

# EDPS DPIA Survey 2024

## EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data  
protection authority

Manuel García Sánchez

HoS Consultation and Audits  
Supervision and  
Enforcement Unit



The background is a complex composition of geometric shapes and colors. It features a light gray background with a dark blue rectangle in the upper left containing a white circle. A large blue rectangle is positioned in the center, containing the text 'The trigger...'. To the right of this rectangle, there is a vertical strip of white space, followed by a large orange semi-circle. The right side of the image is filled with a pattern of binary code (0s and 1s) in a light gray color. The overall design is modern and abstract.

# The trigger...

# Why this survey?

Data Protection Impact Assessments (DPIAs) are an accountability tool meant to help EUs to ensure compliance with data protection principles in practice and to demonstrate such compliance to external stakeholders, including the EDPS as an advisory and supervisory authority.

**After four years, it was time to ask again, given:**

**DPIAs as an  
essential  
compliance  
tool**

**Few prior  
consultation  
s under  
Article 40(1)  
EUDPR**

**New  
processing  
activities /  
technologie  
s**



# Methodology



Two prong approach: targeted questionnaire and a request concerning the last two DPIAs (ten for EC, GSC and EP) 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

**72 EUIs  
consulted for  
a maximum  
of 168 DPIAs**

**79 DPIAs  
received  
and  
analysed**

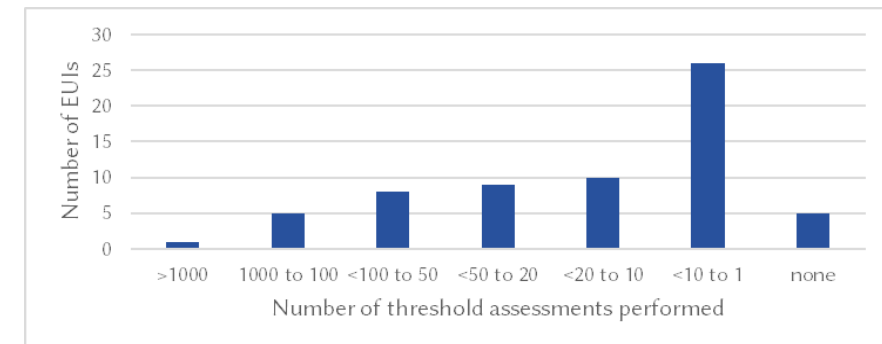
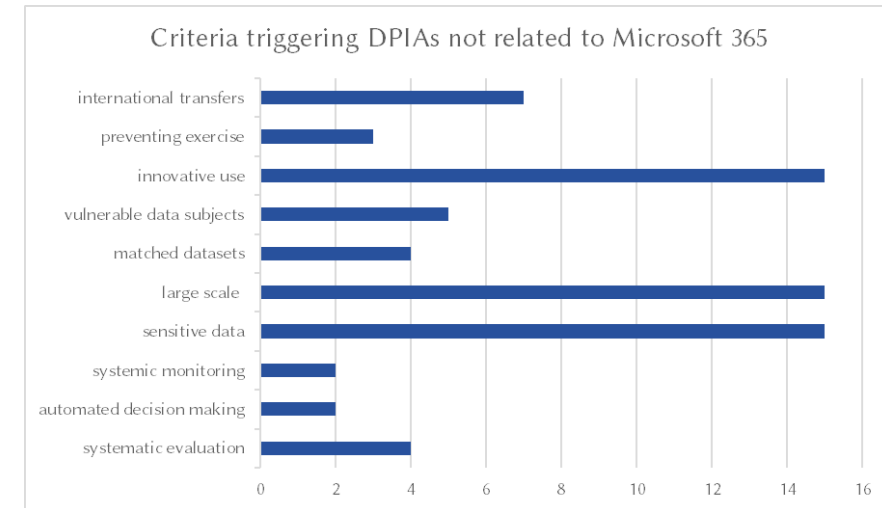
**31 EUIs  
have never  
carried out  
a DPIA**

The background features a light gray field with a blue rectangle in the top-left corner containing a white circle. A large yellow semi-circle is positioned in the upper-middle section. A dark blue rectangle, which serves as the text container, is located in the center-left. The right side of the image is filled with a pattern of faint, light gray binary code (0s and 1s).

# **What we asked... and what we saw in the DPIAs**

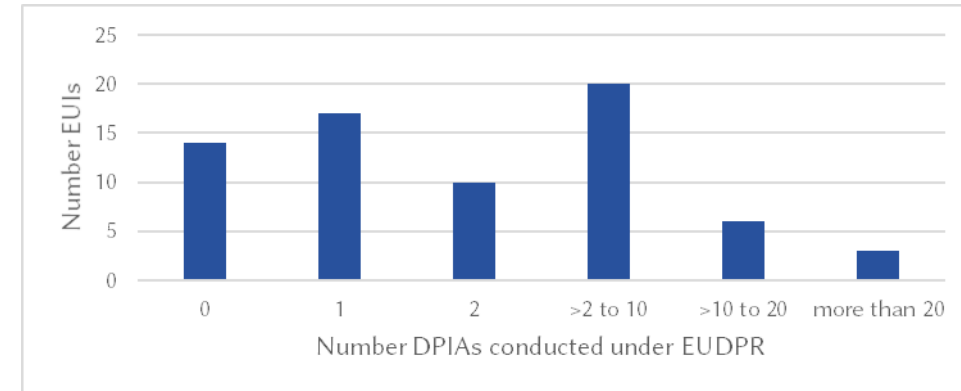
# Threshold assessment

- 31 EUIs have performed **less than 10** threshold assessments
- 12 EUIs state that **they routinely conduct a threshold assessment** for each processing they establish
- There seems **not to be structural issues** in recognising risks or interpreting them
- In many cases, the **involvement of the DPO was not documented**



