Data Protection Impact Assessment

A structured DPIA for high-risk processing - with the technical detail that engineers, legal, and product all need in one place, and a defensible record at the end.

FRAMEWORK	TIME TO COMPLETE	VERSION
GDPR ART. 35	60-90 MINUTES	JULY 2026

How to use this

Complete the sections in order. A DPIA is a living record, not a one-off form - save your version, date it, and revisit it whenever the processing changes. The goal is a document you could hand to a regulator and defend.

When a DPIA is required

Under GDPR Art. 35 a DPIA is mandatory for processing likely to result in a **high risk** to people - in particular: large-scale profiling or automated decisions with legal/similar effects; large-scale special-category data; or systematic monitoring of a public area. When in doubt, do a short screening and record the decision either way.

0 DPIA screening

Use this before the full assessment. If any answer is Yes or Unknown, complete the DPIA.

Screening trigger	Y / N / ?	Notes
New technology, AI, profiling, or automated decisions with significant effects		
Special-category, criminal-offence, children's, or vulnerable-person data at meaningful scale		
Large-scale monitoring, tracking, location data, or behavioural analytics		
Data matching, enrichment, scoring, or decisions that may affect access to services		

1 Processing overview

Processing / project name	Data controller (legal entity)

Assessment owner & DPO (if any)	Date & version

Describe the processing: what data, whose, how collected, and what you do with it

Related RoPA record / product spec / data-flow diagram

2 Necessity & proportionality

Answer plainly. Useful is not a lawful basis.

Question	Answer / justification
What is the specific, legitimate purpose?	
What is the lawful basis (Art. 6) - and condition for special-category data (Art. 9)?	
Could you achieve the purpose with less data, or less identifiable data?	
How are data subjects informed (transparency)?	
How do you support their rights (access, erasure, objection)?	
Have you sought DPO advice and, where appropriate, views from affected people or representatives?	

3 Data flows, actors & processors

One row per data category. This is the map everything else is scored against.

#	Data category	Subjects	Source	Recipients / processors	Location & transfer	Retention
1	e.g. contact data	customers	sign-up form	CRM, email tool	EU / US (SCCs)	24 mo
2						
3						
4						

4 Risk identification & scoring

Score each risk to people's rights & freedoms. Likelihood x Severity, each 1-3. Risk = L x S (1-2 low / 3-4 medium / 6-9 high).

#	Risk to individuals	L	S	Score	Notes
1	e.g. unauthorised access to sensitive data				
2	e.g. unfair exclusion, chilling effect, loss of confidentiality, inability to exercise rights				
3					
4					

5 Mitigating controls & residual risk

For each high/medium risk above, record the control and the risk that remains after it.

#	Mitigating control / measure	Residual risk	Approved?	Owner
1	e.g. encryption, access controls, minimisation	Low / Med / High	Y/N	
2				
3				

Prior consultation

If a high residual risk remains that you can't mitigate, GDPR Art. 36 requires you to consult your supervisory authority **before** starting the processing. Record that decision here.

6 Outcome, sign-off & action plan

Decision

Proceed / Proceed with conditions / Do not proceed

Approved by & date

Residual high risk remains?

No / Yes - if yes, record Art. 36 prior-consultation decision

#	Action to complete before / after go-live	Owner	Due
1			
2			
3			

Scheduled review date

Need a practical compliance review?

This template gets you started. If you'd like an engineer who does compliance to pressure-test your answers - or turn them into working controls, documentation, and audit-ready evidence - book a free 30-minute discovery call.

Book a free discovery call or visit rdelune.dev

This template is provided by rdelune LLC for general informational purposes only and does not constitute legal, regulatory, or professional advice, nor create a consultant-client relationship. Regulatory obligations depend on your specific facts and jurisdiction. Validate your completed document against the applicable law (e.g. the EU GDPR, the ePrivacy Directive, and the EU AI Act) and, where appropriate, with a qualified professional. © 2026 rdelune LLC. You may use and adapt this template freely within your organisation; please retain this attribution.