data protection and the requirement of the AI Act: "As regards the questions related to Artificial intelligence, the delegated controllers expressed the need to receive urgent additional clarifications as to the articulation of the requirements related to data protection and the requirement of the AI Act. In particular the new AI Act will introduce specific risks assessments, which prima facie consider rather similar elements as under a DPIA. Going forward, the question of how the EU Data protection regime applies to AI should therefore not be looked at in isolation but taking a holistic view of the potentially overlapping assessments. A clear line also needs to be established to what extent, if any, the AI Act takes precedence of the data protection regime as *lex specialis* and *lex*

posterior. What is certain is that the AI act contains certain authoritative political choices by the legislator which need to be taken on board for DP purposes as well."

Another EUI noted that "...with the outcome of the upcoming AI Act, more guidance is needed on how DPIAs will evolve in view of the need to carry out other types of assessments, such as the Fundamental Rights Risk Assessment (FRA). Without becoming a burden for Data Controllers, principles of accountability and risk-based approach principles should be encouraged when performing this task. Therefore, finding the right balance between performing assessments and protecting fundamental rights of individuals should be struck."

For one example, several quotations might illustrate that taking promotional statements by certain AI providers at face value might distract from the intention pursued by conducting a DPIA:

- **The use of a particular AI tool as a lesser means?** "...the potential high risk due to the wide interest and usage of tools in public Internet already available by (EUI) Staff without guidance, offering (EUI) Staff a reliable and trustworthy AI, in a safer environment with safeguards and measures in place to ensure its security: (a particular product of a certain provider) (offers a lower risk choice)."

- **Consumer lock-in as "special relationship"?** "Secondly, and as part of the above-mentioned study on the most reliable AI tools available in the market, (a particular product of a certain provider) was considered as the first option due to the special relation between the (EUI) and (a particular provider), taking into consideration the existing Framework contract with specific contractual clauses covering the most important security issues, including personal data protection clauses and (a particular) License procured from them."

- **Ethics through the use of a particular provider?** "The (EUI), through (a particular provider), is committed to the advancement of AI driven by ethical principles, and in particular is committed to a lawful, secure, proportionate and clear use of personal data."

- The above then results in a risk assessment that reads as follows: "After carrying out the data protection impact assessment and after seeking advice of the Data Protection Officer, the controller is of the opinion that: ☒ Taking into account the safeguards, security measures and mechanisms to mitigate the risk, the processing of personal data **does not represent a high risk to the rights and freedoms of natural persons** and the processing of personal data will be carried out". No further reasoning is provided, **although no less than 24 risks had been identified**.

12.3. Other comments or suggestions as regards DPIAs

As expected and explicitly announced in our survey, due to the volume and complexity of the submissions, we could not provide detailed, individual feedback to respondents[10]. Instead, we focussed on conducting a comprehensive review to identify overarching patterns and notable exceptions. This approach allowed us to analyse effectively the collective data, ensuring that we capture significant trends and anomalies that emerge from the broader set of submissions.

[10] We also assured respondents that all information will be treated with the utmost confidentiality and will only be used internally, on a strict need-to-know basis.

However, we gave respondents the possibility to **share other comments or suggestions** as regards DPIAs with us via a free text field in the survey. **16 respondents used the opportunity** to do so.

