// KI-Hub VON STRUKTURAFLOW

COMPLIANCE

DSFA & Verarbeitungsverzeichnis für KI-Tools: Pflichten in Österreich

Wann ein KI-Tool eine DSFA auslöst, was ins Verarbeitungsverzeichnis gehört und wie DSFA-V, DSFA-AV und die FRIA nach Art. 27 KI-VO zusammenspielen.

AUTOR
Strukturaflow IT-Team

VERÖFFENTLICHT
2. Oktober 2026

ONLINE LESEN
https://wissen.strukturaflow.com/datenschutz-folgenabschaetzung-verarbeitungsverzeichnis-ki-tools-oesterreich/

Ein Steuerberatungsbüro in Linz nutzt seit acht Monaten eine KI-Textassistenz für Mandantenkorrespondenz. Ein Handelsbetrieb in Graz lässt Bewerbungen von einem Matching-Tool vorsortieren. Beide Tools laufen produktiv, in beiden Fällen fehlt der Eintrag im Verarbeitungsverzeichnis und eine dokumentierte Schwellenprüfung. Auffällig wird dann nicht das Tool, sondern die fehlende Unterlage — das Verzeichnis ist nach Art. 30 Abs. 4 DSGVO auf Anfrage vorzulegen.

Dieser Artikel klärt die Reihenfolge der Pflichtdokumente und die zwei österreichischen Verordnungen dazu. Die Einordnungen sind eine Auslegung der zitierten Normen nach aktueller Rechtslage — die Bewertung Ihres Falls gehört zu Ihrer Kanzlei.

Warum Verzeichnis, DSFA und FRIA drei verschiedene Dokumente sind

Das **Verarbeitungsverzeichnis** nach Art. 30 DSGVO ist ein Inventar: Es dokumentiert jede Verarbeitungstätigkeit in Ihrer Zuständigkeit, unabhängig vom Risiko. Die **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO ist eine Bewertung — nur für Verarbeitungen, die „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ haben, und zwar „vorab“. Maßstab ist dabei das Risiko für die betroffenen Personen, nicht das eigene Bußgeld- und Reputationsrisiko; die Verwechslung ist der häufigste inhaltliche Fehler. Die **Grundrechte-Folgenabschätzung** (FRIA) nach Art. 27 KI-VO ist ein drittes, eigenständiges Dokument mit deutlich engerem Adressatenkreis.

	DSFA (Art. 35 DSGVO)	FRIA (Art. 27 KI-VO)
Gilt	seit 25.5.2018	ab 2. Dezember 2027 (Anhang III)
Verpflichtet	jeden Verantwortlichen bei hohem Risiko	Einrichtungen des öffentlichen Rechts, private Erbringer öffentlicher Dienste, Betreiber nach Anhang III Nr. 5 lit. b und c
Behörde	keine Vorlage, Konsultation nur bei hohem Restrisiko	Mitteilung der Ergebnisse an die Marktüberwachungsbehörde

Die DSFA bewertet das Schutzniveau personenbezogener Daten, die FRIA die Grundrechte insgesamt. Ein Privatunternehmen, das KI zur Bewerbervorauswahl einsetzt, ist nach Art. 27 Abs. 1 KI-VO **nicht** FRIA-pflichtig, solange es keine öffentlichen Dienste erbringt — wohl aber DSFA-pflichtig. Wer betroffen ist, darf nach Art. 27 Abs. 4 KI-VO in der Fassung der Digital-Omnibus-Verordnung einschlägige Abschnitte der DSFA in die FRIA aufnehmen. Für Hochrisiko-Systeme kommt eine technische Dokumentationsschiene hinzu; deren Umfang beschreibt der Beitrag zu den Dokumentationspflichten für Hochrisiko-KI in Österreich.

