BSA SUBMISSION ON THE EDPB'S DRAFT DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

Response to the Public Consultation

May 2026

The Business Software Alliance (www.bsa.org) welcomes the opportunity to provide input on the European Data Protection Board's (EDPB) voluntary Data Protection Impact Assessment Template.

BSA is the global trade association of the enterprise software industry, representing companies[1] that are leaders in artificial intelligence, cybersecurity, cloud computing, quantum, and other breakthrough technologies. We work in over 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation.

BSA welcomes the EDPB's initiative to develop a voluntary Data Protection Impact Assessment (DPIA) template. A common EU-level reference tool has strong potential to improve consistency, reduce fragmentation across Member States, and support controllers in meeting their obligations under Article 35 GDPR.

At the same time, given the likelihood that this template may be operationalized by national data protection authorities (DPAs), it is essential that the template remains flexible, risk-based, and practical to implement across a wide range of different processing activities and organizational structures. The voluntary template should support compliance without introducing new legal obligations beyond the GDPR.

We offer the following recommendations:

- Preserve flexibility and avoid a "one-size-fits-all" approach
- Reinforce the risk-based purpose of DPIAs
- Provide clearer guidance on when and how often DPIAs are required
- Ensure proportionality and avoid disproportionate requirements
- Promote harmonization and interoperability across frameworks

[1] BSA's members include: Adobe, Akamai, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

1. Preserve flexibility and avoid a "one-size-fits-all" approach

While the template is described as voluntary, its anticipated adoption by DPAs as a common or "meta-template" may transform it from a voluntary tool to an expected standard. This creates a risk it may be interpreted overly rigid in practice. Controllers should not be required to follow the template structure in every circumstance, and alternative formats achieving equivalent outcomes should be accepted.

At the same time, the template provides limited operational guidance on how key GDPR principles should be assessed and weighed in practice. Combined with its level of detail, this may encourage a formalistic, "check-the-box" approach to compliance rather than meaningful risk assessment.

BSA recommends that the EDPB:

- Emphasize that the template is a voluntary supporting tool, not a mandatory format, and that alternative approaches achieving equivalent outcomes will continue to be accepted;
- Clarify that controllers may adapt the structure, format, and level of detail to reflect their specific processing activities and internal compliance systems;
- Provide practical examples or explanatory guidance on how to carry out key assessments; and
- Avoid overly prescriptive instructions that may not be adaptable across organizations.

2. Reinforce the risk-based purpose of DPIAs

The primary objective of a DPIA is to assess risks to individuals' rights and freedoms and to identify appropriate mitigation measures. However, the current template appears to place significant emphasis on the format of a DPIA rather than its substance, including requiring significant descriptive and operational detail. As a result, controllers may interpret the template as treating all sections as equally important.

BSA recommends that the EDPB:

- Emphasize that risk identification, assessment, and mitigation are the core components of a DPIA;
- Clarify that not all sections require the same level of detail, and that effort should be proportionate to their relevance to risk;
- Provide guidance on prioritization, in particular ensuring that sections addressing risks to fundamental rights are given appropriate weight; and
- Consider developing a more flexible or simplified approach (e.g., a "DPIA light" or baseline privacy impact assessment) for lower-risk processing, allowing controllers to document key elements of processing in support of privacy by design and by default, even where a full DPIA is not required. This would further support the goals of DPIAs in protecting fundamental rights, even in situations where the GDPR does not require a DPIA.
- Clarify Section 0.5 that the template should not require controllers to document processing activities, features, configurations, integrations, or deployment choices that fall outside the scope of the DPIA, nor justify why such elements are excluded, as this risks creating unnecessary inventories without added value for assessing risks to individuals and is not required under the GDPR.

Otherwise, an overly broad and insufficiently prioritized template could divert effort away from assessing and mitigating risks to individuals toward largely descriptive documentation.

3. Provide clearer guidance on when and how often a DPIA is required

The template provides limited clarity on how controllers should determine whether a DPIA is required. In particular, the section outlining the "reasons to conduct the DPIA" combines different legal bases and risk indicators without clearly distinguishing applicable thresholds, and may be interpreted as suggesting that a DPIA is required where a single WP29 criterion applies. This differs from the 2017 WP29 Guidelines, which indicate that two or more criteria should generally be met.

More broadly, the lack of harmonized guidance across the EU on when DPIAs are required continues to create legal uncertainty for controllers, as national DPA lists and practices diverge.

In addition, while the template includes some references to updates over time, it provides limited clarity on how frequently DPIAs should be conducted or updated and does not clearly indicate when a DPIA should be revisited or reviewed.

