Samen aanjagen van vernieuwing

EDPB DPIA Template consultation

SURF Vendor Compliance response

Authors: Sophia Gelpke, Daisy Brugman, Valerija Kornilova
Version: 1.0
Date: 9 June 2026

Table of contents

1 Introduction SURF

To give the reader an idea of the perspective from which this response to the DPIA Template ('the Template') consultation has been written, this document provides a short introduction of the organisation SURF and the role of SURF Vendor Compliance in performing DPIAs.

SURF
SURF is the Dutch IT cooperative of education and research. It is owned by its members, comprised mostly of educational institutions and research institutions. Through SURF, they work together to, amongst other, procure the best possible digital services and develop and share knowledge with each other. Part of SURF's services is that the Vendor Compliance team conducts DPIAs on IT services that a lot of members use.

Reference DPIAs versus individual DPIAs
In GDPR terms, SURF is not the data controller for the processing of personal data via the use of the services it performs its DPIAs on. Each individual educational or research institution that uses these services is the data controller. However, as the Dutch IT cooperative, SURF takes the responsibility to assess general data protection risks for end users of these services and to ensure the data processing complies with the GDPR. Therefore, SURF conducts reference DPIAs to assist its members to select a privacy-compliant deployment, and conduct their own DPIAs where necessary. The Dutch DPA has endorsed this approach to improve the protection of personal data within the education sector. This reference DPIA is meant to help educational and research organisations with the DPIA they must conduct when they deploy certain services, but it cannot replace the specific risk assessments the organisations must make themselves.

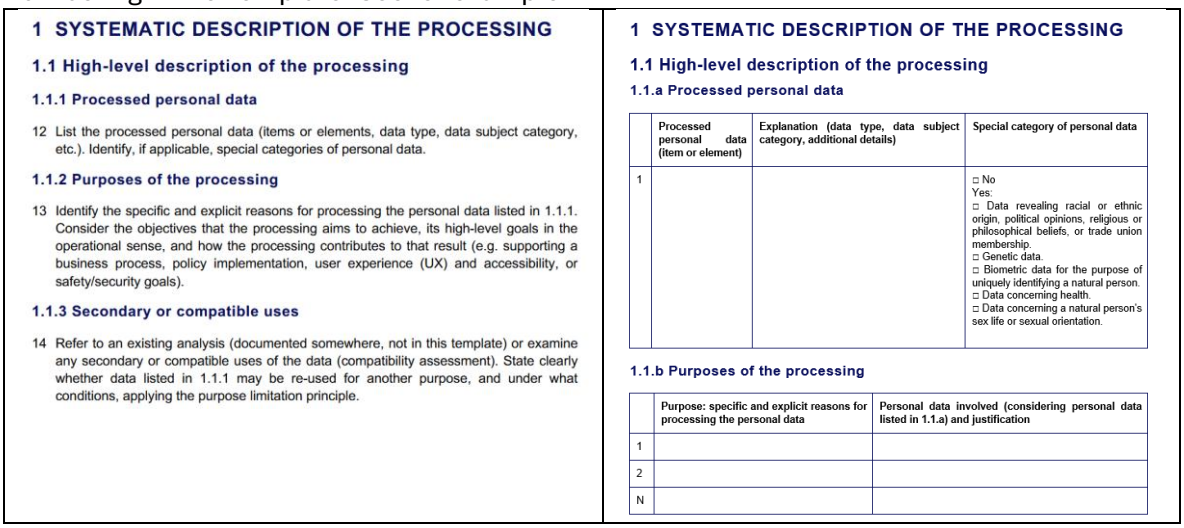
SURF chooses which services to assess based on an inventarisation of requests from its members. These can be new services that the education sector wants to use, as well as services that are widely in use in the sector.

Performing one reference DPIA on an IT service has benefits for SURF's members, as well as for the vendors of the products SURF assesses. For the members, it saves the cost of each of them having to do an entire DPIA individually. They are also able to incorporate their combined knowledge about a product and experiences with a vendor in the reference DPIA. Additionally, SURF can more effectively negotiate mitigating measures with the vendors, because it has the combined negotiating power of the entire sector as a representative. For the vendors, it saves time, effort and money as well to not have to assist every institution individually with DPIAs that will likely be very similar. It's also more efficient for them to be able to implement measures that benefit all members at once.

2 Review of the DPIA Template

2.1 Explainer

- A minor thing, but the numbering in the Explainer doesn't always correspond to the numbering in the Template. See for example:



1 SYSTEMATIC DESCRIPTION OF THE PROCESSING

1.1 High-level description of the processing

1.1.1 Processed personal data

12 List the processed personal data (items or elements, data type, data subject category, etc.). Identify, if applicable, special categories of personal data.

1.1.2 Purposes of the processing

13 Identify the specific and explicit reasons for processing the personal data listed in 1.1.1. Consider the objectives that the processing aims to achieve, its high-level goals in the operational sense, and how the processing contributes to that result (e.g. supporting a business process, policy implementation, user experience (UX) and accessibility, or safety/security goals).