# Conducting a DPIA

- **242 DPIAs have been conducted since 2018** (only 17 in 2020)
- Only **three EUIs have performed more than 20 DPIAs**
- In contrast, 41 EUIs have performed either none or only one DPIA
- Only **8 EUIs** indicated that they actually **have a policy to publish DPIAs**



*“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 even in a more privacy-friendly manner”*





# DPIA methodology / template



- 70 EUIs use the EDPS guidance for threshold assessments and DPIAs
- 31 EUIs have a written procedure to apply Article 39 EUDPR
- 39 EUIs rely on the EDPS template when conducting their DPIAs
- 32 EUIs either rely on a different template or use their own template, including the ones offered by COM, ICO and the CNIL
- Remarkable spread regarding the length, but lots of box-ticking and lack of joint DPIAs

When selecting the controls/mitigating measures, compliance with the Regulation is the minimum standard you cannot go below

While good templates do not necessarily guarantee good DPIAs, bad templates invariably make for bad DPIAs.



# Necessity and proportionality assessment

- 15 DPIAs (from nine EUIs) failed to provide the minimum content
- The most frequent problem was a **examination limited to necessity without assessing the proportionality of the processing operation in relation to the purpose**
- In other cases **the template used to conduct the DPIA led to shortcomings**

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 operation purposes

Be sure to explain that there is a real need for the processing in order to achieve the aims of the legal basis [...] and that the processing is the least intrusive alternative [...] 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)

## Risk analysis: identifying / assessing

- 37 of 79 DPIAs fell short of providing an **assessment to the rights and freedoms of data subjects**
- In some cases, the template does not allow to integrate the result of the threshold assessment
- In other cases, an assessment is done but not on the risks to the rights and freedoms of data subjects
- **Too much reliance on information security risk management**

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”.

As noted in the [2020 Survey](#), “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).



- Often EUIs adopt a numerical system to evaluate risks. Many times, however, **DPIAs do not clarify how they end up with a specific numerical score**
- Some **DPIAs do not include proper assessments**
- In other cases, **identified risks are simply ignored in the assessment**
- Several DPIAs **do not refer to the risks identified in the threshold assessment**

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 processes working exactly risk or a planned may have impact

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).

# Risk treatment

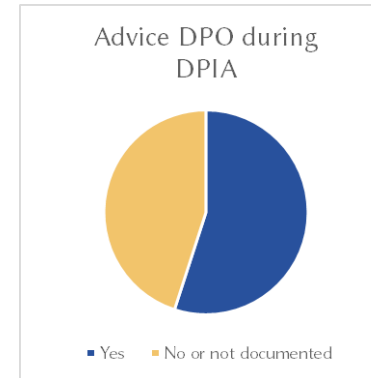
- In two cases, this section encompassed less than a page; in one instance, the DPIA referred to “possible measures” without identifying any actual measures.
- The criteria to attribute values to severity, likelihood and impact often remain unclear
- Templates make difficult for controllers to deal with risks that are not information security related
- When identifying measures, controllers should not simply copying documentation provided by service providers.
- The selected mitigation measures should match the identified risks

“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”

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.

## Sign-off

- Only 45 of 79 DPIAs contained some documentation of input by the DPO to the process
- While in several cases the involvement of the DPO was fruitful, in other was not considered or simply overruled
- Sometimes, the involvement of the DPO went well beyond the role of facilitator
- Only three DPIAs from 79 actually documented that data subject representatives have been consulted
- There are cases of reliance on service providers and outsourcing but all best practices identified were not the result of outsourced DPIAs.



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)?”

As noted in the [2020 Survey](#) , it would seem safe to say that the involvement of external consultants is **not a silver bullet**

# Prior consultation of the EDPS

- Several EUIs have noted that they have never consulted the EDPS under Article 40(1) EUDPR, because risk mitigation always addressed risks to an acceptable level
- Others decided to informally consult the EDPS
- Two EUIs referred to relying on DPIAs conducted by other EUIs as a reason for not separately consult the EDPS
- The involvement of the DPO in advising on the need for a prior consultation was documented in only 26 DPIAs

“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.

# EDPS Conclusions



## (Preliminary) conclusions

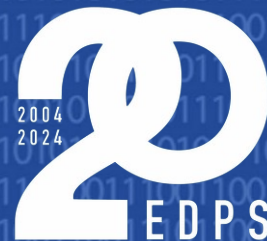
- **the DPIAs' landscape has changed since the last EDPS DPIA Survey in 2020** and now the **majority of the EUIs have performed a DPIA** (compared to the only 17 DPIAs that had been finalised in 2020), even if **31 EUIs** stated in response to the Survey that they have **never conducted a DPIA at all** or none covered by our request;
- Sometimes EUIs identify the relevant risks of a processing activity in the threshold assessment - but then they fail to transfer these insights to the DPIA, which is often due to deficiencies in the DPIA template used;
- The involvement of the DPO in the threshold assessment, the DPIA and the decision whether to consult the EDPS is often not documented;
- Most EUIs adopt a numerical system to evaluate risks, some without clarifying how they end up with a specific score instead of another;
- Threshold assessments and DPIAs that use a checklist with full text instructions (rather than Excel sheets) including guiding examples and counterexamples, fare best. This is in particular the case, where the controller is forced to explicitly reason respective ~~bo~~icking.



# Some (initial) recommendations



- User proper, available risk assessment tools
- Ensuring some training on risk assessment methodologies
- Share good practices and resources among DPOs
- Showcase compliance and the DPO's work



# EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data  
protection authority

