

Kurze Checkliste für eine Datenschutzfolgenabschätzung (DSFA)

gem. Art. 35 DSGVO für digitale Archive

Inhalt

I. Prüfung der Erforderlichkeit einer DSFA (Schwellwertanalyse).....	1
I.1 Prüfprozess.....	1
Schritt 1: Abgleich mit den Positiv- und Negativ-Listen geprüfter Verarbeitungsvorgänge der Datenschutzaufsichtsbehörde.....	1
Schritt 2: Prüfung allgemeiner Ausschlusskriterien	2
Schritt 3: Prüfung erhöhter Risiken gem. Art. 35 Abs. 3 DSGVO.....	2
I.2 Begründung und Dokumentation der Ergebnisse der Schwellwertanalyse.....	3
II. Durchführung der DSFA.....	3
II.1 Organisatorische Vorbereitung	3
II.2 Durchführung der DSFA.....	4
III. Vorgehen nach dem Abschluss der DSFA.....	5

I. Prüfung der Erforderlichkeit einer DSFA (Schwellwertanalyse)

Eine DSFA ist gem. Art. 35 Abs. 1 DSGVO durchzuführen, wenn die Form der Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge hat. Der diesbezüglich zu prüfende Verarbeitungsvorgang umfasst dabei Hardware, Software und die verarbeiteten Daten.

I.1 Prüfprozess

Schritt 1: Abgleich mit den Positiv- und Negativ-Listen geprüfter Verarbeitungsvorgänge der Datenschutzaufsichtsbehörde

Die jeweilige Datenschutzaufsichtsbehörde veröffentlicht gem. Art 35 Abs. 4 DSGVO obligatorisch eine Liste derjenigen Verarbeitungsvorgänge, für die eine DSFA *zwingend erforderlich* ist (Blacklist) und gem. Art. 35 Abs. 5 optional eine Liste derjenigen Verarbeitungsvorgänge, für die eine DSFA *nicht erforderlich* ist (Whitelist).

1. Listet die Blacklist der zust. Datenschutzaufsichtsbehörde gem. Art. 35 Abs. 4 DSGVO das Verfahren der digitalen Archivierung als solches auf oder die dabei zur Anwendung kommenden Verarbeitungsprozesse?

=> **DSFA erforderlich => weiter mit Punkt II**

2. Gibt es eine Whitelist der zust. Datenschutzaufsichtsbehörde gem. Art. 35 Abs. 5 DSGVO, die die digitale Archivierung oder die dabei zur Anwendung kommende Verarbeitungsprozesse auflistet?
 => **keine DSFA erforderlich => Ende der Schwellwertanalyse**
3. Werden die digitale Archivierung als solche oder die dabei zur Anwendung kommenden Verarbeitungsprozesse weder auf einer Black- noch auf einer Whitelist der zust. Datenschutzaufsichtsbehörde genannt?
 => **Fortsetzung der Schwellwertanalyse => weiter mit Schritt 2, Punkt 4**

Schritt 2: Prüfung allgemeiner Ausschlusskriterien

4. Gibt es im jeweiligen Datenschutzgesetz des Bundes bzw. des Landes eine Öffnungsklausel, dass eine DSFA nicht mehr erforderlich ist, wenn diese bereits durch eine andere (öffentl.) Stelle oder im Rahmen eines Gesetzgebungsverfahrens durchgeführt wurde?
 => **keine DSFA erforderlich, wenn eine entsprechende DSFA bereits durchgeführt wurde => Ende der Schwellwertanalyse**
5. Wurde bereits eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken gem. Art. 35 Abs. 1 DSGVO durchgeführt?
 => **keine spezielle DSFA erforderlich => Ende der Schwellwertanalyse**

Schritt 3: Prüfung erhöhter Risiken gem. Art. 35 Abs. 3 DSGVO

6. Handelt es sich beim Verarbeitungsvorgang um eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen?
 => **DSFA erforderlich => weiter mit Punkt II**
7. Handelt es sich beim Verarbeitungsvorgang um eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO?
 => **DSFA erforderlich => weiter mit Punkt II**
8. Risikoeinschätzung, ob der geplante Verarbeitungsvorgang voraussichtlich ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge hat. Dabei sind die folgenden Fragen abzuklären:
 - a) Findet ein sogen. Scoring statt, d.h. umfasst die Verarbeitungstätigkeit eine Bewertung und Einstufung der betroffenen Personen (Erstellen von personenbezogenen Profilen, Prognosen etc.)?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**
 - b) Erfolgt durch die Verarbeitungstätigkeit eine komplett automatisierte oder in entscheidenden Teilen automatisierte Entscheidungsfindung, die qualifiziert ist, dass sie mit Rechtswirkung oder in ähnlich erheblicher Weise auf natürliche Personen einwirkt?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**
 - c) Werden besonders vertrauliche und höchstpersönliche Daten im Sinne Art. 9 Abs. 1 DSGVO, Art. 35 Erstes Buch Sozialgesetzbuch oder Finanzdaten des Betroffenen verarbeitet?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**
 - d) Handelt es sich um Big Data, d.h. um eine Datenverarbeitung in großem Umfang hinsichtlich der kumulativ zu betrachtenden Faktoren Personenanzahl, Datenumfang, Dauerhaftigkeit und geografischer Reichweite?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**

