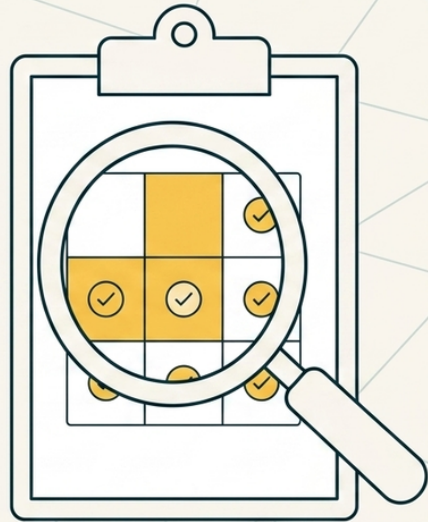


DPIA Template GDPR Article 35

FREE TEMPLATE — DOCX · PDF · MD



DPIA Template — GDPR Article 35

Screening · description · necessity & proportionality · risk matrix · sign-off · AI annex

FREE TEMPLATE — DOCX · PDF · MD | Version 1.0 · Updated 2026-07-15

Complete BEFORE the processing starts (Art 35(1)).

Sections 4–11 carry the mandatory Art 35(7)(a)–(d) content.

Where a DPO is designated, their advice is mandatory (Art 35(2)).

High residual risk → consult your supervisory authority first (Art 36: 8 weeks + 6).

Review at least when the risk changes (Art 35(11)).

1. Document control

DPIA reference	Internal ID, e.g. DPIA-2026-004
Processing / feature name	Short name of the processing under assessment
Controller / assessor	Legal entity; person completing this DPIA
Date started / approved	Lifecycle dates

2. Screening — is a DPIA required?

2a. Article 35(3) always-DPIA cases

Case	Applies?
35(3)(a) Systematic, extensive automated evaluation/profiling with legal or similarly significant effects	Yes / No
35(3)(b) Large-scale processing of special-category (Art 9) or criminal-conviction (Art 10) data	Yes / No
35(3)(c) Large-scale systematic monitoring of a publicly accessible area	Yes / No

2b. WP248 rev.01 nine high-risk criteria (rule of thumb: two met → DPIA)

Criterion	Met?
1. Evaluation or scoring (incl. profiling, predicting)	Yes / No
2. Automated decision-making with legal or similarly significant effect	Yes / No
3. Systematic monitoring	Yes / No
4. Sensitive data or data of a highly personal nature	Yes / No
5. Data processed on a large scale	Yes / No
6. Matching or combining datasets	Yes / No
7. Data concerning vulnerable data subjects	Yes / No
8. Innovative use / new technological or organisational solutions (incl. AI)	Yes / No
9. Processing preventing exercise of a right or use of a service/contract	Yes / No

Also check your supervisory authority's Art 35(4) list — e.g. CNIL's 14-category list (FR), the ICO's UK high-risk list, Datatilsynet's Norwegian list.

3. Screening outcome

DPIA required?	Yes / No — with the trigger(s): Art 35(3) case, number of WP248 criteria met, or an Art 35(4) list entry
If no	Record the reasoning and keep this document; re-screen if the processing changes

4. Systematic description of the processing (Art 35(7)(a))

Nature, scope, context, purposes	<i>What the processing does, for whom, at what scale, and why</i>
Categories of personal data	<i>Flag special categories (Art 9) explicitly</i>
Categories of data subjects	<i>Flag vulnerable groups (children, employees, patients)</i>
Recipients	<i>Internal teams, processors, third parties</i>
International transfers	<i>Third countries + transfer mechanism (SCCs, adequacy)</i>
Retention	<i>Period and deletion trigger</i>
Systems and data flows	<i>Where the data lives and moves</i>
Legitimate interest pursued	<i>Only if Art 6(1)(f) is relied on</i>

5. Consultation record (Art 35(2), 35(9))

DPO advice	<i>Mandatory where a DPO is designated — record the advice and date</i>
Data subjects' views	<i>Where appropriate; if not sought, record why</i>
Processors / vendors consulted	<i>E.g. the AI provider's documentation reviewed</i>

6–7. Necessity and proportionality (Art 35(7)(b))

Lawful basis	<i>Art 6 basis; Art 9 condition if special categories</i>
Necessity	<i>Why this processing achieves the purpose; data minimisation applied</i>
Proportionality	<i>Less intrusive alternatives considered and why they do not suffice</i>
Transparency & rights	<i>How data subjects are informed; how access, erasure, objection, portability are honoured</i>

8–10. Risk assessment (Art 35(7)(c))

Risks to the rights and freedoms of data subjects — not business risks. Score likelihood × severity on a 3×3 matrix.

	Severity: Low	Severity: Medium	Severity: High
Likelihood: High	Medium	High	High
Likelihood: Medium	Low	Medium	High
Likelihood: Low	Low	Low	Medium

Worked example row:

ID	Risk	L	S	Measure	Residual
EX1	Unauthorised access to customer-support AI logs containing personal data	M	H	Access restricted to on-call support role; logs pseudonymised after 24h; retention cut to 30 days; access audited	Low

11. Mitigation measures (Art 35(7)(d))

One specific measure per risk. Generic statements do not reduce scores; specific TOMs (Art 32), access controls, pseudonymisation and retention cuts do.

12. Residual risk & Article 36 decision

Overall residual risk	Low / Medium / High — after all measures
Prior consultation required?	If residual risk remains HIGH: consult the supervisory authority BEFORE processing (Art 36) — written advice within 8 weeks, extendable by 6
Authority consulted / response	Date, reference, outcome — or n/a

13–14. Sign-off & review log (Art 35(2), 35(11))

Controller approval	Name, role, date
DPO opinion recorded	Yes / No — date
Review triggers	New data category, new AI model, new recipient, new purpose
Next scheduled review	Date

AI Annex — AI/LLM features and the EU AI Act

Complete for any AI-driven processing (WP248 criterion 8, typically plus 1, 2 and 5). For high-risk AI systems where you are a deployer in scope of EU AI Act Art 27, the FRIA may be documented jointly with this DPIA — neither assessment replaces the other.

Model / system	Provider, model, version
Training-data provenance	Personal data in training/fine-tuning data? Provider documentation reviewed?
Automated decisions & effects	Legal or similarly significant effects (Art 22 GDPR)? Human in the loop?
Explainability & oversight	Can outcomes be explained to data subjects? Which oversight measures apply?
Bias / accuracy risks	Testing performed; known failure modes; monitoring plan
EU AI Act classification	Prohibited / High-risk / Limited (transparency) / Minimal
FRIA reference (Art 27)	If high-risk and in scope: joint documentation reference