Die Arbeitsreihenfolge bleibt dieselbe: Verzeichniseintrag, Schwellenprüfung, dann falls nötig DSFA — am besten vor dem Rollout, wie der Fahrplan für die KI-Einführung von der Bestandsaufnahme bis zur Umsetzung zeigt. Nach dem Erkenntnis des Verwaltungsgerichtshofs vom 24. Juni 2026 (Ro 2025/04/0007) macht eine fehlende oder fehlerhafte DSFA die Verarbeitung übrigens nicht rechtswidrig; eigenständig sanktionierbar bleibt die Pflicht trotzdem.

Wer überhaupt ein Verarbeitungsverzeichnis führen muss

Art. 30 Abs. 1 DSGVO verpflichtet jeden Verantwortlichen. Die Entlastung in Abs. 5 gilt für Unternehmen mit weniger als 250 Mitarbeitern — „es sei denn", die Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, sie erfolgt nicht nur gelegentlich, oder es werden besondere Datenkategorien nach Art. 9 Abs. 1 bzw. Daten nach Art. 10 DSGVO verarbeitet. Diese drei Rückausnahmen sind nach dem Positionspapier der Artikel-29-Datenschutzgruppe vom 19. April 2018 alternativ verknüpft: Eine genügt. Zwei Punkte daraus sind entscheidend:

- Die Schwelle lautet im Original „a risk (not just a high risk)" — sinngemäß übersetzt: ein Risiko, nicht erst ein hohes Risiko. Sie liegt damit **deutlich unter** der DSFA-Schwelle.
- „Gelegentlich" ist eine Verarbeitung nur, wenn sie außerhalb des gewöhnlichen Geschäftsbetriebs erfolgt — Beschäftigtendaten laut Papier also nicht.

Faktisch ist damit jedes Unternehmen mit Angestellten betroffen; kleiner ausfallen darf nur der Umfang. Wer ein KI-Tool im Auftrag anderer betreibt, führt das schlankere Auftragsverarbeiter-Verzeichnis nach Art. 30 Abs. 2 DSGVO — ohne Zwecke, Datenkategorien, Empfänger und Löschfristen. Auch eine Konzernlösung entlastet nicht: Das Bundesverwaltungsgericht hielt am 25. August 2022 (W214 2207491-1) fest, dass ein Verzeichnis der Holding nicht genügt.

Was für ein KI-Tool ins Verarbeitungsverzeichnis gehört

Die Pflichtfelder nach Art. 30 Abs. 1

Bevor Sie ein Feld ausfüllen, müssen Sie den **Datenfluss erfassen**: Welche Daten gelangen in das Tool, wer greift darauf zu, wohin gehen sie weiter, wie lange bleiben sie dort.

Die vier Felder, an denen bei KI-Tools die Arbeit hängt, sind **Zweck, Kategorien, Empfänger, Löschfrist**. Der Zweck (lit. b) ist nicht „Einsatz von KI", sondern der fachliche Zweck. Die Kategorien betroffener Personen und die Datenkategorien (lit. c) fallen breiter aus als erwartet, weil Prompt-Historie und Nutzungsprotokolle mitlaufen. Bei Empfängern (lit. d) und Drittlandübermittlungen (lit. e) gehören Anbieter, Sub-Dienstleister und Hosting hinein — bei US-

Anbietern mit Standardvertragsklauseln und Transfer Impact Assessment. Löschfrist (lit. f) und die technischen und organisatorischen Maßnahmen (lit. g) stehen unter „wenn möglich". Eine **Rechtsgrundlage** verlangt Art. 30 Abs. 1 DSGVO nicht.

Strukturprinzip dabei: ein Eintrag pro Verarbeitungszweck, nicht pro Tool. Dieselbe KI-Textassistenz kann drei Einträge erfordern — Kundenkorrespondenz, interne Protokolle, Bewerberkommunikation —, weil Zweck, betroffene Personen und Fristen sich unterscheiden.

