Studio Associato Servizi Professionali Integrati
www.wstlegal.eu

To: European Data Protection Board (EDPB) – Rue Wiertz 60, B-1047 Brussels – via public consultation

Date: Milan, 8 June 2026.

Subject: contribution to the public consultation on the Template [2026] for Data Protection Impact Assessment (DPIA), version 1.0, adopted by the EDPB on 10 March 2026.

Dear Members of the Board,

The GDPR Club, a round table forum now in its sixth edition and dedicated to ongoing dialogue between Data Protection Officers, Privacy Officers and Legal and Compliance Managers from leading Italian and International companies on the most significant issues relating to personal data protection, hereby submits its contribution to the public consultation launched by the Board on 14 April 2026, with deadline on 9 June 2026, on the *Template [2026] for Data Protection Impact Assessment ('DPIA')*, version 1.0, adopted on 10 March 2026 (hereinafter, the **"Template"**), and on its accompanying *EDPB DPIA Template Explainer* (hereinafter, the **"Explainer"**), both published on the official consultation page (https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en).

The contribution has been prepared by the **GDPR Club**, coordinated by the Data Protection &New Tech Department of Studio Associato Servizi Professionali Integrati – **WST Law & Tax Firm**.

1. Methodological premise

The following observations aim to strengthen the operational usability of the Template, the verifiability of the controller's assessments and the documentability of the underlying decision-making process.

We support the flexible approach of the Template, which accommodates different organisational, sectoral and technological contexts. We respectfully suggest, however, that such flexibility should be accompanied by more granular criteria, examples and fields in those sections requiring qualitative assessments, in order to reduce the risk of arbitrary, non-comparable or hardly defensible entries vis-à-vis supervisory authorities.

2. General observations

2.1 Description of the processing

Section 1 of the Template adopts a primarily tabular structure from the outset. While ensuring order and readability, this approach may encourage schematic and fragmented entries that fail to capture the overall logic of the processing, particularly where the processing is complex, involves multiple parties or relies on articulated technological architectures.

We suggest preceding the tables with a narrative section in which the controller sets out the purposes, context, parties involved, categories of data subjects and of data, flows, technologies, assets, transfers and retention. The tables would then serve to verify, detail and document what has already been described.

2.2 Criteria for discretionary assessments

Several sections of the Template (see sections 2.3, 3 and 4) require assessments of appropriateness, effectiveness, likelihood, severity, modulating factors and risk acceptability. The Explainer acknowledges the controller's methodological freedom and allows reference to consolidated external methods, but this approach leaves controllers

without a structured internal methodology (notably SMEs, to which the *EDPB Data Protection Guide for Small Businesses* referenced in Annex 1 of the Template is itself addressed) without operational guidance.

We suggest supplementing the Explainer with non-binding examples of scales, criteria, evaluation grids and acceptability thresholds, without prejudice to the controller's freedom to adopt internal methodologies or recognised standards (by way of example, ISO/IEC 29134:2017; the methodologies published by the French CNIL and by the Spanish AEPD, also referenced in Annex 1), provided they are applied in a documented and verifiable manner.

2.3 Logical sequence between sections

The Template provides cross-references but does not make sufficiently explicit how the information contained in one section should feed into subsequent assessments, with the risk of independent compilation of the sections and consequent loss of overall logical consistency.

We suggest clarifying in the Explainer (possibly through a non-binding flow chart) the following sequence, starting from the description of the processing (sec. 1):

i. lawfulness, minimisation and data quality (sec. 2);
ii. necessity and proportionality (sec. 3);
iii. structural risks (3.1) and non-default events (4.1.a);
iv. inherent risk (4.1.c);
v. additional mitigation measures (4.2.a);
vi. residual risk (4.2.b);
vii. action plan (4.2.c).

3. Specific observations

3.1 Data quality (section 2.2.b)

Section 2.2.2 requires the controller to provide "*data quality metrics, requirements or thresholds*" without clarifying what is meant by data quality in the DPIA context. The concept is relevant, first and foremost, to the accuracy principle under Article 5(1)(d) GDPR and shapes the assessment of risks to data subjects, particularly in processing involving automated decisions, profiling or assessments of a medical, economic or behavioural nature.

We respectfully ask the Board to clarify (i) what is meant by data quality in this context, (ii) whether the assessment should consider accuracy, completeness, currency, consistency, relevance to the purpose, source, traceability and rectifiability, and (iii) whether metrics and thresholds should be defined per data category, per purpose or per level of risk to the data subject.