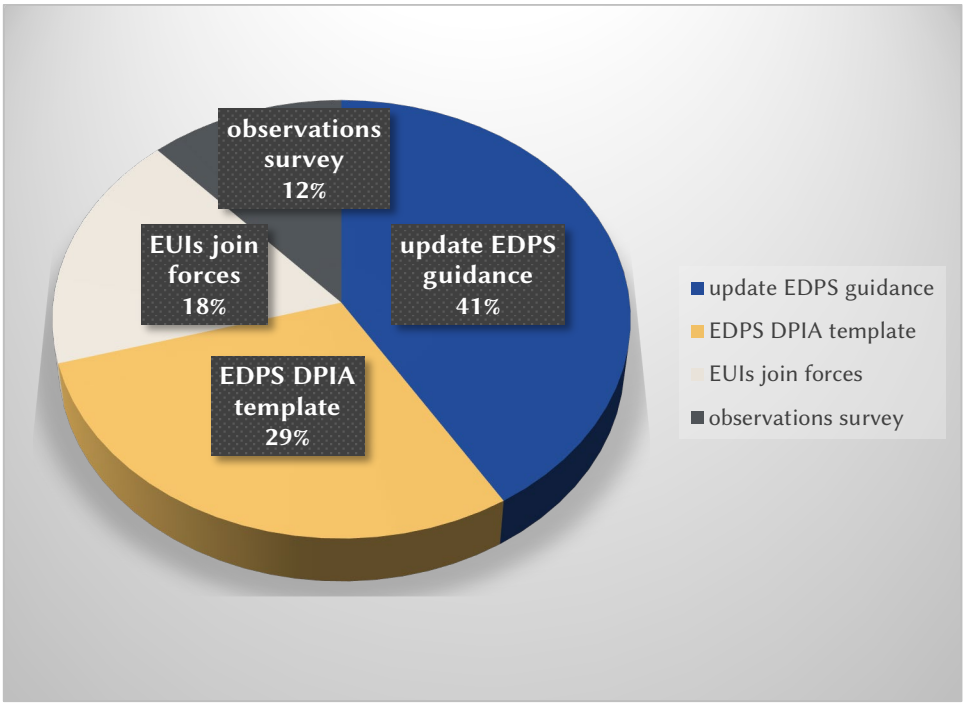


Figure 16: Suggestions as regards DPIAs from the EDPS' survey respondents

The main topics were:

- the need for updated EDPS guidance, either generally or regarding specific points (7 EUIs),
    - "some refresh of the guidance with training would be welcome";
    - "Please check if the Threshold Assessment Guidelines need to be updated. In general they are fine, but maybe it's time to check them."
    - "The threshold assessment would benefit from an update to become more relevant again."
    - "Considering to modify EDPS guidance on DPIA and to exclude cloud computing as a high risk."
    - "DPIAs need to include a part on international data transfers. There's also a requirement to carry out a TIA for international data transfers. We would appreciate guidance on how to ensure alignment of the two documents in cases where both DPIA and TIA are required..."
    - "...we consider that additional guidance on the conditions to apply article 3(3) of the EDPS decision on DPIA list ("If a controller decides not to carry out a DPIA, although more than one criterion in the template in Annex 1 is applicable, the controller shall document and justify that decision") would be useful to avoid duplication of the work."

- "EDPS should provide detailed guidance to the EUI Controllers and DPOs on DPIAs with the major contractors of the EUIs (...). EUI Controllers and DPOs should not be alone against large contractors. We don't have the knowledge and muscle to make an impact."

- the request for a standard EDPS template for DPIAs (5 EUIs),
  - "We would suggest that the EDPS create a standard officially approved DPIA form containing all of the necessary elements, to be used by every EUI"
  - "A simplified DPIA template would be very useful as it could facilitate the task of data controllers to draft DPIAs."
  - "From a guidance point of view, a template for DPIAs approved by the EDPS will be very helpful and could be part of the EDPS guidance package. Support on how to embed the Transfer Impact Assessment within the DPIA will also be appreciated."
  - "We would greatly appreciate if EDPS could create a DPIA template that the EUIs could use - that would ensure better quality of DPIAs and make the process more straightforward. We believe it would also significantly simplify the work of EDPS if EUIs would use a more coherent standard for DPIAs."
  - "...a common DPIA template among EUIs would be useful to share best practices and experience, especially in cases of shared services (e.g. of the European Commission)...."
- the suggestion for the DPO network or Agencies to join forces in the context of DPIAs (3 EUIs)
  - EUI: "In terms of suggestion: use the findings of the present survey as a starting point of a structured discussion among the EU Agencies ...) on how a tool for conducting DPIAs could be built (or if it already exists how it can be rolled-out for more (EUIs)."
  - "It would be useful if DPIA were shared within DPO network to identify similar projects and assure coherence."
  - "...the possibility for joint DPIAs (for similar data processing activities) could be further explored within the EDPS-DPOs network."
- observations on how the survey was conducted (2 EUIs):
  - "Be aware that some questions of this survey could be interpreted in different ways. Or they could conduct to opposite answers. Indeed, the limited marge of manoeuvre "Yes" and "No" is not enough to explain the real situation."
  - "Yes/No reply options to some of the Qs in this survey eliminate possibility for nuancing replies...".

13. EDPS conclusions

The EDPS analysed the replies given by the DPOs on the DPIA Survey 2024 and concluded as main findings that:

1. **The DPIAs' landscape has changed since the last EDPS DPIA Survey in 2020.** Now the **majority of the EUIs have performed a DPIA** (compared to the only 17 DPIAs that had been finalised in 2020). **31 EUIs** stated in response to the Survey that they have **never conducted a DPIA at all** or none covered by our request.
    - **EDPS Recommendation: the controller should perform a DPIA when the EUI's processing operation meets the criteria for one**, in accordance with Article 39 EUDPR and the EDPS guidance.
      In certain processing operations, as for example when processing personal data through generative Artificial Intelligence, there will be high risks to data subjects and your EUI will meet the criteria of 39(1) EUDPR to carry out a DPIA. When EUIs identify high risks in a processing operation, the next step is to perform a DPIA - and not to immediately apply mitigating measures to those risks with the aim of lowering them and avoiding a DPIA. It is thanks to the assessment in a DPIA that your EUI will know better which mitigating measures to apply.