Das Feld „Löschfrist" ist der häufigste Leerstand; woher die Fristen kommen, zeigt das Löschkonzept für KI-Tools mit Vorlage. Dass Backups einer eigenen Logik folgen, erklärt Löschpflicht und Backup-Retention nach österreichischer Rechtslage. Die Angaben zu Empfängern und Sub-Auftragsverarbeitern holen Sie aus dem Auftragsverarbeitungsvertrag — welche Klauseln dort stehen sollten, listet der Beitrag zu den Pflichtklauseln im Vertrag mit KI-Anbietern.

Mustereintrag: KI-Textassistenz im Kundenservice

FELD	BEISPIELINHALT
Zweck	Antwortentwürfe für Kundenanfragen, Versand durch Mitarbeitende
Betroffene Personen	Kundinnen und Kunden, Interessenten, Mitarbeitende im Service
Datenkategorien	Name, Kontaktdaten, Anfrageinhalte, Prompt- und Protokolldaten
Empfänger	Anbieter als Auftragsverarbeiter, Hosting laut Vertragsanhang
Löschfrist	Anfragedaten sechs Monate nach Fallabschluss, Prompts 30 Tage

Wann ein KI-Tool eine Datenschutz-Folgenabschätzung auslöst

Die Prüfung folgt einer festen Kette, nicht dem Bauchgefühl:

1. Werden personenbezogene Daten verarbeitet (Art. 4 Z 1 DSGVO)? Wenn nein: keine DSFA, kein Eintrag.
2. Greift eine Ausnahme der DSFA-AV? Sie ist nach § 2 Abs. 1 DSFA-V vorrangig zu prüfen.
3. Ist ein Kriterium des § 2 Abs. 2 DSFA-V oder sind zwei des § 2 Abs. 3 DSFA-V erfüllt? Dann ist die DSFA zwingend.
4. Liegt unabhängig davon nach **Art. 35** Abs. 1 oder Abs. 3 DSGVO ein voraussichtlich hohes Risiko vor?

Für Schritt 4 nennt Art. 35 Abs. 3 DSGVO drei Regelbeispiele: systematische und umfassende Bewertung persönlicher Aspekte als Entscheidungsgrundlage, umfangreiche Verarbeitung besonderer Datenkategorien nach Art. 9 Abs. 1 oder Art. 10, und systematische umfangreiche Überwa-

chung öffentlich zugänglicher Bereiche. Das Wort „insbesondere“ heißt: Die Liste ist nicht abschließend. Sobald besondere Daten im Spiel sind, verschiebt sich die Bewertung deutlich; der HR-spezifische Fall ist in DSGVO und KI-Tools für Mitarbeiterdaten in Österreich ausgearbeitet.

Der Schritt ist nicht optional: Die Datenschutzbehörde hat am 16. November 2018 (DSB-D213.692/0001-DSB/2018) festgehalten, dass DSFA-V und DSFA-AV keine abschließenden Aufzählungen sind und dann die Einzelfallprüfung greift. Als Hilfsmaßstab dienen dann die neun Kriterien der Leitlinien WP 248 rev.01 der Artikel-29-Datenschutzgruppe — eine Orientierungshilfe, keine Rechtsnorm.

DSFA-V und DSFA-AV: die zwei österreichischen Verordnungen

Hier sind die meisten Ratgebertexte ungenau. Die Datenschutzbehörde hat die Listen nach Art. 35 Abs. 4 und 5 DSGVO gemäß § 21 Abs. 2 DSG als **Verordnung im Bundesgesetzblatt** kundgemacht — verbindliche Rechtsnormen. Deutsche Landeslisten oder „Muss-Listen“ gelten in Österreich nicht.

