# RAKUTEN GROUP, INC. SUBMISSION ON THE EUROPEAN DATA PROTECTION BOARD DATA PROTECTION IMPACT ASSESSMENT (DPIA) TEMPLATE

Rakuten Group, Inc. welcomes the work done by the EDPB to achieve a common template accepted by all Supervisory Authorities aiming to facilitate the consistent conducting of DPIAs by controllers operating across the European Union (EU).

Since the adoption of GDPR ten years ago, numerous other countries have followed and have also enacted their own privacy legislation, sometimes modeling their laws after the GDPR, and often requiring similar impact assessments. Such a document is therefore to be welcomed and may be an example followed across the globe.

To support this initiative from the EDPB, Rakuten would like to suggest ways to limit the redundancy of the template and make it easier to fill for organizations, as well as seek clarifications regarding the legal impact of the template that could be provided in the accompanying notice.

## Simplify and reorganize the template to streamline the assessment

### A. The redundancy of the template could be limited

As the EDPB itself has noted in the template explainer, the template can be quite redundant. In view of conducting efficient assessments, both in terms of resources and time, such redundancy should be limited to the absolute minimum and only when relevant, which often appears not to be the case here.

This is mostly evident in section 2.3.a, which requires assessing compliance with each of the principles under Article 5 GDPR, which then duplicates the assessments made under other sections of the template:

i. Transparency is assessed directly in section 2.3.a, and then again under 2.3.b, when compliance with the right to be informed must also be assessed.
ii. The purpose limitation principle assessed in section 2.3.a can already be documented under sections 1.1.b and 1.1.c., for which Rakuten welcomes the distinction between primary purposes and secondary or compatible uses.
iii. Data minimization and retention/storage limitation measures are assessed both under section 2.2.a and 2.3.a.
iv. The integrity and confidentiality principle is already covered, notably through the security measure assessment under section 2.3.e.

### B. Relevant information should be gathered in the same sections

Similarly, to avoid having to review similar and linked aspects of the processing in different sections and thus limit cross-references within the same document, the items contained in Section 2.3.c could be integrated into other relevant sections as follows:

i. "*Requirements on the provisions and withdrawal of consent*" could be moved to section 2.3.b regarding data subjects' rights.

| **Data subject rights** | **List of supporting measures** | **Discussion of appropriateness and effectiveness** | **Implementation status** |
|---|---|---|---|
| Information to be provided to the data subjects (Articles 12, 13 and 14 GDPR) [···] | | | * Planned<br>* Partially implemented<br>* Implemented |
| Requirements on the provisions and withdrawal of consent (Article 7 GDPR) | | | * Planned<br>* Partially implemented<br>* Implemented |

ii. "*Relationship with processors*" could be moved to section 1.3., regarding the means of processing, supporting assets and underlying architecture.

| **Processing phase or stage (considering the functional description under 1.2)** | **Means of processing and supporting assets (Including, when relevant, the measures framing the relationship with processors)** | **Explanation** |
|---|---|---|
| | | |

iii. "*Safeguards relating to international transfer(s)*" could be moved to section 1.1.d, as a follow-up to the question regarding international data transfer. This section could also be modified to better distinguish the context of the processing, its cross-border nature (if any), and the eventual international transfer it entails. A refined section 1.1.d. could be presented as follows:

| | |
|---|---|
| Context of the processing: circumstances and environment (use cases, supported business processes, status of the controller and relationship with the data subjects, data subjects categories and potential vulnerable groups, ~~cross-border processing, international transfers~~, etc.). | |
| Is this a cross-border processing? | * No<br>* Yes (justification and details): _____ |
| Is personal data going to be transferred to a recipient in a third country or international organisation? | * No<br>* Yes (justification and details, including safeguards): _____ |

## Avoid adding complexity to the existing legal framework

Rakuten Group, Inc. would welcome clarification on the regulatory impact of the template.

Indeed, the template explainer mentions that the template contains the "*minimum amount of information that should always be documented*", but it goes further than the previous "Criteria for an acceptable DPIA" in the WP29 Guidelines on DPIA[1], and from the express GDPR requirements for a DPIA.

To illustrate this, section 2.2.b. concerns data quality, a notion not defined by the GDPR. Either this refers to the accuracy of the data, which is already covered by section 2.3.a., or this refers to a different concept, which would lead to the EDPB adding new requirements to an already stringent analysis, without a clear legal basis to do so. In any event, this should be clarified to avoid increasing the regulatory burden on organizations.

Rather than a specific example, and following what was mentioned above, section 2.3.a. and its enhanced granularity on compliance with each GDPR principles might lead to artificial and burdensome distinctions between compliance measures, as well as redundancy with other questions contained in the template.

Especially when read in the context of the WP29 Guidelines on DPIA[2], section 2.3.a. appears superfluous to the necessity and proportionality analysis required under section 3. The WP29 Guidelines previously quoted already adequately delineated the scope of the assessment required for a DPIA. The EDPB's template should focus on clarifying this checklist and providing practical guidance on how to complete a DPIA, rather than introducing additional non-statutory requirements that exceed the existing framework.

[1] *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP29, 4 October 2017
[2] *Ibid*

## Foster global cooperation on data protection impact assessments worldwide

In the future, the relationship with other regional data protection impact assessments or similar requirements should be developed. This could take the form of a joint document, similar to the "*Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*"[3] the European Commission published in the past in cooperation with the ASEAN.

Beyond global companies' interests, such a document would facilitate cooperation between controllers and processors established in different regions, by fostering a common understanding of regulations, in line with EU's goals to limit regulatory burdens on companies while maintaining a high level of compliance.

A collaboration between EU's and other countries' privacy regulators would also be beneficial for the public side, as this would allow sharing of good practices and move towards mutual recognition of assessments made under different laws, hence reducing the constraints both for organizations and enforcers.

For instance, it is worth noting that Texas[4] and Nebraska[5] privacy laws already provide for the recognition of data protection assessments done in compliance with foreign privacy laws, if the requirements are reasonably similar. In the absence of joint cooperation with foreign authorities on this matter, the EDPB could similarly provide guidance on how other assessments can be adapted or recognized by European Data Protection Authorities.

This DPIA template could therefore serve as a baseline for future joint documents and lead the way for similar templates across the globe.

[3] https://commission.europa.eu/system/files/202305/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf
[4] § 541.105 of the Business and Commerce Code
[5] §87-1116 of the Nebraska Revised Statutes

## Conclusion

Rakuten Group, Inc. appreciates the EDPB's efforts in developing a unified DPIA template, and hopes that its contribution will support these efforts to make this document clearer and more practical for the organizations that will use it.

To ensure that it fulfills its purpose of supporting organizations in their privacy compliance journey while not adding obligations for controllers and processors, the template would also benefit from additional precisions regarding its legal impact.

Finally, Rakuten Group, Inc. strongly believes that increased cooperation with other privacy regulators globally would benefit companies as well as enforcers in having a common understanding of global practices and methodologies, and calls for the EDPB and European Commission to move towards joint work with third countries' data protection authorities and regional organizations on this matter.

**About Rakuten Group, Inc.**

Rakuten Group, Inc. (TSE: 4755) is a global leader in internet services that empower individuals, communities, societies and businesses. Founded in Tokyo in 1997 by Hiroshi Mikitani, Rakuten has grown to offer services in e-commerce, fintech, digital content and communications to more than 2.1 billion members around the world. The company is dedicated to providing innovative platforms that foster entrepreneurship and economic growth, all connected by the globally recognized Rakuten Points loyalty program. For more information on the company, visit the Rakuten Group Corporate Website.