RESOURCE · COMPLIANCE · RES-002

AI Data Protection Impact Assessment template

VERSION

v1.0

TRACKED AT

agentmodeai.com/holding/RES-002/

SOURCE

agentmodeai.com/resources/

LICENCE

CC BY 4.0

Agent Mode AI publishes editorial work for senior IT leaders. Every claim including the premise of this template is tracked on a public ledger. Verdict updates and corrections at agentmodeai.com/holding/.

Version 1.0 · Published 4 May 2026 · 90-day review cycle

A pre-deployment DPIA for AI and agentic AI systems. Fuses GDPR Article 35 with EU AI Act Articles 26 + 27 (deployer obligations and Fundamental Rights Impact Assessment) into a single working-session document.

Source explainer: https://agentmodeai.com/resources/ai-dpia-template/ Holding-up tracking: https://agentmodeai.com/holding/RES-002/

Use this template BEFORE vendor selection

The most common DPIA failure observed in 2025 supervisory authority decisions: "DPIA conducted after deployment to retrofit the documentation."

Convene in one room or call:

- Data Protection Officer
- Business owner of the AI deployment
- IT lead responsible for integration
- Works-council representative (EU employee-facing systems)

Target: 3-6 hours to complete. Sections 7 and 8 are conditional on the EU AI Act risk classification in section 1.

Section 1: System characterisation

#	Field	Answer
1	AI system name + version (incl. foundation model lineage)	
2	Vendor name + contract reference	
3	Intended use case (1 paragraph + alternatives considered)	
4	Personal data categories at training time	
4b	Personal data categories at inference time	
5	Data subject categories (customers, employees, prospects, public, vulnerable groups)	
6	Geographic scope of deployment + inference processing	
7	GDPR Article 6 lawful basis (+ legitimate-interests assessment if applicable)	
8	EU AI Act risk classification (prohibited / Annex III high-risk / limited-risk / minimal-risk)	

Section 2: Necessity and proportionality (Article 35(7)(b))

#	Field	Answer
1	Why personal data is necessary (could anonymised/aggregated/synthetic suffice?)	
2	Why AI approach is proportionate (could rules-based system suffice?)	
3	Data minimisation measures applied	
4	Retention period at each layer (vendor logs, audit logs, training data)	
5	Consent mechanism OR legitimate-interests assessment outcome	

Section 3: Risks to rights and freedoms (Article 35(7)(c))

#	Risk	Mitigation
1	Automated decision-making materially affecting data subject (Article 22)	Human-in-the-loop mechanism
2	Model output leaking training data (memorisation attacks)	Vendor non-memorisation commitment
3	Biased outcomes affecting protected characteristics	Bias-testing methodology + cadence
4	Confidentiality breach via prompt injection or jailbreaking	Input sanitisation approach
5	Accountability gap when AI errs	Escalation, override, appeal mechanism
6	Function creep: use beyond documented purpose	Change-control process
7	Vendor-side processing creep	Contract review cadence

Section 4: Mitigation measures (Article 35(7)(d))

Category	Measures
Technical	Encryption at rest/transit, access controls, sub-processor restrictions, retention windows, deletion mechanisms
Organisational	RBAC policies, operator training, incident escalation, DPIA review cadence
Contractual	DPA, sub-processor list + notification SLA, model deprecation notice, kill-switch SLA, data portability on termination
Transparency	Privacy notice updates, in-product AI disclosure, documentation accessible to data subjects
Data subject rights	Access, rectification, erasure, objection, Article 22 review request operationalisation

Section 5: Consultation (Article 35(2), 35(9))

#	Field	Answer
1	DPO consultation date + opinion attached	
2	Works-council consultation: jurisdiction (BetrVG §87(1)6 / WOR Art 27 / CSE / other) + outcome	
3	Vulnerable-group representative consultation (if applicable)	
4	If consultation omitted: reason + supervisory authority position relied upon	

Section 6: Residual risk and decision (Article 35(11))

#	Field	Answer
1	Residual risk after mitigation: low / medium / high + rationale	
2	Decision: proceed / proceed with conditions / do not proceed / refer under Article 36	
3	Conditions (if applicable) + verification mechanism for each	
4	If Article 36 referral: date of referral + consultation outcome	

Section 7: EU AI Act Article 26 deployer obligations

Complete only if section 1 question 8 = Annex III high-risk. Active from 2 August 2026.

#	Obligation	Answer
1	Technical + organisational measures ensuring use per vendor instructions	
2	Human oversight assignment + competence/training/authority documentation	
3	Operation monitoring + serious-incident reporting procedure	
4	Automated logging: retention period, content, supervisory-authority access	
5	Worker information + representative notification (employment / education / essential services use cases)	
6	Suspension procedure for Article 79 risk scenarios	

Section 8: Fundamental Rights Impact Assessment (Article 27)

Complete if deployer is a public body, providing public services, or using high-risk system for credit scoring or insurance pricing.

#	Field	Answer
1	Description of deployer processes using the system	
2	Period of time + frequency of intended use	
3	Categories of natural persons + groups likely affected	
4	Specific risks of harm to those categories/groups	
5	Human oversight, internal governance, complaint mechanisms	
6	FRIA results notified to market surveillance authority (where applicable) + date	

Sign-off

Role	Name	Date	Signature
Data Protection Officer			
Business owner			
IT lead			
Works-council representative (EU)			
Compliance / AI governance committee			

Retain signed DPIA for the lifetime of the deployment + 6 years.

Review triggers

- Material change to AI system being deployed
- Change to categories of data processed
- Extension of use case beyond originally documented scope
- Calendar review at 12 months regardless

Frameworks referenced

- GDPR (Regulation 2016/679) Articles 6, 22, 35, 36
- EU AI Act (Regulation 2024/1689) Articles 26, 27, 79; Annex III; Annex IV
- Datenschutzkonferenz Muss-Liste 2024 (DE)
- Dutch Autoriteit Persoonsgegevens AI framework 2025
- Italian Garante AI human-in-the-loop guidance 2024

Licence