

CHECKLISTE · TOMORIS TOOLBOX

KI und Datenschutz: Checkliste mit Datenschutz-Folgenabschätzung

Prüfschritte vor dem Einsatz eines KI-Dienstes, Pflicht und Mindestinhalt der Datenschutz-Folgenabschätzung, Vorprüfung nach DSFA-V und Bezug zur KI-Verordnung

STAND

25.10.2026

UMFANG

PDF, 8 Seiten

ONLINE

tomoris.com/downloads/ki-datenschutz-folgenabschaetzung

AUF EINEN BLICK

1

Kriterium nach § 2 Abs. 2 DSFA-V genügt für die DSFA

4

Mindestinhalte einer DSFA (Art. 35 Abs. 7)

8 Wochen

Frist der Behörde bei vorheriger Konsultation (Art. 36)

2.12.2027

Hochrisiko-KI nach Anhang III: Pflichten gelten

FÜR WEN

- Datenschutzverantwortliche und Datenschutzbeauftragte, die KI-Dienste freigeben
- Projektleitungen, die Chat-Assistenten, Transkription oder Auswertungen mit KI einführen
- IT und Einkauf, die Verträge mit KI-Anbietern abschließen
- Geschäftsführung, die für den rechtskonformen Einsatz verantwortlich ist

WURUM ES GEHT

Sobald Beschäftigte personenbezogene Daten in einen KI-Dienst eingeben, Gespräche transkribieren oder Dokumente auswerten lassen, gilt die DSGVO, und neben ihr die KI-Verordnung. Diese Checkliste führt durch die Prüfung vor dem Einsatz: Rollen und Vertrag mit dem Anbieter, Rechtsgrundlage, Information der Betroffenen, Drittlandübermittlung und automatisierte Entscheidungen. Den Schwerpunkt bildet die Datenschutz-Folgenabschätzung: wann sie nach Art. 35 DSGVO und der österreichischen DSFA-V Pflicht ist, was sie mindestens enthält und wie sie mit der KI-Verordnung zusammenspielt.

Diese Checkliste ist eine Empfehlung von TOMORIS und gibt einen Überblick. Sie ersetzt keine Rechtsberatung und keine Datenschutz-Folgenabschätzung im Einzelfall; maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung.

INHALT

01	DSGVO und KI-Verordnung: was wofür gilt	2
02	Prüfschritte vor dem Einsatz eines KI-Dienstes	3
03	Drittland: KI-Dienste aus den USA	4
04	Wann eine Datenschutz-Folgenabschätzung Pflicht ist	5
05	Ablauf und Mindestinhalt der DSFA	6
06	DSFA-Vorprüfung zum Ausfüllen	7
07	Häufige Fehler	7
08	Quellen	8

01

DSGVO und KI-Verordnung: was wofür gilt

Die DSGVO regelt die personenbezogenen Daten, die KI-Verordnung das KI-System; beide gelten nebeneinander.

Die DSGVO gilt, sobald ein KI-Dienst personenbezogene Daten verarbeitet: in Eingaben, hochgeladenen Dateien, Aufzeichnungen, Ausgaben und Protokollen. Wer den Dienst für eigene Zwecke einsetzt, ist Verantwortlicher; der Anbieter ist Auftragsverarbeiter, wenn er nur nach Weisung verarbeitet. Bestimmt er Zwecke und Mittel selbst, etwa indem er Eingaben für eigene Zwecke nutzt, gilt er insoweit als Verantwortlicher (Art. 28 Abs. 10 DSGVO). Die KI-Verordnung (VO (EU) 2024/1689, geändert durch VO (EU) 2026/1744) regelt daneben Pflichten für Anbieter und Betreiber von KI-Systemen; sie ersetzt keine Prüfung nach der DSGVO.

Art. 4 KI-VO

Anbieter und Betreiber ergreifen Maßnahmen, um die KI-Kompetenz ihres Personals und anderer Personen in ihrem Auftrag zu unterstützen; in der Fassung der VO (EU) 2026/1744, in Kraft seit 27.7.2026.

