DSFA-Mustervorlage

Systematische Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO mit Schwellwertanalyse, Risikobewertung und Dokumentation aller Mindestinhalte für rechtssichere Compliance bei Hochrisiko-Verarbeitungen.

Diese Vorlage unterstützt Sie bei der strukturierten Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Füllen Sie alle Abschnitte aus und dokumentieren Sie Ihre Bewertungen.

Schritt 1: Notwendigkeitsprüfung

- ☐ Verarbeitungsvorgang auf Muss-Liste der Aufsichtsbehörde geprüft
- ☐ Falls nicht auf Muss-Liste: Schwellwertanalyse (9 Kriterien) durchgeführt

Ergebnis: ☐ DSFA erforderlich ☐ DSFA nicht erforderlich

Schritt 2: Schwellwertanalyse (9 Kriterien)

Faustregel: Treffen mindestens 2 Kriterien zu, ist eine DSFA erforderlich.

- ☐ Scoring/Profiling: Bewertung, Einstufung oder Vorhersage von Verhalten
- ☐ Automatisierte Entscheidung mit Rechtswirkung oder erheblicher Beeinträchtigung
- ☐ Systematische Überwachung (z. B. kontinuierliche Videoüberwachung)
- ☐ Besondere Datenkategorien (Gesundheit, Biometrie, genetische Daten, etc.)
- ☐ Großer Umfang (große Personenanzahl oder große Datenmengen)
- ☐ Zusammenführung von Datensätzen aus verschiedenen Quellen
- ☐ Daten schutzbedürftiger Personen (Kinder, Beschäftigte, Patienten)
- ☐ Innovative Nutzung neuer Technologien (KI, Gesichtserkennung, IoT)
- ☐ Verhinderung von Rechtsausübung oder Dienstnutzung

Anzahl zutreffender Kriterien: _____ (≥2 = DSFA erforderlich)

Schritt 3: DSFA-Dokumentation

3.1 Systematische Beschreibung der Verarbeitung

- ☐ Welche Daten werden verarbeitet? (Datenkategorien aufgelistet)
- ☐ Von wem? (Verantwortlicher, Auftragsverarbeiter benannt)
- ☐ Wie? (Verarbeitungsprozesse beschrieben)
- ☐ Wo? (Speicherorte, Drittlandtransfers dokumentiert)
- ☐ Zu welchem Zweck? (Verarbeitungszwecke konkret benannt)

3.2 Bewertung der Notwendigkeit und Verhältnismäßigkeit

- ☐ Ist die Verarbeitung zur Zweckerreichung erforderlich?
- ☐ Gibt es weniger eingriffsintensive Alternativen?
- ☐ Rechtsgrundlage geprüft und dokumentiert

3.3 Risikobewertung für Rechte und Freiheiten

- ☐ Welche Gefährdungen bestehen? (Risiken identifiziert)
- ☐ Eintrittswahrscheinlichkeit bewertet (gering / mittel / hoch)
- ☐ Schwere des Schadensfalls bewertet (gering / mittel / hoch)
- ☐ Gesamtrisiko ermittelt (Wahrscheinlichkeit × Schwere)

3.4 Geplante Abhilfemaßnahmen (TOM)

- ☐ Technische Maßnahmen dokumentiert (Verschlüsselung, Zugriffskontrolle, etc.)
- ☐ Organisatorische Maßnahmen dokumentiert (Schulungen, Richtlinien, etc.)
- ☐ Garantien und Sicherheitsvorkehrungen beschrieben
- ☐ Restrisiko nach Maßnahmen bewertet

3.5 Nachweis der Einhaltung der DSGVO

- ☐ Datenschutzgrundsätze eingehalten (Art. 5 DSGVO)
- ☐ Betroffenenrechte gewährleistet (Art. 15-22 DSGVO)
- ☐ Dokumentation vollständig und nachvollziehbar

Schritt 4: DSB-Beteiligung & Prüfung

- ☐ Datenschutzbeauftragter (DSB) eingebunden (Art. 35 Abs. 2 DSGVO)
- ☐ DSB hat Stellungnahme abgegeben
- ☐ Falls Restrisiko hoch: Aufsichtsbehörde vorab konsultiert (Art. 36 DSGVO)
- ☐ Überprüfungszyklus festgelegt (spätestens alle 3 Jahre)

Abschließende Dokumentation

Verantwortlicher: _____

DSB-Stellungnahme vom: _____

DSFA-Ergebnis: ☐ Risiken akzeptabel ☐ Behörde konsultiert

Nächste Überprüfung: _____

Wichtig: Eine DSFA ist bei hohem Risiko gemäß Art. 35 DSGVO verpflichtend. Bei fehlender oder mangelhafter DSFA drohen Bußgelder. Diese Vorlage ersetzt keine individuelle Datenschutzberatung.