Memo Pure instead of DPIA Pure

SURF Vendor Compliance (SVC) is experienced in conducting in-depth risk assessments on Data Privacy and Security (a.k.a. DPIA's). These DPIA's require a lot of time, resources and money. Before SVC starts any assessment, SVC takes the time to evaluate the request for these assessments to ensure that our actions are aligned with the right motives. After consulting with member institutions, SVC has decided to publish a memo instead of a DPIA for the Pure application from Elsevier. This memo will present our findings and recommended measures for institutions. This decision enables us to deploy resources more effectively for doing assessments on other applications with higher risk profiles.

What is Pure by Elsevier?

In short, Pure is a workflow management system for administering publications and other research output from your own institution. Some institutions also use it as a repository, but its core function is workflow management. The system helps to establish links between authors (researchers), documents (publications) and institutions (author affiliations).

For a better understanding on how Pure is used within the institutions and to define any privacy sensitivities, SVC has been in contact with the PUG (Pure User Group). This is a group of key-users and administrators with extensive Pure experience. Through a dedicated meeting and subsequent email correspondence with several administrators, SVC gathered detailed user experiences and feedback. A few institutions have also shared their pre-DPIAs. Based on this information, combined with our own analysis of Pure, SVC has conducted an independent pre-DPIA.

Conclusions from our pre-DPIA

Conducting a DPIA is mandatory where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.[1] The Dutch Data Protection Authority has published a list of seventeen types of processing for which a DPIA is always mandatory in the Netherlands.[2] If a processing is not included in this list, an organisation must itself assess whether the data processing is likely to present a high risk.[3] The European Data Protection Board have also published a list of nine criteria.[4] As a rule of thumb if a data processing meets two of these criteria a DPIA is required. [5]

SVC can conclude that from the EDPB list, only number 7 applies:

[1] Article 35(1) GDPR.

[2] Article 35(4) GDPR; Government Gazette, Nr.64418/ 27 November 2019.

[3] Dutch Data Protection Authority, 'Data protection impact assessment (DPIA)', autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia, accessed on 2 April 2026.

[4] European Data Protection Board, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', ec.europa.eu/newsroom/article29/items/611236, accessed on 2 April 2026.

[5] Dutch Data Protection Authority, 'Data protection impact assessment (DPIA)', autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia, accessed on 2 April 2026.

- *Number 7 – Data concerning vulnerable data subjects*: Employees (researcher and support staff) data will be processed in Pure. There is a power imbalance between employers and employees.

It should be noted that this analysis is limited to the processing activities necessary for the workflow management and repository in Pure. On that basis, it can be concluded that the personal data provided by institutions and subsequently processed in Pure does not qualify as special categories of personal data within the meaning of Article 9 GDPR. The processing is limited to name, email address, position, and institutional affiliation, which are required for the use of Pure. Furthermore, no non-public personal data relating to researchers is made available on any publication platform.

Based on the currently available information, the processing does not appear likely to result in a high risk within the meaning of Article 35 GDPR. Consequently, a DPIA is not considered mandatory. For this reason, SVC has decided to draft a memo outlining several recommended measures.[6]

Recommended measures for institutions

It is recommended that institutions take the following four measures, if these are not yet in place:

1) **Establish a read-only integration in the institution's HR administration**
   Institutions must ensure personal data is accurate and, where necessary, kept up to date.[7] This means institutions should carefully consider how they configure Pure. Preferably, a read-only integration should be established with the institution's HR administration within the central ERP system, so that up-to-date information automatically flows into Pure.

2) **Limit personal data processing**
   Institutions must ensure compliance with the principles of purpose limitation and data minimisation, meaning that only personal data that is strictly necessary for the specified purpose is processed.[8] In the context of Pure, processing should be limited to what is necessary for the workflow management and repository. The personal data for researchers and support staff should be limited to name, email address, position, and institutional affiliation.

   If researchers wish, they can add extra personal details in Pure. Employees can also amend the personal details they have entered themselves. Please inform and train staff on this matter.

   Following the first recommendation to integrate HR systems with Pure, institutions should limit data sharing exclusively to personnel whose personal data must be processed by the application. What is often observed is that data

[6] SVC would like to emphasize that SVC is open to conducting a full DPIA in place of this memo if there is widely supported community support. Additionally, if the nature of the processing changes, SVC will certainly re-evaluate and return 'Pure' to the SURF Vendor Compliance calendar.

[7] Article 5 (d) GDPR.

[8] Article 5(1)(b) and (c) GDPR.

is shared in advance, just in case they end up using an application. So Pure should not have access to all HR data, but only to the data (from the HR system) of researchers who publish via Pure and support staff.

3) **Restrict data retention**
Institutions must ensure that personal data are not retained for longer than necessary for the purposes for which they are processed, in accordance with the storage limitation principle.[9] Within Pure, personal profiles and user accounts remain after an individual has left the institution. Upon termination of employment, all personal data that are not related to publications should be deleted. Any other remaining data must be limited to what is necessary for workflow management and repository purposes. Furthermore, institutions must ensure that data subjects (both current and former employees) are able to effectively exercise their rights, including the right of access and the right to erasure.[10]

4) **Inform the data subjects**
Institutions must provide data subjects with clear and accessible information regarding the processing of their personal data, in accordance with the transparency requirements of the GDPR.[11] This information should be provided through a privacy notice and must specify, among other things, which personal data are processed, for which purposes, and how data subjects can exercise their rights, and for how long their personal data is retained.

Responsibility remains with the institutions

Notwithstanding the above, it should be emphasized that the institutions remain independently responsible as controllers within the meaning of Article 4(7) GDPR for the processing of personal data in Pure. As such, they are required to independently assess and ensure the lawfulness and compliance of their specific processing activities. In particular, this entails that institutions must critically assess how Pure is implemented and used within their own organization.

Similar to a reference DPIA, it does not replace a case-by-case assessment. Depending on the specific manner in which Pure is configured and used, additional institution-specific risks may arise, which may require further analysis and the implementation of supplementary mitigating measures.

Contact

Do you have any questions about this memo or our services? Please contact us at vendorcompliance@surf.nl.

[9] Article 5 (e) GDPR.

[10] Articles 12-23 GDPR.

[11] Article 5 (a) GDPR.