Art. 26 Abs. 9 KI-VO

Betreiber von Hochrisiko-KI-Systemen verwenden die Informationen des Anbieters nach Art. 13, um ihre Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen. Für Hochrisiko-Systeme nach Anhang III gilt Kapitel III Abschnitte 1 bis 3 ab 2.12.2027 (Art. 113 lit. c in der Fassung der VO (EU) 2026/1744).

Art. 27 KI-VO

Bestimmte Betreiber, vor allem Einrichtungen des öffentlichen Rechts und private Einrichtungen, die öffentliche Dienste erbringen, führen für Hochrisiko-Systeme eine Grundrechte-Folgenabschätzung durch. Ist eine Pflicht daraus bereits durch die Datenschutz-Folgenabschätzung erfüllt, kann der Betreiber auf diese verweisen oder ihre Teile übernehmen (Abs. 4).

Im Verfahren, nicht geltendes Recht: Der Digital-Omnibus-Vorschlag COM(2025) 837 (Verfahren 2025/0360(COD), Stand 25.10.2026 laut Legislative Observatory im Ausschuss) würde unter anderem EU-weit einheitliche Listen für die Datenschutz-Folgenabschätzung einführen und Regeln zur Verarbeitung für KI-Entwicklung und -Betrieb ergänzen. Bis zu einer Kundmachung gelten Art. 35 DSGVO und die österreichischen Verordnungen DSFA-V und DSFA-AV.

02

Prüfschritte vor dem Einsatz eines KI-Dienstes

Zum Abhaken, bevor personenbezogene Daten in einen KI-Dienst fließen; je Anwendungsfall einmal durchgehen.

- ☐ Anwendungsfall beschrieben: Welche Daten, welcher Zweck, welche Personen sind betroffen, welche Ausgaben werden wie verwendet
- ☐ Rollen geklärt: Sie als Verantwortlicher, der Anbieter als Auftragsverarbeiter, und es ist vertraglich ausgeschlossen, dass er Eingaben für eigene Zwecke nutzt, oder diese Nutzung ist bewusst bewertet
- ☐ Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen, mit Unterauftragsverarbeitern, Orten der Verarbeitung und Löschrufen
- ☐ Rechtsgrundlage nach Art. 6 festgelegt; bei berechtigtem Interesse die dreistufige Prüfung (Interesse, Erforderlichkeit, Abwägung) dokumentiert, wie sie der EDSA in der Stellungnahme 28/2024 beschreibt
- ☐ Besondere Kategorien nach Art. 9 (z. B. Gesundheitsdaten) und Strafdaten nach Art. 10 nur mit eigener Grundlage, sonst technisch und organisatorisch ausgeschlossen
- ☐ Datenminimierung nach Art. 5 Abs. 1 lit. c: nur nötige Daten, wo möglich pseudonymisiert oder ohne Personenbezug
- ☐ Information der Betroffenen nach Art. 13 und 14 ergänzt, etwa in Datenschutzerklärung, Mitarbeiterinformation oder Gesprächshinweis

- ☐ Drittlandübermittlung geprüft: Angemessenheitsbeschluss oder Garantien nach Kapitel V, auch für Support und Unterauftragsverarbeiter
- ☐ Keine ausschließlich automatisierte Entscheidung mit rechtlicher oder ähnlich erheblicher Wirkung ohne Grundlage nach Art. 22 Abs. 2 und Schutzmaßnahmen nach Abs. 3
- ☐ Betroffenenrechte umsetzbar: Auskunft, Berichtigung falscher Ausgaben, Löschung von Eingaben und Protokollen
- ☐ Herkunft des Modells hinterfragt: Laut EDSA berücksichtigen Aufsichtsbehörden, ob der Betreiber angemessen geprüft hat, dass das Modell nicht durch rechtswidrige Verarbeitung entwickelt wurde (Stellungnahme 28/2024, Rn. 129)
- ☐ Technische und organisatorische Maßnahmen nach Art. 32: Zugriff, Protokollierung, Speicherdauer, Konfiguration des Dienstes
- ☐ Eintrag im Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 ergänzt
- ☐ Prüfung auf Datenschutz-Folgenabschätzung durchgeführt und dokumentiert (siehe Vorprüfung)
- ☐ KI-Kompetenz der Nutzenden nach Art. 4 KI-VO durch Schulung und Regeln unterstützt

Die Checkliste ist eine Empfehlung von TOMORIS. Gesetzlich vorgegeben sind die genannten Pflichten der DSGVO und der KI-Verordnung; welche davon für Ihren Anwendungsfall greifen, hängt von Daten, Zweck und Dienst ab.

