Panasonic truly welcomes the efforts undertaken by the EDPB in line with its Helsinki Statement to make GDPR compliance easier and strengthen consistency across Europe. A DPIA template which can be adopted by local Data Protection Authorities as their sole standard or as a 'meta-template' to which national-specific templates will align is a highly practical resource.

The template covers all mandatory elements of a DPIA as per Article 35(7) GDPR in a systematic way. Additionally, the DPIA template extends to detailed considerations regarding general GDPR compliance requirements and covers elements of Articles 5, 28 and 30 GDPR. The expanded scope increases complexity and may duplicate documentation already maintained by controllers without adding value to the risk assessment.

The template appears to be drafted by privacy professionals for privacy professionals. The language, complexity, and sheer volume may well overwhelm and frustrate non-specialists. Business managers, project leads, or IT professional may struggle to complete it without substantial guidance. This may either lead to superficial answers, significant delays, outright rejection of the template as „too complicated", and ultimately increase the workload for the legal/privacy team/DPO to review DPIAs.

To support broader adoption by business owners, we respectfully offer the following recommendations:

1. **Shorten and streamline the template**
   - Limit the scope of the template to the requirements set out in Art. 35(7) GDPR.
   - Separate threshold analysis from DPIA.
     The need for a DPIA should stem the outcome of the threshold analysis, which can be embedded or uploaded as appropriate. For all processing activities controllers need to assess the risk to determine if a DPIA is needed. This is done via the so-called threshold analysis based on the GDPR in Article 35(3), guidance issued by Article 29 Working Party, and local blacklists issued by European Supervisory Authorities. A DPIA is needed only if the threshold analysis is positive. Embedding the threshold analysis into the DPIA as proposed (0.5 DPIA technical sheet) would require the DPIA template to be used for all processing activities. Requiring the controller (i.e., the business) to always work with such a long and detailed document may lead to reluctance in practice.
     If the threshold analysis remains integrated, please consider clearly indicating that employees are considered vulnerable data subjects, in line with Article 29 Working Party Guidance (Working Paper 248 rev. 01, p. 10 and 11).

2. **Simplify language and provide for more guidance**
   Free-text fields are hard for non-privacy professionals to fill consistently and accurately without explicit guidance or examples. For average business users, understanding what kind of answer is expected in each field is crucial.

   - If compliance with core data protection principles remains integral part of the DPIA template, consider including examples of common measures supporting compliance with Article 5, the exercise of data subjects' rights, Article 7, data

protection by design and default, etc., as tick boxes or placeholders. Also, consider including guidance on data quality metrics, requirements or thresholds.

- Consider listing examples of common threats posed by the processing as it has been designed, how these can be materialised, and impacts on data subjects‘ rights and freedoms as tick boxes or placeholders to improve ease of use.
- Consider listing examples of common threats posed by malfunctions and deviations from design and default, how these can be materialised, and impacts on data subjects‘ rights and freedoms as tick boxes.
- Consider providing concrete descriptions for likelihood and severity with simple, business-understandable language and for example a simple 3x3 risk matrix.
- Consider providing at least one filled in example (e.g. on CCTV in public facing areas or large-scale marketing programs) to illustrate proper completion.

3. **Recording of final decision and DPO role**

   The template does not detail the decision maker. The explainer requires “approval of the DPIA as complete and finished by a responsible official (Managing Director, CEO, etc.)” which may not be practical. The business project owner or equivalent should typically sign off, accepting residual risk where appropriate.

   Clarify in the explainer that the DPO cannot sign off the DPIA and consider including a RACI that reiterates the DPO’s advisory role rather than preparation responsibility.