Die DSFA-V (BGBl. II Nr. 278/2018) ist die Muss-Liste. Ihr § 2 Abs. 2 enthält sechs Kriterien, von denen bereits eines allein die Pflicht auslöst. Für KI-Projekte ist Z 4 der Kern, wörtlich:

> „Verarbeitungen von Daten unter Nutzung oder Anwendung neuer bzw. neuartiger Technologien oder organisatorischer Lösungen, welche die Abschätzung der Auswirkungen auf die betroffenen Personen und die gesellschaftlichen Folgen erschweren, insbesondere durch den Einsatz von künstlicher Intelligenz und die Verarbeitung biometrischer Daten […]“

Der Verordnungsgeber nennt künstliche Intelligenz also seit 2018 ausdrücklich im Normtext. Entscheidend ist die Einschränkung im Relativsatz: Die Technologie muss die Abschätzung der Auswirkungen erschweren. Nicht jeder KI-Einsatz ist damit DSFA-pflichtig — bei intransparenten oder generativen Systemen mit Personenbezug ist Z 4 aber der naheliegende Fall.

§ 2 Abs. 3 DSFA-V verlangt zwei oder mehr Kriterien und nennt **Arbeitnehmer ausdrücklich als schutzbedürftige betroffene Personen** — jeder KI-Einsatz mit Beschäftigtendaten erfüllt damit bereits eines. Dazu ein Punkt, der meist fehlt: Nach den Schlusssätzen des § 2 Abs. 2 DSFA-V gilt die Pflicht „im Zusammenhang mit Beschäftigungsverhältnissen“ nicht, „wenn eine Betriebsvereinbarung oder Zustimmung der Personalvertretung vorliegt“. Das betrifft dem Wortlaut nach nur die Verordnungspflicht; eine Pflicht nach Art. 35 DSGVO kann fortbestehen, und eine Klarstellung dazu ist nicht ersichtlich.

Die DSFA-AV (BGBl. II Nr. 108/2018) ist die Ausnahmeliste mit 22 Tatbeständen, von Kundenverwaltung und Buchführung bis zur Videoüberwachung. Sie entlastet den Normalbetrieb, ist aber **zweckbezogen, nicht technikbezogen**: Sobald ein KI-Tool auf denselben Daten Bewertung, Prognose, Profilbildung oder Biometrie hinzufügt, verlässt es den beschriebenen Zweck. DSFA-A02 etwa erfasst Bewerberdaten nur, „wenn diese Daten vom Betroffenen angegeben wurden“.

Und aus einer Ausnahme folgt keine Zulässigkeit: Das Bundesverwaltungsgericht stellte am 29. Juni 2022 (W245 2232755-1) klar, dass die Liste über die Rechtmäßigkeit nach Art. 6 DSGVO „überhaupt keine Aussage" trifft.

Typische KI-Einsätze und ihre Einordnung

Die Tabelle ist eine Einordnung unter die zitierten Normen, keine behördliche Beurteilung. Österreichische Judikatur speziell zu DSFA und KI-Tools gibt es nicht; die Bewertung ist im Einzelfall zu treffen.

ANWENDUNGSFALL	EINORDNUNG	TRAGENDE GRUNDLAGE
KI-gestützte Bewerbervorauswahl	DSFA erforderlich	§ 2 Abs. 2 Z 1, Z 4 DSFA-V; Art. 35 Abs. 3 lit. a DSGVO
Leistungsauswertung von Mitarbeitenden	DSFA erforderlich	§ 2 Abs. 2 Z 1, Z 3 lit. a, Z 4; § 2 Abs. 3 Z 4 DSFA-V
KI-Videoanalyse mit Personenerkennung	DSFA erforderlich	§ 2 Abs. 2 Z 3, Z 4 DSFA-V; Art. 35 Abs. 3 lit. c
Bonitätsbewertung	DSFA erforderlich, dazu FRIA ab 2.12.2027	§ 2 Abs. 2 Z 1, Z 2, Z 4, Z 5 DSFA-V; Anhang III Nr. 5 lit. b KI-VO
Transkription, Chatbot, interne Dokumentensuche	Einzelfallprüfung	je nach Inhalt, Auswertung und Berechtigungskonzept
Textgenerierung ohne Personenbezug	keine DSFA, kein Eintrag	DSGVO nicht anwendbar (Art. 2 Abs. 1, Art. 4 Z 1)

Der letzte Fall kippt in der Praxis fast immer, weil Prompts häufiger Personenbezug enthalten als beabsichtigt. Beim Monitoring von Beschäftigten ist die Schwelle umgekehrt fast immer erreicht; die Grenzen dort behandelt der Beitrag zu KI-Tools für Mitarbeiterüberwachung für die deutsche Rechtslage.

