

CHECKLIST · TOMORIS TOOLBOX

AI and Data Protection: Checklist with Data Protection Impact Assessment

Review steps before deploying an AI service, obligation and minimum content of the data protection impact assessment, pre-assessment under the DSFA-V, and link to the AI Act

UPDATED

Oct 25, 2026

LENGTH

PDF, 8 pages

ONLINE

tomoris.com/en/downloads/ki-datenschutz-folgenabschaetzung

AT A GLANCE

1

Criterion under § 2 para. 2 DSFA-V is enough for a DPIA

4

Minimum contents of a DPIA (Art. 35(7))

8 weeks

Authority's deadline for prior consultation (Art. 36)

Dec 2, 2027

High-risk AI under Annex III: obligations apply

WHO IT IS FOR

- Data protection officers and those responsible for data protection who approve AI services
- Project managers who introduce chat assistants, transcription, or analyses with AI
- IT and purchasing teams that conclude contracts with AI providers
- Executive management responsible for lawful use

WHAT THIS COVERS

As soon as employees enter personal data into an AI service, have conversations transcribed, or have documents analyzed, the GDPR applies, and alongside it the AI Act. This checklist guides you through the review before deployment: roles and contract with the provider, legal basis, information for data subjects, third-country transfers, and automated decisions. The focus is on the data protection impact assessment: when it is mandatory under Art. 35 GDPR and the Austrian DSFA-V (Datenschutz-Folgenabschätzungs-Verordnung, the Austrian regulation listing processing operations that require a DPIA), what it must contain at a minimum, and how it interacts with the AI Act.

This checklist is a TOMORIS recommendation and provides an overview. It does not replace legal advice or a case-by-case data protection impact assessment; the statutory text in its current version is authoritative.

CONTENTS

01	GDPR and AI Act: what applies to what	2
02	Review steps before deploying an AI service	3
03	Third countries: AI services from the US	4
04	When a data protection impact assessment is mandatory	5
05	Procedure and minimum content of the DPIA	6
06	Fillable DPIA pre-assessment	7
07	Common mistakes	7
08	Sources	8

01 —

GDPR and AI Act: what applies to what

The GDPR governs personal data, the AI Act governs the AI system; both apply side by side.

The GDPR applies as soon as an AI service processes personal data: in inputs, uploaded files, recordings, outputs, and logs. Anyone who uses the service for their own purposes is the controller; the provider is a processor if it processes data only on instructions. If it determines the purposes and means itself, for example by using inputs for its own purposes, it is considered a controller in that respect (Art. 28(10) GDPR). The AI Act (Regulation (EU) 2024/1689, amended by Regulation (EU) 2026/1744) additionally sets out obligations for providers and deployers of AI systems; it does not replace a review under the GDPR.

Art. 4 AI Act

Providers and deployers take measures to support the AI literacy of their staff and of other persons acting on their behalf; as amended by Regulation (EU) 2026/1744, in force since July 27, 2026.

Art. 26(9) AI Act

Deployers of high-risk AI systems use the information provided by the provider under Art. 13 to carry out their data protection impact assessment under Art. 35 GDPR. For high-risk systems under Annex III, Chapter III Sections 1 to 3 apply from December 2, 2027 (Art. 113(c) as amended by Regulation (EU) 2026/1744).

Art. 27 AI Act

Certain deployers, above all bodies governed by public law and private entities providing public services, carry out a fundamental rights impact assessment for high-risk systems. If an obligation under it is already met by the data protection impact assessment, the deployer may refer to it or adopt parts of it (para. 4).

In the legislative process, not applicable law: The Digital Omnibus proposal COM(2025) 837 (procedure 2025/0360(COD), in committee as of October 25, 2026, according to the Legislative Observatory) would, among other things, introduce EU-wide uniform lists for the data protection impact assessment and add rules on processing for AI development and operation. Until it is promulgated, Art. 35 GDPR and the Austrian regulations DSFA-V and DSFA-AV (Datenschutz-Folgenabschätzungs-Ausnahmenverordnung, the Austrian regulation listing processing operations exempt from a DPIA) apply.

02

Review steps before deploying an AI service

To check off before personal data flows into an AI service; go through once per use case.

