Dr. Anu Talus, Chair, European Data Protection Board
Rue Wiertz/Wiertzstraat 60
1047 Bruxelles/Brussel
Belgium

By webform

02 June 2026

DPIA Template Public Consultation

Dear Dr. Talus,

I welcome the opportunity to respond to the European Data Protection Board's public consultation on its draft Data Protection Impact Assessment (DPIA) template. I agree that such a template is necessary as a practical tool to assist controllers in fulfilling their obligations under Article 35 of the GDPR and will limit my comments to three points: (1) the delineation of scope; (2) the assessment of proportionality; and (3) the absence of provisions governing review periods and review triggers.

1. Scope

Page 6 of the template requires controllers to identify the scope of the DPIA, i.e. 'what has been considered and what has been left out of the assessment and why.' Paragraph 9 of the explainer elaborates on this by stating that controllers should 'Clarify the scope of this DPIA: identify what has been considered and what has been left out of the assessment and why, what are the boundaries of the assessment'. However, the template and explainer do not provide any further guidance on how controllers should delimit the scope of the DPIA.

Scoping is a well-documented and recurring deficiency in DPIA practice. The importance of precise scoping can be illustrated by three examples. First, in the Brussels Airport case, the absence of a complete processing scope meant that the DPIA failed to capture the full extent of the risks.[1] Second, in the Toyota Bank case, the DPIA produced by the bank concerned the issuance of loans, but did not include the profiling of customers as a part of the loans process.[2] The UODO found that this violated Article 35(1) and (7) of the GDPR.[3] Third, in relation to Covid-19 contact tracing apps, my research found widespread confusion over the role of Google and Apple in

[1] APD/GBA (Belgium), 'Temperature measurement and processing relating to specific categories of personal data at Brussels Airport in the context of COVID-19' (2022) 48/2022 para 188 <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-48-2022.pdf> accessed 19 April 2026.
[2] 'Toyota Bank' (2024) DKN.5112.14.2022 21 <https://uodo.gov.pl/decyzje/DKN.5112.14.2022> accessed 1 March 2026.
[3] ibid 25.

these systems and whether processing conducted by those entities as part of the contact tracing systems should be considered as in scope for national DPIAs.[4]

I acknowledge that some of these issues will be addressed by the references in sections **1.1.2. Purpose** and **1.1.4 Nature, scope and context** to identifying the lifecycle of the personal data being processed. I therefore suggest that paragraph 0.5.9 of the explainer be expanded to provide guidance on scoping. In particular, the explainer could clarify that controllers should identify *all* processing operations that form part of the envisaged processing activity, justify any exclusions, and explain how they have determined the boundaries of the assessment. These should include where processing is carried out by processors, joint controllers, platform providers, or other third parties whose activities are functionally necessary to the processing under assessment.

---

2. Proportionality

I note the EDPB's proposed enhancement in explicitly naming risks to data subjects from normal processing in paragraph 32 in addition to the non-default risk in paragraph 35. However, I contend that this to not go far enough as proportionality has proven a very difficult concept for controllers to understand.[5] Three enforcement cases illustrate the consequences of inadequate proportionality assessment in DPIAs. In the Cosmote case, the Hellenic SA found the controller's response to be 'insubstantial and missing any justification.'[6] A Hungarian Bank approached the question of proportionality only from the perspective of the bank and not the data subjects, which the Hungarian SA concluded was not fit for purpose.[7] In its findings on an unacceptable AENA biometric DPIA the Spanish AEPD referred to the Constitutional Court's doctrine of the "triple juicio de proporcionalidad."[8]

I submit that the template should adopt the AENA finding to clearly and explicitly lay out the three steps in proportionality in language comprehensible to a controller.[9] This approach is naturally consistent with the findings in AENA and would directly address the superficial engagement documented in the Cosmote and the Hungarian Bank cases.