Vierschrittige Prozessgrafik zur DSFA-Pflicht bei KI-Tools: Prüfung des Personenbezugs, vorrangige Prüfung der Ausnahmeverordnung DSFA-AV, Kriterien der DSFA-V und abschließend die Risikoprüfung nach Artikel 35 DSGVO.

So läuft eine DSFA für ein KI-Tool praktisch ab

Von der Erfassung bis zur Risikobewertung

#	SCHRITT	GRUNDLAGE
0	**Datenfluss erfassen**, Verzeichniseintrag anlegen oder aktualisieren	Art. 30 Abs. 1 DSGVO
1	Schwellenprüfung dokumentieren — **Art. 35** DSGVO und **die DSFA-V**, vorab die DSFA-AV	Art. 35 Abs. 1 und 3 DSGVO, § 2 DSFA-V
2	Rat der Datenschutzbeauftragten einholen, sofern eine benannt ist	Art. 35 Abs. 2 DSGVO
3	Verarbeitung beschreiben, Notwendigkeit und Verhältnismäßigkeit prüfen	Art. 35 Abs. 7 lit. a und b DSGVO
4	Risiken für die betroffenen Personen nach Wahrscheinlichkeit und Schwere bewerten	Art. 35 Abs. 7 lit. c DSGVO

Auch ein negatives Ergebnis der Schwellenprüfung wird dokumentiert — im Straferkenntnis der Datenschutzbehörde vom 7. Dezember 2023 (2023-0.583.644) war das fehlende Verzeichnis der Punkt, an dem nichts vorgelegt werden konnte. Die Unterlagen für Schritt 3 müssen Sie nicht erfinden: Art. 28 Abs. 3 lit. f DSGVO verpflichtet den Auftragsverarbeiter zur Unterstützung bei den Art. 32 bis 36 DSGVO, und Art. 26 Abs. 9 KI-VO nennt die Anbieterinformationen nach Art. 13 KI-VO als DSFA-Input.

Maßnahmen, Restrisiko und der Review-Termin

An den Abhilfemaßnahmen nach Art. 35 Abs. 7 lit. d DSGVO entscheidet sich, ob eine DSFA trägt oder Formblatt bleibt. Bei KI-Tools wirken erfahrungsgemäß: Zweckbindung samt Ausschluss der Trainingsnutzung, Eingabebeschränkungen, ein Berechtigungskonzept, menschliche Letztentscheidung und Protokollierung. Dazu zählt bei angebundenen Tools die Verbindung selbst, siehe API-Verbindungen in KI-Workflows DSGVO-konform absichern. Auch ein Meldeweg für Datenpannen gehört hinein — eine Struktur dafür liefert der Notfallplan für Datenpannen in KI-Workflows.

Danach folgt der Schritt, der am häufigsten fehlt: die Bewertung des Restrisikos nach Umsetzung der Maßnahmen. Bleibt es hoch, ist nach Art. 36 DSGVO die Datenschutzbehörde zu konsultieren — sonst nicht. Eine Vorlage- oder Meldepflicht für eine „normale“ DSFA gibt es nicht, und ein DSFA-Muster stellt die Behörde ebenfalls nicht bereit; für die Methodik verweist sie auf die Leitlinien des Europäischen Datenschutzausschusses.

Die DSFA ist kein Einmaldokument. Art. 35 Abs. 11 DSGVO verlangt eine Überprüfung zumindest dann, wenn sich das Risiko geändert hat, und WP 248 beschreibt die DSFA als laufenden Prozess. Setzen Sie deshalb einen festen **Review-Termin zur Neubewertung** und zusätzlich Auslöser, die ihn vorziehen: Modellwechsel, neue Funktionen, neue Datenquellen, Anbieterwechsel.