03 —

Drittland: KI-Dienste aus den USA

Was für Übermittlungen in die USA gilt und warum Sie den Verfahrensstand vor der Entscheidung prüfen sollten.

Viele KI-Dienste werden von Anbietern in den USA betrieben oder unterstützt. Für Übermittlungen an Organisationen, die in der Data Privacy Framework List des U.S. Department of Commerce eingetragen sind, besteht ein Angemessenheitsbeschluss der EU-Kommission (Durchführungsbeschluss (EU) 2023/1795, Art. 1). Für andere Empfänger brauchen Sie Garantien nach Art. 46 DSGVO, etwa Standardvertragsklauseln. Das Gericht der EU hat eine Klage gegen den Beschluss am 3.9.2025 abgewiesen (T-553/23); dagegen wurde am 31.10.2025 Rechtsmittel beim Gerichtshof eingelegt (C-703/25 P), über das bis 25.10.2026 kein Urteil veröffentlicht ist. Prüfen Sie vor der Entscheidung, ob der Empfänger eingetragen ist und wie das Verfahren steht.

04

Wann eine Datenschutz-Folgenabschätzung Pflicht ist

Art. 35 DSGVO, die österreichische Liste der DSFA-V und die Ausnahmen der DSFA-AV.

Eine Datenschutz-Folgenabschätzung (DSFA) ist vorab durchzuführen, wenn eine Verarbeitung, insbesondere bei Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 35 Abs. 1 DSGVO). Art. 35 Abs. 3 nennt Regelfälle. In Österreich legt die Verordnung der Datenschutzbehörde DSFA-V fest, wann jedenfalls eine DSFA nötig ist, die DSFA-AV, wann nicht. Beide gelten seit 2018 unverändert (RIS, Fassung vom 25.10.2026).

Auslöser für eine DSFA mit Bezug zu KI-Diensten

AUSLÖSER	FUNDSTELLE	WAS ER FÜR KI BEDEUTET
Neue Technologien, welche die Abschätzung der Auswirkungen erschweren, insbesondere künstliche Intelligenz; ein Kriterium aus Z 1 bis 6 genügt	§ 2 Abs. 2 Z 4 DSFA-V	Für viele KI-Einsätze mit personenbezogenen Daten der wichtigste Auslöser
Bewertung oder Einstufung von Personen, ausschließlich automatisiert, mit möglichen negativen rechtlichen, physischen oder finanziellen Auswirkungen	§ 2 Abs. 2 Z 1 DSFA-V	Etwa KI-gestützte Vorauswahl von Bewerbungen oder Bonitätsprognosen
Systematische und umfassende Bewertung persönlicher Aspekte als Grundlage für Entscheidungen mit Rechtswirkung	Art. 35 Abs. 3 lit. a DSGVO	Profiling mit Entscheidungen über Personen
Umfangreiche Verarbeitung besonderer Kategorien (Art. 9) oder von Strafdaten (Art. 10)	Art. 35 Abs. 3 lit. b DSGVO	Etwa Auswertung von Gesundheitsdaten mit KI
Zwei oder mehr Kriterien, u. a. schutzbedürftige Personen wie Arbeitnehmer, Patienten oder unmündige Minderjährige	§ 2 Abs. 3 DSFA-V	Etwa KI-Auswertungen über Beschäftigte zusammen mit einem weiteren Kriterium

Ausnahmen: Für die in der Anlage zur DSFA-AV beschriebenen Verarbeitungen (DSFA-A01 bis DSFA-A22, etwa Kundenverwaltung oder Personalverwaltung) ist keine DSFA nötig (§ 1 DSFA-AV, § 2 Abs. 1 DSFA-V). Ob ein KI-Einsatz noch innerhalb der Beschreibung einer Ausnahme liegt, ist im Einzelfall zu prüfen. Für Beschäftigtendaten enthält § 2 DSFA-V Sonderregeln für Fälle mit Betriebsvereinbarung oder Zustimmung der Personalvertretung.

