

Datenschutz-Folgenabschätzung (DSFA)

gemäß Art. 35 DSGVO · Vorlage & Workflow für KMU · DE

Rechtlich geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E) · Bereitgestellt von ETHYX · Version 1.0 · Juni 2026

» **HINWEIS** Eine DSFA bewertet die Risiken, die eine geplante Verarbeitung für die Rechte und Freiheiten von Personen birgt, sowie die Maßnahmen zu deren Verringerung. Sie ist vor Beginn einer risikoreichen Verarbeitung erforderlich (Art. 35). Arbeiten Sie die Schritte der Reihe nach durch: Schritt 1 klärt, ob überhaupt eine DSFA nötig ist – falls ja, füllen Sie Schritte 2–7 aus. Ersetzen Sie jeden [Platzhalter], füllen Sie die Tabellen aus und lassen Sie das Ergebnis von Ihrem DSB prüfen. Bewahren Sie die fertige DSFA als Nachweis der Rechenschaftspflicht auf (Art. 5 Abs. 2).

Dokumentenkontrolle

FELD	EINTRAG
Verarbeitungstätigkeit / Projekt	[Name des Projekts oder Systems]
Verantwortlicher	[Firmenname]
Ersteller der DSFA	[Name, Funktion]
DSB konsultiert	[Name – siehe Schritt 3]
Begonnen am	[Datum]
Version / Status	[v1.0 – Entwurf / final]

Schritt 1 – Brauchen Sie eine DSFA? (Vorprüfung)

Eine DSFA ist in den Fällen des Art. 35 Abs. 3 DSGVO zwingend und in der Regel erforderlich, wenn zwei oder mehr der nachstehenden EDSA-Kriterien zutreffen. Prüfen Sie die geplante Verarbeitung zunächst vor.

Immer erforderlich (Art. 35 Abs. 3)

#	PFLICHTFALL	ZUTREFFEND?
a	Systematische und umfassende Bewertung/Profiling mit rechtlicher oder ähnlich erheblicher Wirkung	[Ja/Nein]
b	Umfangreiche Verarbeitung besonderer Kategorien (Art. 9) oder von Straftatdaten (Art. 10)	[Ja/Nein]
c	Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche	[Ja/Nein]

EDSA-Risikokriterien (zwei oder mehr → DSFA in der Regel erforderlich)

#	KRITERIUM	ZUTREFFEND?
1	Bewertung oder Einstufung, einschließlich Profiling und Prognose	[Ja/Nein]
2	Automatisierte Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung	[Ja/Nein]

#	KRITERIUM	ZUTREFFEND?
3	Systematische Überwachung	[Ja/Nein]
4	Sensible Daten oder Daten höchstpersönlicher Natur	[Ja/Nein]
5	Verarbeitung in großem Umfang	[Ja/Nein]
6	Abgleich oder Zusammenführung von Datensätzen	[Ja/Nein]
7	Daten schutzbedürftiger Personen (z. B. Kinder, Beschäftigte)	[Ja/Nein]
8	Innovative Nutzung oder Einsatz neuer technischer/organisatorischer Lösungen	[Ja/Nein]
9	Verarbeitung, die Betroffene an der Ausübung eines Rechts oder der Nutzung einer Leistung hindert	[Ja/Nein]

Ergebnis der Vorprüfung: **[DSFA erforderlich – weiter mit Schritt 2 / DSFA nicht erforderlich – diese Schlussfolgerung und Begründung dokumentieren, dann beenden]** .

» **HINWEIS** Im Zweifel führen Sie die DSFA durch – sie ist günstiger als eine Beanstandung. Wenn Sie zu dem Schluss kommen, dass keine DSFA nötig ist, dokumentieren Sie die Begründung; dieser Nachweis ist selbst Teil Ihrer Rechenschaftspflicht.

Schritt 2 – Beschreibung der Verarbeitung

PUNKT	BESCHREIBUNG
Art der Verarbeitung	[was mit den Daten geschieht: Erhebung, Nutzung, Speicherung, Weitergabe, Löschung]
Umfang	[Menge und Vielfalt der Daten, Zahl der Betroffenen, geografische Reichweite, Speicherdauer]
Zusammenhang	[Beziehung zu den Personen, ihre Erwartungen, frühere Bedenken, Stand der Technik]
Zwecke	[was erreicht werden soll; beabsichtigte Wirkung auf Personen; der Nutzen]
Datenarten	[Kategorien personenbezogener Daten, inkl. besonderer Kategorien]
Betroffene Personen	[wessen Daten: Kunden, Mitarbeitende usw.]
Empfänger / Auftragsverarbeiter	[wer die Daten erhält; beteiligte Auftragsverarbeiter]
Drittlandübermittlungen	[Übermittlung außerhalb EU/EWR + Garantie]

Schritt 3 – Konsultation

Dokumentieren Sie den Rat des DSB sowie die Standpunkte relevanter Beteiligter und, soweit angebracht, der betroffenen Personen (Art. 35 Abs. 2, Abs. 9).