2. Since 2018, EUIs carried out 242 DPIAs; during the same period, the EDPS received 3 prior consultations under Article 40 EUDPR.
    - **EDPS Recommendation: the controller should make a realistic assessment of the risks and how they are mitigated.**
      In the EDPS' view, some of the DPIAs carried out by EUIs and shared in this survey would have met the criteria for an EDPS prior consultation under Article 40(1) EUDPR. Considering the number of DPIAs conducted by EUIs and the number of prior consultations received by the EDPS in the past years, there is a concern that the assessment of the risks' mitigation from EUIs might be too optimistic.

3. 31 EUIs have performed less than 10 threshold assessments.
    - **EDPS Recommendation: the controller should conduct a threshold assessment when assessing whether a planned processing operation triggers the obligation to conduct a DPIA under Article 39 of Regulation (EU) 2018/1725 (EUDPR).**
      The EDPS has published an EDPS template (see EDPS guidance Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, section 4.3 and Annex 5) to facilitate this task. Threshold assessments that use a checklist with full text instructions will be easier to follow by the controller.

4. Sometimes EUIs identify the relevant risks of a processing activity in the threshold assessment - but then they fail to reflect these insights to the DPIA, e.g. the DPIA only focuses on security risks and does not reflect risks to data subjects.
    - **EDPS Recommendation: the controller should cover all potential high risks to data subjects rights and freedoms in the DPIA.**
      EUIs should not uncritically adopt the DPIAs of processors/third parties without ensuring its adaptation to their own circumstances, nor the completeness of processors/third parties' assessment. It does not suffice to replace the word "controller" with the EUI's name without further assessing the applicability of a DPIA to the actual EUI's reality.

5. 39 out of the 71 EUIs participating in this survey replied that they **rely on the EDPS template** when conducting their DPIAs

   - **EDPS Recommendation: the controller should use the EDPS DPIA template structure as a minimum standard.**
     As already said, a good template does not necessarily guarantee a good DPIA, but a bad DPIA template certainly contributes to a poor quality assessment. To avoid such a pitfall, the EDPS suggests that controllers use a methodology that is comprehensive and focused on data protection.
     As outlined in EDPS guidance (Accountability on the ground Part II, pp. 6/7), EUIs are free to use any compliant methodology and are not obliged to use the EDPS DPIA template structure provided in Annex 3. However, if the controller decides not to use that template it should have a better one in view.

6. From the total of 79 DPIAs examined (two submitted were actually only a threshold assessment), **13% of the DPIAs failed to provide a systematic description of the processing activities.**

   - **EDPS Recommendation: the controller should include a systematic description of the processing activities in the DPIA.**
     Article 39(7) EUDPR defines the minimum content of a DPIA and includes in point a) a systematic description of the envisaged processing operations and the purposes of the processing. This is a cornerstone part of a DPIA, since it provides the context and describes the processing operations: what you plan to do, how you plan to do it and why you are doing it.

7. The majority if the DPIAs examined did not include a detailed data flow diagram (flowchart).

   - **EDPS Recommendation: the controller should include a detailed data flow chart diagram in the DPIA.**
     This data flow chart diagram should illustrate which personal data is collected, from where/whom, what is done with it, where is it kept, for how long to whom is it given.
     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.

8. In 15 out of the 79 DPIAs examined in this survey, EUIs failed to demonstrate an assessment of the necessity and proportionality of the processing operations in relation to the purposes.

   - **EDPS Recommendation: the controller should include an assessment of the necessity and proportionality of the processing operations in relation to the purposes in the DPIA.**
     Article 39(7) EUDPR refers the minimum content of a DPIA and explicitly mentions in point b) this necessity and proportionality assessment. This information is relevant to assess compliance with the data minimisation principle (Article 4(1)(c) EUDPR) and the minimum requirements of a DPIA, in accordance with Article 39(7)(b) EUDPR.

9. The involvement of the DPO in the threshold assessment, in the elaboration of the DPIA and the elaboration of the decision whether to consult the EDPS is often not documented by the controller.