Finally, the template should not create an expectation that DPIAs will routinely be published or shared externally beyond circumstances required under applicable law. (Section 0.5)

BSA recommends that the EDPB:

- Clarify the threshold for when a DPIA is required, including alignment with existing WP29 guidance;
- Promote greater harmonization across the EU, including through the development of a common approach to determining when DPIAs are required;
- Provide guidance on when DPIAs should be reviewed and updated, in particular in response to substantial material changes in the processing or associated risks, while ensuring that any such guidance remain proportionate and aligned with industry practice;
- Support broader policy efforts, such as the proposed **Digital Omnibus amendments** to Article 35 GDPR, to establish a single EU-wide list of processing activities that do or do not require a DPIA, alongside a common methodology, as an important step toward improving legal certainty.
- Clarify that the template does not imply that publication or external sharing of DPIAs is generally expected beyond disclosures required under applicable law, as DPIAs may contain sensitive and confidential information relating to security controls, infrastructure, system architecture, contractual arrangements, operational dependencies, risk assumptions, and mitigation measures.

4. Ensure proportionality and avoid disproportionate requirements

Several elements of the template risk introducing disproportionate levels of detail and documentation that go beyond the requirements set out in Article 35 GDPR.

In particular, the template provisions relating to the means of processing (Section 1.3) call for highly granular descriptions of assets—including hardware, infrastructure, network components, and software—often grouped by technical layer or function. This level of detail appears overly prescriptive, especially where it is

not necessary to assess risks to individuals. Moreover, these descriptions may change regularly over time, as controllers adopt new hardware and infrastructure based on market conditions and other factors that do not create new risks to data subjects. As a result, the template risks seeking detailed information that may be quickly outdated, rather than more general descriptions of the processing that may continue to be applicable even as specific vendors change.

The data quality section (Section 2.2.b) requires the definition of metrics or thresholds, which appears to exceed the requirements of Article 35 GDPR. The GDPR focuses on ensuring data accuracy, rather than quantifying it, and the introduction of such metrics risks creating unnecessary quasi-quantitative obligations. These descriptions, too, risk becoming so detailed that they become outdated over time rather than creating a durable description that continues to underpin the controller's assessment of relevant risks.

In addition, the necessity and proportionality assessment (Sections 3.2 and 3.3) requires controllers to demonstrate that the same objective could not be achieved through "less intrusive means." In practice, this entails documenting and justifying rejected alternatives, rather than focusing on the assessment of the chosen processing, and goes beyond common practice under the GDPR.

Finally, the template should not require exhaustive identification of processors and sub-processors or documentation of contractual arrangements already addressed under Article 28 GDPR, as this may create duplicative and unnecessary compliance obligations. (Section 0.2)

BSA recommends that the EDPB:

- Ensure that the template reflects a proportionate, risk-based approach, allowing the level of detail to vary depending on the risks of the processing and ensure that the descriptions are at a sufficient level of detail that they remain valid over time;
- Clarify that the template should not require metrics or thresholds where not necessary, and that data quality should focus on how accuracy is ensured; and
- Clarify that the template does not require documenting all alternatives or demonstrating that no "less intrusive means" exist in all cases, and does not introduce additional obligations beyond Article 35 GDPR.
- Clarify that information relating to processors and sub-processors should be limited to what is relevant for assessing risks to individuals and should not require exhaustive or duplicative documentation of arrangements already governed by Article 28 GDPR.

5. Promote harmonization and interoperability across frameworks

BSA supports the development of an EU-wide voluntary DPIA template as a step toward greater consistency. However, the current draft does not in itself resolve fragmentation in the implementation of DPIAs across jurisdictions and frameworks.

DPIAs increasingly play a role across multiple regulatory regimes, including as a basis for Fundamental Rights Impact Assessments (FRIAs) under the EU AI Act, as well as under a growing number of global privacy and

data protection laws. This creates a need for greater interoperability and alignment, to avoid duplication and unnecessary administrative burden for controllers.

In particular, where controllers conduct DPIAs or similar assessments under other legal frameworks, they should be able to build on those existing processes by supplementing them with any additional elements under GDPR, rather than being required to conduct entirely separate assessments using a different format.

BSA recommends that the EDPB:

- Support broader policy initiatives, including the proposed Digital Omnibus amendments to Article 35 GDPR;
- Ensure that the voluntary template supports interoperability with other EU and global frameworks, including the EU AI Act; and
- Clarify that controllers may build on existing DPIAs or similar assessments conducted under other laws, including in other jurisdictions, by supplementing them where necessary to meet EU requirements, rather than duplicating processes.

Conclusion

BSA supports the EDPB's objective of enhancing consistency and compliance through a common and voluntary DPIA template. To achieve this effectively, the template should remain flexible, risk-based, and interoperable, while avoiding unnecessary complexity and administrative burden.

Ensuring that the voluntary template supports meaningful risk assessment in practice—rather than a prescriptive or formalistic approach—will be key to its success and uptake across the EU.

For further information, please contact Irma Gudžiūnaitė,

Director, Policy – EMEA, at irmag@bsa.org.