Fällt der Einsatz unter keine Liste, hilft die Leitlinie WP 248 rev.01 der Art.-29-Datenschutzgruppe, vom Europäischen Datenschutzausschuss (EDSA) bestätigt: Sie nennt neun Kriterien, darunter Bewertung oder Scoring, automatisierte Entscheidungen, systematische Überwachung, sensible Daten, große Datenmengen, schutzbedürftige Personen und innovative Technologien. In den meisten Fällen ist bei zwei erfüllten Kriterien eine DSFA durchzuführen, manchmal schon bei einem.

05 —

Ablauf und Mindestinhalt der DSFA

Was die Folgenabschätzung nach Art. 35 Abs. 7 enthalten muss und wann die Datenschutzbehörde zu konsultieren ist.

1

Verarbeitung systematisch beschreiben

Vorgänge, Zwecke und gegebenenfalls die berechtigten Interessen (Art. 35 Abs. 7 lit. a): Datenflüsse vom Eingeben über das Modell bis zur Ausgabe, Speicherung und Protokollierung beim Anbieter, beteiligte Unterauftragsverarbeiter.

2

Notwendigkeit und Verhältnismäßigkeit bewerten

Ist die Verarbeitung für den Zweck erforderlich, gibt es mildere Mittel, etwa ohne Personenbezug oder mit weniger Daten (lit. b)?

3

Risiken für Betroffene bewerten

Risiken für Rechte und Freiheiten (lit. c), bei KI etwa falsche Ausgaben über Personen, Weitergabe vertraulicher Eingaben, Diskriminierung durch Bewertungen, fehlende Nachvollziehbarkeit. Bei Hochrisiko-KI die Informationen des Anbieters nach Art. 13 KI-VO nutzen (Art. 26 Abs. 9 KI-VO).

4

Abhilfemaßnahmen festlegen

Garantien, Sicherheitsvorkehrungen und Verfahren (lit. d), etwa Datenminimierung, menschliche Prüfung vor Entscheidungen, Zugriffsbeschränkung, kurze Speicherfristen, Schulung.

5

Beteiligen

Den Rat des Datenschutzbeauftragten einholen, falls benannt (Art. 35 Abs. 2), und gegebenenfalls den Standpunkt der Betroffenen oder ihrer Vertreter, etwa des Betriebsrats (Abs. 9).

6

Restrisiko entscheiden

Bleibt trotz Maßnahmen ein hohes Risiko, vor der Verarbeitung die Datenschutzbehörde konsultieren (Art. 36 Abs. 1); sie hat bis zu acht Wochen Zeit, verlängerbar um sechs Wochen (Abs. 2).

7

Überprüfen

Erforderlichenfalls prüfen, ob die Verarbeitung der DSFA entspricht, zumindest wenn sich das Risiko ändert (Art. 35 Abs. 11), etwa bei neuem Modell, neuen Funktionen oder neuem Anbieter.

06

DSFA-Vorprüfung zum Ausfüllen

Je KI-Anwendungsfall ausfüllen und zum Verzeichnis von Verarbeitungstätigkeiten legen.

Vorprüfung für den Anwendungsfall [Bezeichnung], Stand [Datum], geprüft von [Name, Funktion]