   - **EDPS Recommendation: the controller should showcase compliance and the DPO's work.**

The involvement of the DPO on DPIAs is of utmost importance, to guide the controller and raise awareness to the risks related to the intended processing operation. As part of the DPO tasks (Article 45 EUDPR) and the controller accountability obligations under Articles 4(2) and 39(2) EUDPR, it is necessary to ensure that DPOs are duly and timely involved, and that controllers are able to demonstrate such involvement. Consequently, the EDPS recommends that controllers document in writing their DPOs involvement when performing a DPIA.

10. Most EUIs adopt a numerical system to evaluate risks, some without clarifying how they end up with a specific score instead of another.

    - **EDPS Recommendation: the controller should use risk assessment tools to support risks evaluation.**
      As a starting point, there are several risk assessment tools available on the market that are useful for controllers to assess the risks to data subjects related with their intended processing operations. Some of those tools are free of charge and are provided by data protection authorities, such as the CNIL tool[11]. The EDPS encourages EUIs to use them when assessing the risks as a support. However, the EDPS is not saying that the tool alone will be sufficient to properly identify the risks.

11. EUIs using threshold assessments and DPIAs that use a checklist with full text instructions including guiding examples and counterexamples, provide a more comprehensive overview for the specific outcome. This is in particular the case, where the controller is forced to explicitly reason respective box-ticking.

    - **EDPS Recommendation: DPOs could share good practices and resources between themselves.**
      The EDPS noted that some EUIs have developed their DPIA methodology and have done a laudable work. Instead of reinventing the wheel, it seems more efficient to rely on the very good work put forward by some EUIs and to benefit from the DPOs network exchanges to share best practices and resources, such as a good DPIA template.

Furthermore, the **EDPS will update the guidelines on DPIA with practical advice, including a standard a DPIA template** to clarify certain misunderstandings and to provide more guidance to the controllers. According to this survey, there is no structural issue in recognising risks or interpreting them. Most DPOs confirmed that they in fact consult the EDPS guidance on DPIA, showing that it is a relevant document[12]. Nonetheless, the update of this guidance seems necessary, in light of the deficiencies in many instances to transfer the relevant risks of a processing activity identified by the controller in the threshold impact assessment to the DPIA report. This update also addresses a request voiced by some DPOs in the free text area of the survey.

In addition, the EDPS is assessing whether an update to the EDPS decision on Article 39(4) EUDPR is needed.

[11] For example, see the DPIA tool provided by the French Data Protection Authority (CNIL) in French and in English available at https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment
[12] See EDPS DPIA Survey 2024 report, p. 14.

Annex 1: Questionnaire

EDPS DPIA Survey 2024 - Questions

1. **The DPO of which EUI are you?**

2. **Threshold assessments**

When assessing whether a planned processing operations triggers the obligation to conduct a DPIA under Article 39 of Regulation (EU) 2018/1725 (EUDPR), the controller shall conduct a threshold assessment, by using the EDPS template
(see EDPS guidance (*Accountability on the ground* Part I: Records, Registers and when to do Data Protection Impact Assessments, section 4.3 and Annex 5).

How many such threshold assessments has your EUI conducted? insert number

3. **Data Protection Impact Assessments (DPIAs)**

Under Article 39(1) EUDPR, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

See EDPS guidance: Positive list of processing operations *prima facie* requiring such a DPIA under Article 39(4) EUDPR and negative list of processing operations *prima facie* not requiring a DPIA under Article 39(5) EUDPR (see EDPS Decision of 16 July 2019; the decision is also reproduced in Annex 5 to part 1 of *Accountability on the ground* toolkit). The EDPS *Accountability on the ground* toolkit also provides explanations on how to carry out a DPIA.

How many **DPIAs** under Article 39 EUDPR has your EUI conducted since the entry into force of the EUDPR? insert number

4. **Publication of DPIAs?**

Under Article 4(2) EUDPR, EUIs as controllers are accountable for being compliant, but also being able to demonstrate it - to all stakeholders, not just the EDPS. DPIAs under Article 39 EUDPR are an accountability tool to achieve this. According to EDPS guidance (*Accountability on the ground* Part II, section 3.9), the publication of DPIA reports is a good practice and EUIs should strive to at least publish a summary of the report (i.e. parts of the reports that should not be disclosed to the public, e.g. details on security measures, can be removed where appropriate).

Do you have a policy to **publish** DPIAs? Y/N

5. **Prior consultation of the EDPS**

Under Article 40 EUDPR, the controller – after consulting the DPO – has to consult the EDPS under certain circumstances prior to the start of processing operations. In line with the EDPB DPIA Guidelines, not all processing operations requiring DPIAs will also require such a prior consultation (where, following a DPIA and the additional controls implemented, risks have been appropriately mitigated to an acceptable level and cases where, following the DPIA, risks cannot

be mitigated to an acceptable level, which leads the EUI to abandon the project). However, there will be cases in which there are "high residual risks" and improvements are necessary to mitigate these risks to an acceptable level. These cases are what prior consultations under Article 40 EUDPR are for.

