

Data Protection Impact Assessment (DPIA)

Pursuant to Art. 35 GDPR · Template & workflow for SMEs · EN

Legally reviewed by a certified Data Protection Officer (CIPP/E) · Provided by ETHYX · Version 1.0 · June 2026

» **HOW TO USE** A DPIA assesses the risks a planned processing activity poses to people's rights and freedoms, and the measures to reduce them. It is required before high-risk processing begins (Art. 35). Work through the steps in order: Step 1 decides whether you even need a DPIA – if you do, complete Steps 2–7. Replace every [placeholder], fill in the tables, and have your DPO review the result. Keep the completed DPIA on file as evidence of accountability (Art. 5(2)).

Document control

FIELD	ENTRY
Processing activity / project	[name of the project or system]
Controller	[company name]
DPIA author	[name, role]
DPO consulted	[name – see Step 3]
Date started	[date]
Version / status	[v1.0 – draft / final]

Step 1 – Do you need a DPIA? (Screening)

A DPIA is mandatory in the cases listed in Art. 35(3) GDPR, and generally required where two or more of the EDPB criteria below apply. Screen the planned processing first.

Always required (Art. 35(3))

#	MANDATORY CASE	APPLIES?
a	Systematic and extensive evaluation/profiling with legal or similarly significant effects	[Yes/No]
b	Large-scale processing of special-category (Art. 9) or criminal-offence (Art. 10) data	[Yes/No]
c	Systematic monitoring of a publicly accessible area on a large scale	[Yes/No]

EDPB risk criteria (two or more → DPIA generally required)

#	CRITERION	APPLIES?
1	Evaluation or scoring, including profiling and prediction	[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]

#	CRITERION	APPLIES?
5	Data processed on a large scale	[Yes/No]
6	Matching or combining datasets	[Yes/No]
7	Data concerning vulnerable data subjects (e.g. children, employees)	[Yes/No]
8	Innovative use or applying new technological or organisational solutions	[Yes/No]
9	Processing that prevents data subjects from exercising a right or using a service	[Yes/No]

Screening outcome: **[DPIA required – continue to Step 2 / DPIA not required – record this conclusion and the reasoning, then stop]** .

» **HOW TO USE** If in doubt, do the DPIA – it is cheaper than a finding. If you conclude no DPIA is needed, document why; that record is itself part of your accountability.

Step 2 – Describe the processing

ITEM	DESCRIPTION
Nature of processing	[what you plan to do with the data: collection, use, storage, sharing, deletion]
Scope	[volume and variety of data, number of data subjects, geographic extent, retention period]
Context	[relationship with individuals, their expectations, prior concerns, state of the art]
Purposes	[what you want to achieve; the intended effect on individuals; the benefit]
Data types	[categories of personal data, incl. any special-category data]
Data subjects	[whose data: customers, employees, etc.]
Recipients / processors	[who receives the data; processors involved]
International transfers	[any transfer outside the EU/EEA + safeguard]

Step 3 – Consultation

Record the advice of the DPO and the views of relevant stakeholders and, where appropriate, data subjects (Art. 35(2), 35(9)).

CONSULTED	INPUT / ADVICE	DATE
Data Protection Officer	[DPO's documented advice]	[date]
Internal stakeholders	[IT / security / business owner input]	[date]
Data subjects (if appropriate)	[how their views were sought, or why not]	[date]

Step 4 – Assess necessity and proportionality

QUESTION	ASSESSMENT
Lawful basis (Art. 6)	[which basis, and why it fits]
Purpose limitation	[data used only for the stated purpose?]

QUESTION	ASSESSMENT
Data minimisation	[is each data item necessary? what was excluded?]
Accuracy & retention	[how kept accurate; how long kept; deletion]
Data-subject rights	[how access, rectification, erasure, objection are supported]
Processor compliance	[Art. 28 DPA in place? safeguards?]
International transfers	[safeguard documented?]

Step 5 – Identify and assess the risks

For each risk to individuals' rights and freedoms, rate likelihood and severity, then read the overall risk level from the matrix below.

LIKELIHOOD ↓ / SEVERITY →	MINIMAL	SIGNIFICANT	SEVERE
Remote	Low	Low	Medium
Possible	Low	Medium	High
Probable	Medium	High	High

#	RISK TO INDIVIDUALS	LIKELIHOOD	SEVERITY	OVERALL RISK
1	[e.g. unauthorised access to customer data]	[Remote/Possible/Probable]	[Minimal/Significant/Severe]	[Low/Med/High]
2	[e.g. data retained longer than necessary]	[]	[]	[]
3	[e.g. function creep – data reused for new purpose]	[]	[]	[]
4	[]	[]	[]	[]

Step 6 – Identify measures to reduce the risk

RISK #	MEASURE TO REDUCE OR ELIMINATE THE RISK	EFFECT	RESIDUAL RISK	APPROVED
1	[e.g. enforce MFA + encryption at rest; restrict access by role]	[Eliminated/Reduced/Accepted]	[Low/Med/High]	[Yes/No]
2	[e.g. automated deletion schedule]	[]	[]	[]
3	[e.g. strict purpose-binding + change control]	[]	[]	[]
4	[]	[]	[]	[]

Step 7 – Sign off and record the outcome

ITEM	OUTCOME
DPO advice	[advice provided – accepted / overruled, with reasons]
Residual risk	[overall residual risk after measures: Low / Medium / High]
Prior consultation (Art. 36)	[required? Yes if high residual risk remains and cannot be mitigated – consult the supervisory authority before processing]
Measures approved by	[name, role, date]
Review date	[when this DPIA will be reviewed, e.g. annually or on change]

» **HOW TO USE** If a high residual risk remains that you cannot mitigate, you must consult your supervisory authority before starting the processing (Art. 36 GDPR). Otherwise, the DPO and accountable owner sign off, and you review the DPIA whenever the processing changes.

This template is provided for guidance only and does not constitute legal advice. Reviewed by a certified Data Protection Officer (CIPP/E) · ETHYX · ethyx.eu