Österreich-Spezifika: Mitbestimmung und Sanktionsrahmen

Bei Beschäftigtenbezug genügt die datenschutzrechtliche Dokumentation nicht. Nach § 96 Abs. 1 Z 3 ArbVG bedürfen technische Systeme zur Kontrolle der Arbeitnehmer, welche die Menschenwürde berühren, zu ihrer **Rechtswirksamkeit** der nicht ersetzbaren Zustimmung des Betriebsrats. § 96a Abs. 1 ArbVG erfasst zusätzlich Systeme zur automationsunterstützten Verarbeitung von Beschäftigtendaten über allgemeine Personalien hinaus und Systeme zur Beurteilung von Arbeitnehmern; dort ist die Zustimmung ersetzbar. Ohne Betriebsrat tritt nach § 10 AVRAG die jederzeit fristlos kündbare Zustimmung der betroffenen Person an ihre Stelle.

Die DSFA ersetzt die Mitbestimmung also nicht; wann zusätzlich eine Betriebsvereinbarung nötig ist, klärt der Beitrag zu Mitarbeiterdaten in KI-Tools und den Betriebsrat-Pflichten in Österreich. Die Verzahnung lohnt doppelt: Die Einbindung der Belegschaftsvertretung erfüllt zugleich Art. 35 Abs. 9 DSGVO, und eine Betriebsvereinbarung kann nach § 2 Abs. 2 DSFA-V entlasten. Führen Sie das Gespräch parallel zur DSFA, nicht danach.

Verstöße gegen Art. 30, 35 und 36 DSGVO fallen nach Art. 83 Abs. 4 lit. a DSGVO in den Rahmen bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes. Weil nach Art. 83 Abs. 3 DSGVO bei verbundenen Verstößen eine Gesamtstrafe im Rahmen des schwerwiegendsten Verstoßes verhängt wird, stand der Dokumentationsmangel in den veröffentlichten österreichischen Verfahren nie allein, und einen bezifferten Teilbetrag dafür nennt keine Entscheidung. Teuer wird es durch die materiellen Verstöße gegen Art. 5, 6 und 9 DSGVO.

Fehler, die wir in Dokumentationen regelmäßig sehen

Bei Strukturaflow sehen wir regelmäßig dieselben Muster:

- **Das Verzeichnis wurde 2018 angelegt und nie wieder angefasst.** Jedes seither eingeführte Tool fehlt — und das sind die riskanten.
- **Die DSFA ist ein ausgefülltes Formblatt.** Der Verwaltungsgerichtshof verlangt in Ro 2025/04/0007 „den Nachweis eines wertenden Abwägens des Verantwortlichen".
- **Die Löschfristen stehen leer.** „Wenn möglich" in Art. 30 Abs. 1 lit. f DSGVO ist keine Freistellung, wenn die Frist ermittelbar ist.
- **Sub-Auftragsverarbeiter fehlen bei den Empfängern.** Die Liste steht im Vertragsanhang, nicht im Marketingmaterial.
- **Der Testbetrieb ist undokumentiert.** Ein Pilot mit echten Kundendaten ist eine Verarbeitung.
- **Es gibt keinen Review-Termin.** Damit veraltet die DSFA beim ersten Modellwechsel.

Wer die Unterlagen prüft und was eine Prüfung kostet, ist keine abstrakte Frage — der Beitrag EU AI Act Audit: wer prüft, wie und was es kostet beschreibt die Zuständigkeiten in Österreich und Deutschland.

Praxis-Tipp: Was ohne eigene Datenschutzbeauftragte realistisch machbar ist

Das Verarbeitungsverzeichnis schaffen Sie intern. Die Informationen liegen im Haus oder im Vertrag, und eine Tabelle mit zehn bis fünfzehn Einträgen ist in zwei konzentrierten Tagen aufgebaut. Dasselbe gilt für die Schwellenprüfung — ein begründetes „keine DSFA erforderlich" ist ein vollwertiges Ergebnis.