1.1.3 Secondary or compatible uses

14 Refer to an existing analysis (documented somewhere, not in this template) or examine any secondary or compatible uses of the data (compatibility assessment). State clearly whether data listed in 1.1.1 may be re-used for another purpose, and under what conditions, applying the purpose limitation principle.

1 SYSTEMATIC DESCRIPTION OF THE PROCESSING

1.1 High-level description of the processing

1.1.a Processed personal data

	Processed personal data (item or element)	Explanation (data type, data subject category, additional details)	Special category of personal data
1			□ No Yes: □ Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. □ Genetic data. □ Biometric data for the purpose of uniquely identifying a natural person. □ Data concerning health. □ Data concerning a natural person's sex life or sexual orientation.

1.1.b Purposes of the processing

	Purpose: specific and explicit reasons for processing the personal data	Personal data involved (considering personal data listed in 1.1.a) and justification
1		
2		
N		

- The Explainer doesn't offer much additional information that doesn't become clear from the Template itself. Additional value could be added to the Explainer by:
  - Referring to sources where definitions and explanations from the EDPB can be found.
  - Providing examples, for example for the measures supporting compliance.
  - Giving guidance on how to complete questions.
  - Anticipating questions that might come up often in certain sections and answering those.
- Under 1.1.4 Nature, scope and context of the processing, it says: "international transfers are transfers of personal data to a third country or an international organisation (an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries)." This definition does not seem to correspond to the EDPB's three criteria: "a controller or a processor is subject to the GDPR for the given processing; this controller or processor discloses by transmission or otherwise makes personal data available to another organisation (data controller or processor); this other organisation is in a country outside EEA or is an international organisation."[1] A transmission of personal data to a third country does not necessarily mean a transfer to an organisation in a country outside the EEA.

2.2 General

- The word 'justification' is used a lot, but since this a very broad term not explained in the Explainer and since it's also not a GDPR term, it's not clear what is meant by

[1] International data transfers, https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en, visited on 8 June 2026.

this. For example, in the context of the question “Is personal data going to be transferred to a recipient in a third country or international organisation?”, is the justification referring to the applicable transfer mechanisms? It’s better for clarity to use the specific terms for the information the Template is asking for, or provide an explanation of what is meant by justification.

2.3 Missing elements

- Adding an executive summary with the main findings and conclusions would be beneficial for readers.

2.4 Notes by number

0.5 DPIA technical sheet
Under “Reasons to conduct the DPIA”, there is an option missing for existing processing activities for which a DPIA is overdue, because it has never been conducted or it hasn’t been updated recently enough. Realistically, this situation exists for many organisations.

1.1.d Nature, scope and context of the processing
The third row of the table in this section seems to be the only place to record transfers and justifications. It would be better to have more structured way, like a separate table to record the transfers, instead of having to put them all in one cell together with details about cross-border processing.

1.4 Compliance with approved codes of conduct
Other than this section, there doesn’t seem to be a place to record the applicable laws and regulations that apply to the processing, which can be useful to assess the lawfulness of the processing.

3.3 Assess the proportionality of the processing
This is an example of a section that would benefit from more guidance. Even though SURF realises the question of proportionality is very broad and hard to define by nature, some structuring or a summary of the EDPS toolkit would be useful.

4.1.a Impacts on the rights and freedoms of the data subjects caused by non-default, accidental, unlawful, or abnormal events
While non-default, accidental, unlawful, or abnormal events can pose a threat to data subject’s rights, it would make more sense to record these types of threats in a security assessment. Article 35 refers specifically to the risks resulting from certain types of processing, not from risks resulting from unintended events. Therefore, an explanation of the EDPB’s decision to incorporate this in the DPIA Template and how this fits into the provisions in article 35 would be fitting.

4.1.b Method
It’s understandable that the EDPB doesn’t want to restrict the Template to only one method of assessing and managing risk. However, some additional guidance is desirable here, since the risk assessment is a part of DPIAs that many organisations struggle with. This even might be some basic guidance on risk assessment and management in general. Some ideas:

- If the EDPB wants to use the term method, a definition of what is meant by method is needed (tools, models, frameworks, templates, etc.?)
- A referral to the Risk Assessment Tools of NIST: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/privacy-risk-assessment/tools.
- An overview of some of the most common risk models and risk frameworks and the type of scenarios for which they might be useful.
- Some sources of parties who provide concrete guidance on how to determine likelihood and impact, like the CNIL: https://www.datapolicy.it/wp-content/uploads/2021/05/2012-CNIL-ManagingPrivacyRisks-Methodology.pdf

5.2 Views of data subjects or their representatives
It's better to put this before the DPO advice (5.1), so the DPO can take these views into account.

7 CONCLUSION AND DECISION
It would be good to either add a space here for the name and job title of the decision maker(s), or to refer back to 0.1 for this.

2.5 On a positive note

SURF likes the tables provided in 3.3 Measures supporting compliance, to be able to record the measures supporting compliance in a structured way.