---

[4] Michael Spratt and Tj McIntyre, 'Assessing Data Protection Impact Assessments: Lessons from COVID-19 Contact Tracing Apps' (2026) 60 Computer Law & Security Review 106233, s 3.4.3 <https://doi.org/10.1016/j.clsr.2025.106233> accessed 13 December 2025.
[5] Michael Spratt, 'Exploring Interpretative Fragmentation in EU Data Protection Impact Assessments — Quantitative Analysis from COVID-19 Proximity Apps' (2026) 61 Computer Law & Security Review 106321, tbl 2 <https://linkinghub.elsevier.com/retrieve/pii/S2212473X26000623> accessed 26 April 2026.
[6] Hellenic Data Protection Authority, 'Decision 4/2022 (Cosmote)' (Hellenic Data Protection Authority 2022) Prot. No.: 222 33 <https://www.dpa.gr/sites/default/files/2022-01/4_2022%20anonym%20%282%29_0.pdf> accessed 7 July 2024.
[7] Hungarian National Authority for Data Protection and Freedom of Information, 'Application of Artificial Intelligence to Analyse Customer Service Audio Recordings' (2022) NAIH-7350/2021., NAIH-85/2022. para 85 <https://www.naih.hu/hatarozatok-vegzesek/file/517-mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei> accessed 23 April 2023.
[8] Agencia Española de Protección de Datos, 'AENA and Facial Recognition' (AEPD) PS/00431/2024 65 <https://www.aepd.es/documento/ps-00431-2024.pdf> accessed 16 March 2026.
[9] ibid 66.

3. Review Periods and Review Triggers

There are currently no EU-wide criteria for a periodic review or for the identification of circumstances that trigger an update of a DPIA. The guidance from the SAs generally makes it clear that completing a DPIA is not the end of the process. The CNIL in France and the IP of Slovenia are outliers with an explicit maximum period between reviews of three years.[10] Outside of the Union the recently released Malaysian guidance specifies a two-year review cycle.[11] However, this template presents the DPIA as a one-off assessment. This points to a wider problem that controllers regard the DPIA as a compliance checkbox. It is rarely integrated as a risk management tool into the development life cycle.

I submit that the template should include a section recommending controllers to: (a) specify a fixed maximum review interval, proportionate to the risk level of the processing; (b) identify specific trigger events that would prompt an unscheduled review; and (c) document the outcome of each review, including any revisions made to the DPIA or the processing activity itself.

4. Conclusion

I believe the current draft of the EDPB's DPIA template offers an opportunity to further strengthen practice regarding scope delineation, proportionality assessment, and ongoing review. Incorporating these elements would help shift the DPIA from a static compliance checklist toward a dynamic tool of process-based regulation, aligning it with the goal of becoming a continuous mechanism for accountability and risk management.

Thank you for the opportunity to comment on the draft template and explainer. I hope these observations are helpful. I remain available to provide further information or to engage with the Board on any of the points raised in this response.

Dr. Michael Spratt BE MBA CEng CIPP/E
Dublin, June 2026

[10] Commission nationale de l'informatique et des libertés, 'Délibération N° 2018-327 Du 11 Octobre 2018' (Commission nationale de l'informatique et des libertés 2018) 2 <https://www.legifrance.gouv.fr/download/file/6n6rVjcbpv8jbOnafuwaxhBcN54StttgEC670rsbjts=/JOE_TEXTE> accessed 28 March 2023; Information Commissioner of the Republic of Slovenia, 'Ocene Učinkov Na Varstvo Podatkov' 19 <https://www.ip-rs.si/fileadmin/user_upload/Smernice_o_ocenah_ucinka__DPIA__nov2017.pdf>.

[11] 'Persoanal Data Protection Guideline Data Protection Impact Assessmemt (Malaysia)' (Department of Personal Data Protection 2026) s 12.1 <https://www.pdp.gov.my/ppdpv1/en/akta/data-protection-impact-assessment-guideline-dpia/> accessed 10 May 2026.