Embracing technology
Embracing ambition

Agoria is the **Belgian National Trade Association** for the sector of **technology**, including manufacturing and digital companies, and represents more than 2200 companies and over 321000 employees.

Agoria welcomes the EDPB's initiative to develop a common template for Data Protection Impact Assessments. A more consistent approach to DPIAs can be valuable for controllers, processors, data protection officers, and supervisory authorities. It may help organisations to structure their assessment, document accountability and identify relevant risks for the rights and freedoms of data subjects in a more transparent manner.

At the same time, we would invite the EDPB to further improve the practical usability and proportionality of the template. In its current form, the template appears to be primarily suitable for organisations that already have substantial legal, privacy, technical and risk assessment expertise. For many organisations, and in particular for SMEs or companies without a mature privacy function, several sections may be difficult to complete without significant external support. This may reduce the practical value of the template and may lead either to formalistic completion or to disproportionate documentation efforts.

1. **The template should provide more practical guidance for non-expert users.**
   The accompanying explainer provides a useful starting point. However, it remains rather limited. We suggest that the final version include, or be accompanied by, concrete examples, sample answers, practical prompts, "good practice" illustrations and warnings against common mistakes.

   A DPIA template should not only indicate what information is expected, but also help users understand how to answer the questions in a meaningful, risk-based and proportionate way. This is particularly important for sections dealing with necessity, proportionality, data quality, risk identification and mitigation measures.

   It could be useful to provide a completed DPIA for a specific processing activity (e.g. monitoring of employees via CCTV) in order to understand what the level of detail should be.

2. **The template should more clearly reflect a scalable and proportionate approach.**
   Not every DPIA requires the same level of detail. The level of documentation should depend on the nature, scope, context, purposes and actual risk profile of the processing. We therefore recommend introducing a clearer layered structure: a baseline level of information that should normally be completed in all cases, supplemented by more detailed questions where the processing is complex, high-risk, innovative, large-scale, involves vulnerable data subjects or requires more extensive technical or organisational analysis (e.g. use of artificial intelligence for the processing of personal data).

3. **The template should avoid unnecessary overlap with other GDPR documentation.**
   Some parts of the template may overlap with the record of processing activities, Article 28 GDPR processor documentation, security documentation, transfer impact assessments, internal risk registers or architectural documentation. We suggest that the EDPB expressly clarify that cross-referencing to existing documentation is acceptable where it provides the necessary information. This would support accountability without requiring organisations to duplicate information in several documents.

4. **Information on processors and sub-processors should remain risk-relevant and proportionate.**
   The template should not be understood as requiring an exhaustive operational catalogue of all sub-processors or a duplication of contractual information already addressed under Article 28 GDPR. The DPIA should identify processors and sub-processors where their involvement is relevant to the assessment of risks to data subjects, for example because of the nature of the service, access to more sensitive data, international transfers, security dependencies or criticality for the processing. Where detailed processor or sub-processor information is already maintained in contractual documentation or vendor management records, reference to those documents should be sufficient.

5. **The scope section should focus on the processing operation assessed in the DPIA.**
   It may be useful to explain what is included and excluded from the assessment, but the template should not lead to a broad inventory of features, configurations, integrations or deployment choices that are outside the relevant processing operation and do not materially affect the DPIA. The final template should clarify that exclusions only need to be documented where they are relevant to understanding the scope, assumptions or risk assessment.

6. **Technical architecture and supporting assets should be described at an appropriate level of abstraction.**
   We agree that it is important to understand the relevant systems, data flows and dependencies.

   However, the DPIA should not become a detailed technical inventory of hardware, network components, software modules, infrastructure layers or security-sensitive architecture. Excessive detail may create confidentiality and security concerns and may not be necessary for the assessment under Article 35 GDPR. The template should therefore encourage a functional and risk-based description of the relevant architecture, with detailed technical inventories kept in separate documentation where appropriate.

7. **Data quality requirements should be contextual.**
   Data quality is clearly relevant, especially where inaccurate data may affect individuals or where automated processing, profiling or AI systems are involved.

   However, formal metrics, thresholds or quantified requirements are not meaningful for every type of processing or every data element. The template should focus on measures to ensure accuracy rather than requiring prescriptive metrics, thresholds or quantified justifications for each data item without clear added value. If the present approach is kept, more guidance on a Q&A basis is recommended.

8. **Publication or external sharing of the DPIA should remain discretionary.**
   DPIAs may contain confidential information on controls, infrastructure, risks, mitigation strategies, contractual arrangements, security measures and operational dependencies.

   While transparency towards data subjects and stakeholders is important, the template should expressly recognise that organisations may publish summaries or partial versions and may withhold confidential or security-sensitive information.

In conclusion, Agoria supports the EDPB's objective of promoting a consistent DPIA approach across the EU. To achieve that objective in practice, the final template should be more accessible, scalable and clearly risk-based. It should help organisations conduct better DPIAs, without turning the DPIA into a duplicative, overly technical or disproportionate documentation exercise.