KONSULTIERT	BEITRAG / RAT	DATUM
Datenschutzbeauftragter	[dokumentierter Rat des DSB]	[Datum]
Interne Beteiligte	[IT / Sicherheit / Fachbereich]	[Datum]
Betroffene Personen (falls angebracht)	[wie ihre Sicht eingeholt wurde, oder warum nicht]	[Datum]

Schritt 4 – Notwendigkeit und Verhältnismäßigkeit

FRAGE	BEWERTUNG
Rechtsgrundlage (Art. 6)	[welche Grundlage und warum passend]
Zweckbindung	[Daten nur für den genannten Zweck genutzt?]
Datenminimierung	[ist jedes Datum erforderlich? was wurde ausgeschlossen?]
Richtigkeit & Speicherdauer	[wie aktuell gehalten; wie lange; Löschung]
Betroffenenrechte	[wie Auskunft, Berichtigung, Löschung, Widerspruch unterstützt werden]
Auftragsverarbeiter	[AVV nach Art. 28 vorhanden? Garantien?]
Drittlandübermittlungen	[Garantie dokumentiert?]

Schritt 5 – Risiken identifizieren und bewerten

Bewerten Sie für jedes Risiko für die Rechte und Freiheiten der Personen die Eintrittswahrscheinlichkeit und die Schwere und lesen Sie das Gesamtrisiko aus der folgenden Matrix ab.

EINTRITT ↓ / SCHWERE →	GERING	ERHEBLICH	SCHWER
Entfernt	Niedrig	Niedrig	Mittel
Möglich	Niedrig	Mittel	Hoch
Wahrscheinlich	Mittel	Hoch	Hoch

#	RISIKO FÜR DIE PERSONEN	EINTRITT	SCHWERE	GESAMTRISIKO
1	[z. B. unbefugter Zugriff auf Kundendaten]	[Entfernt/Möglich/Wahrscheinlich]	[Gering/Erheblich/Schwer]	[Niedrig/Mittel/Hoch]
2	[z. B. Daten länger als nötig gespeichert]	[]	[]	[]
3	[z. B. Zweckentfremdung – Daten für neuen Zweck genutzt]	[]	[]	[]
4	[]	[]	[]	[]

Schritt 6 – Maßnahmen zur Risikoverringering

RISIKO-NR.	MAßNAHME ZUR VERRINGERUNG ODER BESEITIGUNG DES RISIKOS	WIRKUNG	RESTRISIKO	GENEHMIGT
1	[z. B. MFA + Verschlüsselung im Ruhezustand; rollenbasierter Zugriff]	[Beseitigt/Verringert/Akzeptiert]	[Niedrig/Mittel/Hoch]	[Ja/Nein]
2	[z. B. automatisierter Löschanplan]	[]	[]	[]
3	[z. B. strikte Zweckbindung + Änderungskontrolle]	[]	[]	[]
4	[]	[]	[]	[]

Schritt 7 – Freigabe und Ergebnis dokumentieren

PUNKT	ERGEBNIS
Rat des DSB	[erteilter Rat – angenommen / abgewichen, mit Begründung]
Restrisiko	[Gesamt-Restrisiko nach Maßnahmen: Niedrig / Mittel / Hoch]
Vorherige Konsultation (Art. 36)	[erforderlich? Ja, wenn ein hohes, nicht zu minderndes Restrisiko verbleibt – Aufsichtsbehörde vor der Verarbeitung konsultieren]
Maßnahmen genehmigt von	[Name, Funktion, Datum]
Überprüfungsdatum	[wann die DSFA überprüft wird, z. B. jährlich oder bei Änderung]

» **HINWEIS** Verbleibt ein hohes Restrisiko, das Sie nicht mindern können, müssen Sie vor Beginn der Verarbeitung Ihre Aufsichtsbehörde konsultieren (Art. 36 DSGVO). Andernfalls geben der DSB und der verantwortliche Owner frei, und Sie überprüfen die DSFA bei jeder Änderung der Verarbeitung.

Diese Vorlage dient ausschließlich zur Orientierung und stellt keine Rechtsberatung dar. Geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E) · ETHYX · ethyx.eu