DAXAIS
Struktur für Sicherheit. Klarheit für KI.

DSFA,DATENSCHUTZ,PROZESSSICHERHEIT,KI-EINSATZ

Leitfaden Datenschutzfolgeabschätzung (DSFA)

Praxisleitfaden für Datenschutzbeauftragte zur strukturierten Durchführung und Dokumentation einer DSFA anhand klarer Schritte und Rollen.

Struktur für Sicherheit. Klarheit für KI.

Zielgruppe: Datenschutzbeauftragte, Verantwortliche für Datenschutz in Unternehmen

Stand August 2026

ORIENTIERUNG

Worum es geht

Dieser Leitfaden liefert Datenschutzbeauftragten eine nachvollziehbare, dokumentierbare Schritt-für-Schritt-Anleitung für die Datenschutzfolgeabschätzung (DSFA) - unabhängig vom Einzelfall oder KI-Bezug.

NAVIGATOR

Drei Orientierungspunkte

Art. 35 DSGVO

Rechtsgrundlage DSFA

Vier Stufen

Empfohlener Ablauf

Pflicht

Dokumentation je Projekt

CHECKLIST

1. Prüfen der DSFA-Pflicht

Bewerten Sie gezielt, ob und warum die geplante Datenverarbeitung eine DSFA erfordert - unter Einbezug etablierter Prüfschemata.

- Verarbeitungszweck im Projektdokument klar beschreiben.
- Risikofaktoren mit aktuellen Behördenlisten abgleichen.
- Betroffene Personengruppen und Datenarten präzise benennen.
- Vernetzungsgrad und Empfindlichkeit der Daten bewerten.

CHECKLIST

[ ] DSFA-Prüfblatt
Indikatorfragen zur

[ ] Scoping-Feld
Projektskizze mit

[ ] Behördencheck
Vergleich mit Art.

MERKSATZ

Begründete DSFA-Pflicht-Entscheidung schafft Audit-Transparenz.

PROCESS

2. Strukturierte Risikoidentifikation

Erfassen Sie sämtliche Risiken für Betroffene entlang aller Verarbeitungsabschnitte. Dokumentieren Sie externe Dienste und technische Maßnahmen.

- Datenwege in Diagrammen mit Datentypen abbilden.
- TOMs pro Abschnitt separat listen und belegen.
- Drittlandübertragungen und externe Dienstleister aufführen.
- Risiken je Abschnitt tabellarisch erfassen und priorisieren.

PROCESS

Flussdiagramm
Visualisierung von

TOM-Checkliste
Maßnahmen- und

Risiko-Tab
Risiken je

MERKSATZ

Strukturierte Risikoanalyse sichert Revisionsfähigkeit.

MATRIX

3. Bewertung und Maßnahmenentwicklung

Prüfen Sie, wie schwer die einzelnen Risiken wiegen, begründen Sie Bewertungen und dokumentieren Sie abgeleitete Schutzmaßnahmen.

- Risikoausmaß und Eintrittswahrscheinlichkeit numerisch einstufen.
- Maßnahmen nach Wirksamkeit und Aufwand priorisieren.
- Restrisiken samt Begründung offenzulegen.
- Bewertung durch Datenschutzteam revisionieren lassen.

MATRIX

Risiko-Stufen

Matrix mit Bewertungskrite-rien

Maßnahmenplan

Tabellarischer Maßnahmenkatalog

Restrisiko-Na-chweis

Dokumentierte Restgefahren

MERKSATZ

Nur gründlich bewertete Maßnahmen sind auditfest.

TIMELINE

4. Konsultation und Dokumentation

Erstellen Sie einen vollständigen DSFA-Bericht. Konsultieren Sie - bei hohem Restrisiko - die zuständige Aufsichtsbehörde, unter Einbindung der relevanten Teams.

- DSFA-Bericht mit Anlagen und Verantwortlichen abschließen.
- Fachbereiche, Betriebsrat und Betroffene einbeziehen.
- Behördliche Konsultationspflicht anhand Restrisiko prüfen.
- DSFA-Dokumentation revisionssicher ablegen und laufend pflegen.

TIMELINE

DSFA-Report

Gliederung für

Freigabe-Workstep

Schritte zur

Audit-Trail

Konsultationsdokument-

MERKSATZ

Lückenlose Berichtsführung beugt Rückfragen Dritter vor.

FOCUS

5. Umsetzung und Nachjustierung

Überwachen Sie die Wirksamkeit der getroffenen Maßnahmen regelmäßig und dokumentieren Sie Anpassungen.

- Wirksamkeitschecks jährlich terminieren und protokollieren.
- Anpassungen bei Prozessänderungen sofort dokumentieren.
- DSFA-Bericht nach Update neu genehmigen lassen.
- Schulungen zum DSFA-Verfahren jährlich durchführen.

FOCUS

Jahresprüfung

Prüfprotokoll nach

Update-Tracker

Kontinuierliche

Schulungsnachweis

Nachweise zu Trainings

MERKSATZ

DSFA ist dynamisch - regelmäßiges Nachsteuern senkt Risiken.

MUSTERBEISPIEL

Musterbeispiel: DSFA für KI-gestützte Bewerberauswahl

AUSGANGSLAGE

Ein Mittelständler plant ein KI-Modul für die automatisierte Erstselektion von Bewerberprofilen.

1. Pflicht zur DSFA anhand Landesaufsichtsbehörde geprüft und dokumentiert.
2. Datenflüsse zwischen HR, KI-System und Fachabteilung skizziert.
3. Risiken wie Diskriminierung, Fehlklassifikation, Kontrollverlust ausgewiesen.
4. Maßnahmen (bspw. Transparenz, Widerspruch, Überprüfung durch HR-Personal) festgelegt.
5. DSFA abgeschlossen, Maßnahmenstatus im jährlichen Review dokumentiert.

ERGEBNIS

KI-basierte Auswahl eingeführt, alle DSFA-Nachweise bereitgestellt. Nachfragen der Landesaufsicht konnten mit Bericht und Maßnahmenplan beantwortet werden.

ARBEITSBLATT

Umsetzungscheckliste

- [ ] Verarbeitungszweck fachlich belegt und dokumentiert?
- [ ] Prüfung der DSFA-Pflicht mit Behördenliste abgeglichen?
- [ ] Datenarten und betroffene Personengruppen vollständig erfasst?
- [ ] Technische Maßnahmen und Datenflüsse visualisiert?
- [ ] Risiken geprüft und explizit bewertet?
- [ ] Risiko-Minderungsmaßnahmen dokumentiert?
- [ ] Restrisiken konkret begründet?
- [ ] Fachbereiche, Betriebsrat und DSB beteiligt?
- [ ] Konsultationspflicht bei Restrisiko geprüft?
- [ ] Berichte und Nachweise systematisch abgelegt?
- [ ] Aktualisierung und jährliche Prüfung terminiert?
- [ ] Schulungsstatus und Maßnahmen-Reviews dokumentiert?

DAXAIS
Struktur für Sicherheit. Klarheit für KI.

Nächster Schritt

Durch strukturierte DSFA gelingt Transparenz und Nachweisfähigkeit für datenintensive Verfahren wie KI-Anwendungen.

WEITERFÜHRENDE ORIENTIERUNG

Gesetzesbibliothek · KI-Risikobibliothek · DAXAIS Academy

www.daxais.de