- ☐ Use case described: which data, which purpose, which persons are affected, which outputs are used and how
- ☐ Roles clarified: you as the controller, the provider as the processor, and it is contractually excluded that the provider uses inputs for its own purposes, or this use has been deliberately assessed
- ☐ Data processing agreement (DPA) under Art. 28 GDPR concluded, with sub-processors, processing locations, and deletion periods
- ☐ Legal basis under Art. 6 defined; for legitimate interest, the three-step test (interest, necessity, balancing) documented as described by the EDPB in Opinion 28/2024
- ☐ Special categories under Art. 9 (e.g., health data) and criminal offense data under Art. 10 only with a separate legal basis, otherwise excluded by technical and organizational means
- ☐ Data minimization under Art. 5(1)(c): only necessary data, pseudonymized or without personal reference where possible

☐	Information for data subjects under Art. 13 and 14 supplemented, for example in the privacy policy, employee information, or a notice at the start of a conversation
☐	Third-country transfer reviewed: adequacy decision or safeguards under Chapter V, also for support and sub-processors
☐	No decision based solely on automated processing with legal or similarly significant effects without a basis under Art. 22(2) and safeguards under para. 3
☐	Data subject rights can be implemented: access, rectification of incorrect outputs, erasure of inputs and logs
☐	Origin of the model questioned: according to the EDPB, supervisory authorities consider whether the deployer has appropriately verified that the model was not developed through unlawful processing (Opinion 28/2024, para. 129)
☐	Technical and organizational measures under Art. 32: access, logging, retention period, configuration of the service
☐	Entry in the record of processing activities under Art. 30 supplemented
☐	Review for a data protection impact assessment carried out and documented (see pre-assessment)
☐	AI literacy of users under Art. 4 AI Act supported through training and rules

This checklist is a TOMORIS recommendation. The obligations of the GDPR and the AI Act cited are required by law; which of them apply to your use case depends on the data, purpose, and service.

03 —

Third countries: AI services from the US

What applies to transfers to the US and why you should check the status of proceedings before deciding.

Many AI services are operated or supported by providers in the US. For transfers to organizations listed on the Data Privacy Framework List of the U.S. Department of Commerce, there is an adequacy decision of the European Commission (Implementing Decision (EU) 2023/1795, Art. 1). For other recipients, you need safeguards under Art. 46 GDPR, such as standard contractual clauses. The General Court of the EU dismissed an action against the decision on September 3, 2025 (T-553/23); an appeal against this was lodged with the Court of Justice on October 31, 2025 (C-703/25 P), on which no judgment had been published as of October 25, 2026. Before deciding, check whether the recipient is listed and what the status of the proceedings is.

04 —

When a data protection impact assessment is mandatory

Art. 35 GDPR, the Austrian list in the DSFA-V, and the exemptions in the DSFA-AV.

A data protection impact assessment (DPIA) must be carried out in advance if processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons (Art. 35(1) GDPR). Art. 35(3) names typical cases. In Austria, the DSFA-V, a regulation of the Austrian Data Protection Authority (Datenschutzbehörde), defines when a DPIA is required in any case, and the DSFA-AV defines when it is not. Both have applied unchanged since 2018 (RIS, version as of October 25, 2026).

Triggers for a DPIA relating to AI services

TRIGGER	CITATION	WHAT IT MEANS FOR AI
New technologies that make it difficult to assess the impact, in particular artificial intelligence; one criterion from items 1 to 6 is enough	§ 2 para. 2 no. 4 DSFA-V	The most important trigger for many AI deployments involving personal data
Evaluation or classification of persons, solely automated, with possible negative legal, physical, or financial effects	§ 2 para. 2 no. 1 DSFA-V	For example, AI-supported pre-screening of applications or credit scoring forecasts
Systematic and extensive evaluation of personal aspects as the basis for decisions with legal effects	Art. 35(3)(a) GDPR	Profiling with decisions about persons
Large-scale processing of special categories (Art. 9) or of criminal offense data (Art. 10)	Art. 35(3)(b) GDPR	For example, analysis of health data with AI
Two or more criteria, including vulnerable persons such as employees, patients, or minors under 14	§ 2 para. 3 DSFA-V	For example, AI analyses about employees together with another criterion

Exemptions: For the processing operations described in the annex to the DSFA-AV (DSFA-A01 to DSFA-A22, such as customer management or HR administration), no DPIA is required (§ 1 DSFA-AV, § 2 para. 1 DSFA-V). Whether an AI deployment still falls within the description of an exemption must be assessed case by case. For employee data, § 2 DSFA-V contains special rules for cases with a works agreement or the consent of the staff representation.

If the deployment falls under no list, the guideline WP 248 rev.01 of the Article 29 Working Party, endorsed by the European Data Protection Board (EDPB), helps: it names nine criteria, including evaluation or scoring, automated decisions, systematic monitoring, sensitive data, large volumes of data, vulnerable persons, and innovative technologies. In most cases, a DPIA must be carried out if two criteria are met, sometimes even if only one is met.

05 —

Procedure and minimum content of the DPIA

What the impact assessment must contain under Art. 35(7) and when the Data Protection Authority must be consulted.

1

Describe the processing systematically

Operations, purposes, and, where applicable, the legitimate interests (Art. 35(7)(a)): data flows from input through the model to the output, storage and logging at the provider, sub-processors involved.

2

Assess necessity and proportionality

Is the processing necessary for the purpose, are there less intrusive means, for example without personal reference or with less data (lit. b)?