How many times after conducting a DPIA and after seeking the advice of the DPO did the controller decide *not* to consult the EDPS under Article 40(1) EUDPR? insert number

6. Written procedure for applying Article 39 EUDPR

Under Article 27 EUDPR, EUIs as controllers are under the obligation to organise their systems development processes in such a way that data protection considerations are taken into account at each step ('data protection by design'). As noted in EDPS guidance (Accountability on the ground Part II, section 3.1), by providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs under Article 39 EUDPR help organisations to comply with the requirement of 'data protection by design' where it is needed the most, i.e. for 'risky' processing operations. Some EUIs have developed written procedures to guide their structured thinking such as DPIA frameworks.

Did you establish a **written procedure** for applying Article 39 EUDPR? Y/N

7. DPIA template / model DPIA

Article 39(7) EUDPR defines the minimum content of a DPIA, but the EUDPR does not contain a standard methodology for doing DPIAs. However, any methodology used has to comply with the EUDPR's requirements. As outlined in EDPS guidance (*Accountability on the ground* Part II, section 3.1), EUIs are free to use any compliant methodology. For ease of reference, the EDPS provides an example for the generic principles for DPIA processes, including a template structure for a report in Annex 3 and refers to other existing methodologies in Annex 4, first part.

Are you using the EDPS **DPIA template / model DPIA** guiding your EUI in conducting the DPIA in the light of the elements listed in Article 39(7) EUDPR? Y/N

If not, are you using any other **DPIA template / model DPIA**? Y/N

8. Use of EDPS guidance documents

The EDPS has issued guidance for controllers and DPO in the EUIs on how to generate records for their processing operations, how to decide whether they need to carry out data protection impact assessments (DPIAs), how to do DPIAs and when to do prior consultations to the EDPS (Articles 31, 39 and 40 EUDPR). The current version was published in July 2019.

Does your EUI apply this **EDPS guidance** when conducting threshold assessments and DPIAs? Y/N

9. Artificial intelligence (AI) systems, including generative AI

When the use of AI systems, including generative AI, involves the processing of personal data, data protection rules, including the EUDPR, apply in full.

Without appropriate safeguards, the use of AI, with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomy) presents significant risks to privacy and the protection of personal data.

All stages of an AI system life cycle should operate in accordance with EU data protection law. This means considering the unintended consequences of the use of AI systems and the need to follow a risk-based approach covering all the stages of the life cycle of the system. It also entails full transparency regarding the use of training data and its sources, on how algorithms are designed and implemented, what kind of biases might be present in the system and how are tackled possible impacts on individual's fundamental rights and freedoms. In this context, AI systems, in particular generative AI systems, must be transparent, explainable, consistent, auditable and accessible, as a way to ensure fair processing of personal data.

Does your EUI carry out processing activities involving the use of artificial intelligence systems, including **generative artificial intelligence** (AI)? Y/N

10. DPIA on the use of AI systems, including generative AI

The EUDPR requires that a DPIA has to be carried out when the personal data processing is likely to result in a high risk to fundamental rights and freedoms of natural persons, and always before the start of the processing. The EUDPR points out the importance of carrying out such analyses where new technologies are to be used or are a new kind in relation of which no assessment has been carried out before by the controller, such as in the case of generative AI systems. As a result of the assessment, appropriate technical and organizational measures must be taken to reduce the identified risks.

In that regard, the processing of personal data in generative AI systems presents particular risks stemming from systematic and large scale processing, in several cases without the awareness of the individuals affected, carried out in the context of the processing activities linked to model training activities (e.g. personal data is obtained from publicly available sources in the Internet or collected from third parties). Personal data in this context is also obtained from the final users of the system, via the normal use of the system or through inference.

Have you conducted a **DPIA on your EUI's use of AI systems, including generative AI**, to address data protection risks? Y/N

11. Do you have any other comments or suggestions as regards DPIAs? free text box

Please be aware that due to the volume and complexity of the expected submissions, we will not provide detailed, individual feedback to you. Instead, our focus will be on conducting a comprehensive review to identify overarching patterns and notable exceptions. This approach allows us to effectively analyse the collective data, ensuring we capture significant trends and anomalies that emerge from the broader set of submissions.

We also assure you that all information will be treated with the utmost confidentiality and will only be used internally, on a strict need-to-know basis.