We also suggest clarifying in the Explainer that the data quality assessment should be carried out *ex ante* with respect to the start of the processing, consistently with the *data protection by design* logic under Article 25 GDPR.

3.2 Appropriateness and effectiveness of measures (sections 2.3.a–2.3.e)

Sections 2.3.a through 2.3.e all require the controller to "*discuss [the measures'] appropriateness and effectiveness*" without clarifying the relevant benchmark. The implementation-status column allows the controller to document whether a measure is planned, partially implemented or implemented, but does not substitute for a qualitative judgment on the measures themselves.

We suggest clarifying in the Explainer the following operational distinction: (i) **appropriateness** as the suitability of the measure with respect to the GDPR requirement or to the risk to be addressed; (ii) **effectiveness** as the capacity of the measure, once implemented, to produce the intended result and to be verifiable through evidence.

3.3 Consent and withdrawal (section 2.3.c)

Section 2.3.c dedicates a single row to the requirements for consent and its withdrawal, structured along the same three columns provided for the other measures. This structure does not, in itself, allow verification of whether consent was validly collected, whether it is traceable, or whether consistency is ensured with consents collected through other channels or systems.

We suggest providing a dedicated module on consent management, to be completed whenever consent is the legal basis for the processing, including at a minimum: (i) the purposes for which consent is sought; (ii) any granularity of consents across distinct purposes; (iii) collection channels (web, paper-based, call centre, app, etc.); (iv) system for recording the proof and date of consent; (v) withdrawal mechanisms available to the data subject; (vi) alignment across channels and systems; (vii) frequency of periodic compliance checks.

3.4 Security of the processing under Article 32 GDPR (section 2.3.e)

Section 2.3.e requires the controller to list security measures without clarifying the perimeter of the measures to be indicated or their relationship with the risk assessment. Some controllers may therefore limit themselves to referencing the measures listed in Article 32(1) GDPR only, while others may include the organisation's entire security system, without distinguishing between general measures and measures specific to the processing under DPIA.

We suggest a dedicated section, scoped to the tools used and the personal data affected by the processing under DPIA, structured at a minimum into: (i) physical security; (ii) logical security of IT systems and measures relating to personal data; (iii) organisational measures. For each category, the controller should indicate whether the measure is implemented, partially implemented, planned/not implemented or not applicable (with reasons).

This clarification appears necessary insofar as Article 32 GDPR does not impose a closed list of measures but requires the adoption of measures appropriate to the risk: paragraph 1 of the same article provides qualified but non-exhaustive references to the measures that may be documented in the DPIA.

3.5 Threats from non-default, accidental, unlawful or anomalous events (section 4.1.a)

Section 4.1.a requires the identification of threats arising from malfunctions, deviations from design and default values, as well as threats to the confidentiality, integrity and availability of the data. The Template does not clarify, however, whether for the identification of such threats the controller may rely on taxonomies or methodologies based on international standards, security frameworks or documented internal methodologies.

We also suggest strengthening the link between section 4.1.a and Article 32(2) GDPR, which requires the controller to take into account, in assessing the appropriate level of security, the risks presented by the processing and arising, in particular, from destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, whether accidental or unlawful.

We suggest clarifying in section 4.1.a that the controller should classify risk scenarios at least by reference to the categories listed in Article 32(2) GDPR, on the understanding that such categories may constitute the minimum baseline for integration with taxonomies derived from international standards, security frameworks or documented internal methodologies (by way of example, ENISA catalogues, the ISO/IEC 27000 family and the MITRE ATT&CK Framework).

3.6 Risk assessment method (section 4.1.b)

Section 4.1.b requires the controller to set out the method followed to assess and manage risk, including likelihood and severity levels, metrics, prioritisation criteria and acceptability thresholds. The Explainer allows reference to consolidated external methods: a useful option, which however leaves controllers without a structured methodology without guidance.

We suggest supplementing the Template or the Explainer with a minimum set of elements that the method should include: (1) likelihood scale, with operational definition of each level; (2) severity scale, with operational definition of each level;

(3) criteria for assigning levels to a given scenario; (4) risk matrix combining likelihood and severity; (5) acceptability threshold; (6) modulating factors and their impact on the risk level; (7) criterion for moving from inherent to residual risk; (8) link between threat scenarios, measures and residual risk; (9) criterion for prioritising mitigation measures.

