Ingka Group’s submission to the EDPB consultation on GDPR templates

02 December 2025

About Ingka Group

Ingka Group is the largest IKEA retailer, operating in over thirty markets and serving millions of customers worldwide. As a strategic partner to develop and innovate the IKEA business, Ingka Group owns and operates IKEA sales channels under franchise agreements with Inter IKEA Systems B.V. Our business is built on a commitment to creating a better everyday life for the many people, with a strong focus on sustainability, innovation, and responsible data management.

We welcome the EDPB’s initiative to enhance clarity and support for organisations and are committed to sharing our experience and recommendations to help make GDPR compliance more accessible and effective for all.

For more information, please contact:
Giacomo Pizza
EU Public Affairs Leader
Giacomo.pizza@ingka.ikea.com

GDPR compliance templates

1. Individual rights

One of the core pillars of GDPR is empowering individuals with rights over their personal data—such as access, rectification, erasure, and portability. However, without a standardized approach, managing these requests can become inconsistent, inefficient, and prone to errors.

Having standardized templates for GDPR individual rights requests and templates for responses brings significant benefits across multiple dimensions:

- **Efficiency and Consistency:** Templates streamline the process, reducing time spent drafting unique responses for each request and ensures uniformity across all business areas and regions, which is crucial for multinational organizations.
- **Risk Reduction**: Provides a clear structure for including mandatory GDPR elements (e.g., identity verification, timelines, scope of data).
- **Cost Savings:** Reduces operational overhead by standardizing workflows.
- **Operational Clarity:** Templates act as a checklist, ensuring all legal requirements are met and simplifies training for new team members and improves scalability.
- **Improved Communication:** Clear, structured responses reduce misunderstandings with data subjects.
- **Contribution to Rights and Freedoms of Individuals:** Templates make it easier for individuals to exercise their rights without confusion and ensures responses are clear, timely, and informative, reinforcing trust. Standardization guarantees that all individuals receive consistent and fair handling of their requests and prevents discrimination or arbitrary differences in responses.

2. Transfer Impact Assessments

Templates would provide a standardized structure for Transfer Impact Assessments (TIAs), ensuring all organizations follow the same methodology and criteria. This reduces inconsistencies and improves comparability across industries.

- **Efficiency and Time Savings:** Pre-defined sections and checklists streamline the assessment process, reducing the time and resources needed to create TIAs from scratch.
- **Risk Identification and Mitigation:** Templates would guide companies through evaluating local legal frameworks, surveillance risks, and supplementary measures, ensuring thorough and consistent risk analysis.
- **Audit-Ready Documentation:** Using standardized templates makes it easier to demonstrate accountability and compliance during audits or investigations by data protection authorities.
- **Scalability:** For suppliers serving multiple clients, one robust TIA can cover all customers using the same product/service, making compliance scalable.

3. Technical implementation and standards

Guidance from regulatory authorities is essential for setting principles, but relying solely on descriptive documents often creates ambiguity and inconsistency. Human language can be open to interpretation, which makes compliance harder and slows down adoption. To truly advance data protection and privacy, we need to go beyond “what” and provide the “how.”
Instead of only issuing guidelines, authorities could deliver technical specifications and reference implementations that organizations can directly integrate into their workflows. For example:

- Standardized algorithms and procedures for common compliance tasks.
- Open-source libraries and APIs that work across spreadsheets, analytics platforms, and enterprise software.
- Implementation documentation that ensures interoperability and scalability.

This approach would enable automation, reduce compliance costs, and ensure uniform application of privacy principles globally. Technical standards can be versioned and updated as technology evolves, eliminating the need for constant reinterpretation of vague guidance. Rather than multiple authorities issuing separate documents, a unified technical framework supported by a dedicated technical team would dramatically improve privacy outcomes worldwide.

Algorithms and code are precise; guidance is not. By bridging this gap, regulators can transform compliance from a manual, error-prone process into an automated, reliable system—making privacy protection stronger and more practical for everyone.

4. **Pseudonymisation and/or anonymisation robustness assessment template**
   Templates would provide a standardised structure for robustness assessments of pseudonymisation and/or anonymisation techniques, ensuring that all organisations follow the same methodology and criteria. This reduces inconsistencies and improves comparability across industries (e.g. what “means reasonably likely” to re-identify are considered, what technical and organisational measures are in place) so that controllers assess robustness using the same key questions and structure, reducing divergent outcomes between member states.

   - **Efficiency and Time Savings:** Pre-defined techniques, criteria and checklists streamline the assessment process, reducing the time and resources needed to use pseudonymisation and/or anonymisation.
   - **Risk Identification and Mitigation:** assessment templates would guide companies through evaluating the risk of re-identification, ensuring thorough and consistent risk analysis.
   - **Accountability & Audit-Ready Documentation:** using standardised templates makes it easier to demonstrate accountability and compliance during audits or investigations by data protection authorities. Provide a ready-made artefact to show to supervisory authorities during audits, breach investigations or transfer assessments, demonstrating that the controller consistently applied the EDPB’s guidance.
   - **Scalability:** Re-use the same core risk-assessment logic (data types, attacker models, auxiliary information, technical controls) for both pseudonymisation and anonymisation.

5. **DPO reporting template to Senior Management**

Templates would support the DPO's role and provide a further standardised report template for Senior Management. This will help fulfil the DPO role in accordance with GDPR requirements.

- **Improved accountability:** This would better define conditions, frequency, content and effectiveness of DPO reporting to Senior management. A harmonised template would make it clear who the DPO must report to, how often, and on what topics, thereby helping organisations demonstrate that they meet the structural and accountability expectations.
- **Enhanced oversight**: Improved management awareness and accountability for data protection. That in turn enables informed decisions, a visible tone-from-the-top, and more transparent allocation of budget and resources to privacy programmes.

- **Independence**: Stronger DPO independence and position within the organisation, ensuring an essential guarantee of the independence of the DPO, including anchoring the expectation that DPOs regularly escalate issues independently.