Hängen bleibt es an zwei Stellen: an der Risikobewertung aus Sicht der betroffenen Personen, wo ohne Vorerfahrung der Maßstab fehlt — und an der Rollenabgrenzung zum Anbieter. Ob er Auftragsverarbeiter bleibt oder nach Art. 28 Abs. 10 DSGVO zum eigenen Verantwortlichen wird, hängt an Vertragsdetails und Trainingsnutzung, und diese Einordnung trägt die halbe DSFA.

Nächste Schritte

1. **Tool-Inventur anlegen.** Alle genutzten KI-Tools auflisten, auch privat beschaffte Zugänge, und pro Tool den Datenfluss notieren.
2. **Verzeichnis nach Zwecken strukturieren.** Pro Verarbeitungszweck einen Eintrag mit Zweck, Kategorien, Empfänger, Löschfrist anlegen; Drittlandangaben aus dem Vertrag ergänzen.
3. **Schwellenprüfung schriftlich durchführen.** Je Eintrag die Kette DSFA-AV, § 2 Abs. 2 DSFA-V, § 2 Abs. 3 DSFA-V, Art. 35 DSGVO abarbeiten und das Ergebnis datiert ablegen.
4. **Zwei Termine fixieren.** Einen Review-Termin für Verzeichnis und DSFA, bei Beschäftigtenbezug einen mit der Belegschaftsvertretung.

Die Schwellenprüfung in Schritt 3 ist der Punkt, an dem dieser Artikel aufhört: Ob Ihr Tool die Abschätzung der Auswirkungen im Sinne von § 2 Abs. 2 Z 4 DSFA-V tatsächlich erschwert, hängt an Ihrer Konfiguration, an der Trainingsnutzung im Vertrag und daran, wessen Daten in den Prompts landen. Erfahrungsgemäß liegen diese drei Angaben im Haus nicht vollständig vor, bevor jemand das Formular ausfüllt. In der 45-minütigen IT-Sprechstunde von Strukturaflow IT tragen wir sie an Ihren Systemen und Verträgen zusammen, damit die Prüfung trägt — die rechtliche Beurteilung Ihres Falls bleibt bei Ihrer Kanzlei.

FAQ

Reicht ein Auftragsverarbeitungsvertrag mit dem Anbieter aus? Nein. Der Vertrag nach Art. 28 DSGVO regelt das Verhältnis zum Anbieter; Verzeichniseintrag und Schwellenprüfung sind unabhängige Pflichten. Umgekehrt ist er die beste Datenquelle für die Felder „Empfänger“ und „Drittland“.

Wie oft muss das Verzeichnis nachgeführt werden? Eine Frist nennt Art. 30 DSGVO nicht; es muss auf Anfrage aktuell vorlegbar sein. Praktikabel ist ein Jahrestermin plus die Regel, dass jede neue Verarbeitung vor dem Start einen Eintrag erhält. Nachträglich hilft es noch: Laut Bundesverwaltungsgericht vom 3. Juni 2024 (W292 2282284-1) wirkte die späte Erstellung eines Verzeichnisses strafmildernd.

Rechtsstand: 2. Oktober 2026. Tragende Fundstellen: DSGVO (Verordnung (EU) 2016/679), DSG (BGBl. I Nr. 165/1999 idgF), DSFA-V (BGBl. II Nr. 278/2018), DSFA-AV (BGBl. II Nr. 108/2018) und KI-VO (Verordnung (EU) 2024/1689) in der Fassung der Digital-Omnibus-Verordnung (EU) 2026/1744, in Kraft seit 27. Juli 2026. Die FRIA nach Art. 27 KI-VO gilt für Anhang-III-Systeme ab 2. Dezember 2027. Keine Rechtsberatung — bitte prüfen Sie Ihren Fall mit Ihrer Kanzlei.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

https://wissen.strukturaflow.com