It would also be useful for the Explainer to include a non-binding example of a simplified method (for instance, a three-level scale, 3×3 matrix and predefined acceptability criteria).

3.7 Inherent risk assessment (section 4.1.c)

Section 4.1.c requires the assessment of likelihood, severity, modulating factors and risk level without accompanying such variables with operational definitions. In their absence, the same scenario may receive different assessments from different controllers, making it impossible to verify the reasoning followed.

We suggest supplementing the Explainer with an illustrative, non-binding grid for the assessment of **likelihood** (low = highly improbable event or dependent on hardly verifiable conditions; medium = plausible event, already observed in analogous contexts; high = probable or frequent event under the processing conditions) and **severity** (low = limited and reversible impact; medium = significant impact but limited in time or scope; high = serious and hardly reversible impact, with significant prejudice to fundamental rights and freedoms).

We further suggest setting out in the Explainer an illustrative list of **aggravating factors** (very large number of data subjects; special categories of data; vulnerable subjects (minors, patients, employees, migrants); profiling and automated decisions with significant effects; hindrance to the exercise of rights) and **mitigating factors** (data minimisation already implemented; effective pseudonymisation or encryption; access segregation; robust organisational controls; short retention periods; reversibility of the processing).

We finally suggest clarifying that the inherent risk should be assessed with reference to the specific scenarios previously identified, rather than as an independent and abstract assessment.

3.8 Processing based on artificial intelligence systems

The Template does not include a dedicated section on processing involving artificial intelligence systems, although such processing represents one of the categories for which a DPIA is most frequently required under Article 35(3)(a) GDPR: systematic and extensive evaluation of personal aspects based on automated processing, profiling and decisions producing legal or similarly significant effects on the data subject.

The absence of specific guidance risks leaving uncovered the risk dimensions specific to AI systems, including (i) quality, lawfulness and provenance of training data; (ii) model opacity and limits to explainability; (iii) bias and discrimination risks; (iv) model drift and emergent behaviour; (v) training data extraction risks in generative models. These aspects raise appropriateness questions that are not fully captured by the general categories of Article 32 GDPR nor by the aggravating factors traditionally referenced in risk assessment.

We further suggest clarifying in the Explainer the interface between the DPIA under Article 35 GDPR and the Fundamental Rights Impact Assessment (FRIA) under Article 27 of Regulation (EU) 2024/1689 (the AI Act). The two instruments have partially overlapping scopes but different addressees, purposes and methodologies: absent operational guidance, controllers and deployers of high-risk AI systems risk either duplicating the analysis or, conversely, leaving relevant aspects uncovered.

We suggest providing, at least as an annex to the Template or within the Explainer, a dedicated module for AI-based processing, identifying at a minimum: (i) the classification of the system under the AI Act (high-risk under Annex III, GPAI, non-high-risk); (ii) the allocation of responsibilities between provider and deployer; (iii) the specific requirements of lawfulness, quality and traceability of training data; (iv) the documentation of the model (model cards, datasheets) within the DPIA; (v) transparency measures vis-à-vis the data subject and human oversight measures under Article 14 of the AI

Act; (vi) the interface with the FRIA. This approach would be consistent with EDPB Opinion 28/2024 on the use of personal data in the development and deployment of AI models.

4. Conclusion

The observations formulated above aim to strengthen the usability of the Template, the verifiability of the controller's assessments and the internal consistency of DPIAs, without introducing a single methodology or an alternative model.

The Template should retain the flexible approach that characterises it, while providing more granular criteria in those sections where discretionary assessments are required. With specific reference to non-default, accidental, unlawful or anomalous events, the classification of scenarios should be aligned at least with the categories referenced in Article 32(2) GDPR: destruction, loss, alteration, unauthorised disclosure and unauthorised access to personal data. A dedicated module for AI-based processing, together with an explicit interface with the FRIA under Article 27 of the AI Act, would also address one of the most uncertain application areas for controllers and deployers.

These proposals do not affect the controller's methodological freedom. Rather, they seek to make such freedom documented and defensible, consistently with the function of the DPIA under Article 35 GDPR, with the principles of Article 5 GDPR, and with the *data protection by design* and security obligations under Articles 25 and 32 GDPR.

We remain at the Board's disposal for any further clarification.

Yours faithfully,

_____

GDPR Club - il Dipartimento Data Protection & New Tech

Studio Associato Servizi Professionali Integrati – WST Law & Tax Firm