3

Assess risks to data subjects

Risks to rights and freedoms (lit. c); for AI, for example, incorrect outputs about persons, disclosure of confidential inputs, discrimination through evaluations, lack of traceability. For high-risk AI, use the provider's information under Art. 13 AI Act (Art. 26(9) AI Act).

4

Define remedial measures

Safeguards, security measures, and mechanisms (lit. d), for example data minimization, human review before decisions, access restrictions, short retention periods, training.

5

Involve others

Seek the advice of the data protection officer, if designated (Art. 35(2)), and, where appropriate, the views of data subjects or their representatives, such as the works council (para. 9).

6

Decide on the residual risk

If a high risk remains despite the measures, consult the Data Protection Authority before processing (Art. 36(1)); it has up to eight weeks, extendable by six weeks (para. 2).

7

Review

Where necessary, check whether the processing is performed in accordance with the DPIA, at least when the risk changes (Art. 35(11)), for example with a new model, new features, or a new provider.

06 —

Fillable DPIA pre-assessment

Fill in for each AI use case and file with the record of processing activities.

Pre-assessment for the use case [designation], as of [MM/DD/YYYY], reviewed by [name, role]

QUESTION	CITATION	YES / NO, REASONING
Does the processing fall entirely under an exemption of the DSFA-AV? If yes: which one?	§ 1 DSFA-AV	_____
Does the AI deployment make it difficult to assess the impact on data subjects?	§ 2 para. 2 no. 4 DSFA-V	_____
Does the system evaluate or classify persons solely by automated means, with possible negative effects?	§ 2 para. 2 no. 1 DSFA-V	_____
Does another criterion from § 2 para. 2 nos. 2, 3, 5, or 6 DSFA-V apply?	§ 2 para. 2 DSFA-V	_____
Do two or more criteria from § 2 para. 3 DSFA-V apply?	§ 2 para. 3 DSFA-V	_____
Is there a typical case under Art. 35(3)(a) to (c)?	Art. 35(3) GDPR	_____
How many of the nine criteria from WP 248 rev.01 are met?	WP 248 rev.01	_____
Is the system a high-risk AI system under the AI Act?	Art. 6 AI Act	_____
Result: DPIA required, not required, or voluntary; next review date	Art. 35 GDPR	_____

07 —

Common mistakes

Where AI rollouts often fail in terms of data protection law.

- Private account instead of a company contract: without a contract under Art. 28 and proper configuration, it is unclear what the provider does with the inputs.
- DPIA only after the launch: it must be carried out in advance (Art. 35(1)); fundamental decisions are often hard to change afterward.
- Only the AI Act reviewed: an AI system that is not high-risk may still require a DPIA under the GDPR and the DSFA-V.
- Outputs adopted without review: incorrect statements about persons are inaccurate data; data subjects have a right to rectification (Art. 16 GDPR).
- Logs forgotten: inputs and histories are often stored at the provider and in your own system; retention period and access belong in the review.

NEXT STEP

Check It Yourself or Put It into Practice Together

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

08

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **Regulation (EU) 2016/679 (GDPR)**
Art. 5, 6, 9, 10, 13, 14, 16, 22, 28, 30, 32, 35, 36, 46
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 2 **DSFA-V, BGBl. II No. 278/2018, current version in the RIS**
§ 2 para. 1 to 3, version as of October 25, 2026 (original version)
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 3 **DSFA-AV, BGBl. II No. 108/2018, current version in the RIS**
§ 1 and annex DSFA-A01 to DSFA-A22, version as of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 4 **Article 29 Working Party: Guidelines on Data Protection Impact Assessment, WP 248 rev.01 (October 4, 2017)**
Section III.B: nine criteria, rule of thumb of two criteria
ec.europa.eu/newsroom/article29/redirection/document/47711
- 5 **EDPB: Endorsement 1/2018 of the Article 29 Working Party documents**
No. 6: WP 248 rev.01
www.edpb.europa.eu/sites/default/files/files/news/endorsement_o...
- 6 **EDPB: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (December 17, 2024)**
Three-step test of legitimate interest, para. 129 on deployers
www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-...
- 7 **Regulation (EU) 2024/1689 (AI Act)**
Art. 4, 6, 13, 26(9), 27, 113
eur-lex.europa.eu/eli/reg/2024/1689/oj/deu
- 8 **Regulation (EU) 2026/1744 (Digital Omnibus Regulation on AI), OJ L of July 24, 2026**
New Art. 4, Art. 27(4), Art. 113(3)(c); in force since July 27, 2026
eur-lex.europa.eu/eli/reg/2026/1744/oj/deu
- 9 **Implementing Decision (EU) 2023/1795 (EU-US Data Privacy Framework) and appeal C-703/25 P**
Art. 1; appeal lodged on October 31, 2025, against judgment T-553/23 of September 3, 2025
eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/deu
- 10 **European Parliament, Legislative Observatory: Digital Omnibus 2025/0360(COD)**
As of October 25, 2026: Awaiting committee decision; proposal COM(2025) 837
oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025/0...