FRAGE	FUNDSTELLE	JA / NEIN, BEGRÜNDUNG
Fällt die Verarbeitung vollständig unter eine Ausnahme der DSFA-AV? Wenn ja: welche?	§ 1 DSFA-AV	_____
Erschwert der KI-Einsatz die Abschätzung der Auswirkungen auf Betroffene?	§ 2 Abs. 2 Z 4 DSFA-V	_____
Bewertet oder stuft das System Personen ausschließlich automatisiert ein, mit möglichen negativen Auswirkungen?	§ 2 Abs. 2 Z 1 DSFA-V	_____
Trifft ein anderes Kriterium aus § 2 Abs. 2 Z 2, 3, 5 oder 6 DSFA-V zu?	§ 2 Abs. 2 DSFA-V	_____
Treffen zwei oder mehr Kriterien aus § 2 Abs. 3 DSFA-V zu?	§ 2 Abs. 3 DSFA-V	_____
Liegt ein Regelfall nach Art. 35 Abs. 3 lit. a bis c vor?	Art. 35 Abs. 3 DSGVO	_____
Wie viele der neun Kriterien aus WP 248 rev.01 sind erfüllt?	WP 248 rev.01	_____
Ist das System ein Hochrisiko-KI-System nach der KI-Verordnung?	Art. 6 KI-VO	_____
Ergebnis: DSFA erforderlich, nicht erforderlich oder freiwillig; nächster Prüftermin	Art. 35 DSGVO	_____

07

Häufige Fehler

Woran KI-Einführungen datenschutzrechtlich oft scheitern.

- Privates Konto statt Firmenvertrag: Ohne Vertrag nach Art. 28 und Konfiguration ist offen, was der Anbieter mit den Eingaben tut.
- DSFA erst nach dem Start: Sie ist vorab durchzuführen (Art. 35 Abs. 1); nachträglich lassen sich Grundentscheidungen oft nur schwer ändern.
- Nur die KI-Verordnung geprüft: Ein KI-System, das nicht hochriskant ist, kann trotzdem eine DSFA nach DSGVO und DSFA-V erfordern.
- Ausgaben ungeprüft übernommen: Falsche Angaben über Personen sind unrichtige Daten; Betroffene haben ein Recht auf Berichtigung (Art. 16 DSGVO).
- Protokolle vergessen: Eingaben und Verläufe werden oft beim Anbieter und im eigenen System gespeichert; Speicherdauer und Zugriff gehören in die Prüfung.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

08

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **Verordnung (EU) 2016/679 (DSGVO)**
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 Nr. 278/2018, geltende Fassung im RIS**
§ 2 Abs. 1 bis 3, Fassung vom 25.10.2026 (Stammfassung)
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 3 **DSFA-AV, BGBl. II Nr. 108/2018, geltende Fassung im RIS**
§ 1 und Anlage DSFA-A01 bis DSFA-A22, Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 4 **Art.-29-Datenschutzgruppe: Guidelines on Data Protection Impact Assessment, WP 248 rev.01 (4.10.2017)**
Abschnitt III.B: neun Kriterien, Faustregel zwei Kriterien
ec.europa.eu/newsroom/article29/redirection/document/47711
- 5 **EDSA: Endorsement 1/2018 der Dokumente der Art.-29-Datenschutzgruppe**
Nr. 6: WP 248 rev.01
www.edpb.europa.eu/sites/default/files/files/news/endorsement_o...
- 6 **EDSA: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (17.12.2024)**
dreistufige Prüfung des berechtigten Interesses, Rn. 129 zu Betreibern
www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-...
- 7 **Verordnung (EU) 2024/1689 (KI-Verordnung)**
Art. 4, 6, 13, 26 Abs. 9, 27, 113
eur-lex.europa.eu/eli/reg/2024/1689/oj/deu
- 8 **Verordnung (EU) 2026/1744 (Digital-Omnibus-Verordnung zur KI), ABl. L vom 24.7.2026**
neuer Art. 4, Art. 27 Abs. 4, Art. 113 Abs. 3 lit. c; in Kraft seit 27.7.2026
eur-lex.europa.eu/eli/reg/2026/1744/oj/deu
- 9 **Durchführungsbeschluss (EU) 2023/1795 (Datenschutzrahmen EU-USA) und Rechtsmittel C-703/25 P**
Art. 1; Rechtsmittel eingelegt am 31.10.2025 gegen das Urteil T-553/23 vom 3.9.2025
eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/deu
- 10 **Europäisches Parlament, Legislative Observatory: Digital Omnibus 2025/0360(COD)**
Stand 25.10.2026: Awaiting committee decision; Vorschlag COM(2025) 837
oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025/0...