- e) Verknüpfung und Verkettung der Daten, d.h. findet ein für die betroffenen Personen nicht zu erwartendes Abgleichen oder Zusammenführen von Daten aus unterschiedlichen Verarbeitungsvorgängen / Verarbeitungszwecken / Verantwortlichkeiten statt?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**
- f) Werden überwiegend Daten von besonders schutzbedürftigen Personen (insbes. von Kindern) gem. Erwägungsgrund 75 DSGVO verarbeitet?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**
- g) Werden nach dem aktuellen Stand der Technik neue Technologien oder neue organisatorische Lösungen eingesetzt, deren Auswirkungen auf die Betroffenen daher nur schwer abschätzbar sind?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**
- h) Findet die Verarbeitung außerhalb des Europäischen Wirtschaftsraumes statt?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**
- i) Hindert der Verarbeitungsvorgang selbst die betroffenen Personen an der Ausübung eines Rechts, der Nutzung einer Dienstleistung oder der Durchführung eines Vertrags?
 => **Erfordernis einer DSFA gestiegen => bei (mehrfachen) Vorkommen weiter mit Punkt II**

Je mehr Prüfkriterien zutreffen, desto wahrscheinlicher ist die Erfordernis einer DSFA (Daumenregel). Aber es kann auch schon ein einziges Prüfkriterium ausreichen, wenn die Schwere der Risiken und deren Eintrittswahrscheinlichkeit hoch sind. => Als Faustregel wird daher empfohlen ab mindestens zwei Prüfkriterien eine DSFA durchzuführen (weiter mit Punkt II)

I.2 Begründung und Dokumentation der Ergebnisse der Schwellwertanalyse

Das positive oder negative Ergebnis des Prüfprozesses zur Erfordernis einer DSFA ist nebst der Begründung zu dokumentieren.

II. Durchführung der DSFA

Bei einer positiven DSFA-Erforderlichkeitsprüfung ist eine DSFA durchzuführen. Die DSFA ist ggf. mehrfach durchzuführen, wenn sich die Risiken für die Rechte und Freiheiten natürlicher Personen hinsichtlich Art, Umfang und Zwecken der Verarbeitung ändern. Es empfiehlt sich die (Fach)-Sicherheitskonzepte für das jeweilige digitale Archiv für die DSFA nachzunutzen, da sich bestimmte Bereiche stark ähneln (z.B. Risikomatrix).

II.1 Organisatorische Vorbereitung

- Bestimmung einer Arbeitsgruppe / Verantwortlichkeiten für die Durchführung der DSFA

Für eine DSFA werden unterschiedliche (archiv)fachliche, informationstechnische und rechtliche Kompetenzen benötigt, weshalb sich die Einrichtung einer eigenen interdisziplinären Arbeitsgruppe empfiehlt. Insbesondere ist die Durchführung einer DSFA aber eine organisatorische Aufgabe (Projektmanagement, Führung). Die Einbindung der Amtsleitung, der fachlichen und technischen Leitung des digitalen Archivs sowie die behördlichen Datenschutzbeauftragten werden daher empfohlen.

- Auswahl der Erstellungsmethode für die DSFA

Die Erstellungsmethode kann frei gewählt werden: Beispielhaft ist für Deutschland das Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder unter <https://www.datenschutzzentrum.de/sdm/>

- Erstellung eines Prüfplans

Der Projektplan (Prüfplan) benennt die konkreten Meilensteine, Aufgaben und Arbeitspakete zur Durchführung der DSFA.

II.2 Durchführung der DSFA

Gem. Art. 35 Abs. 7 DSGVO muss eine DSFA zumindest enthalten:

- Systematische Beschreibung der Verarbeitungsvorgänge, von deren Zwecken und der berechtigten Interessen die von den Verantwortlichen verfolgt werden gem. Art. 35 Abs. 7 lit. a.
- Architekturbeschreibung des IT-Gesamtsystems (Hard- und Softwarekomponenten) / Netzplan
 - Beschreibung der Datenflüsse und Übertragungswege
 - Erfassung der Verantwortlichen, Auftragsverarbeitenden, Betroffenen und weiteren Betroffenen
 - Dokumentation der einschlägigen Rechtsgrundlagen für die Verarbeitungsvorgänge
- Zweckorientierte Bewertung der Notwendigkeit und Verhältnismäßigkeit der beschriebenen Verarbeitungsvorgänge unter Berücksichtigung der erhobenen Rechtsgrundlagen.
- Bewertung der sich aus den Verarbeitungsvorgängen ergebenden Risiken für die Rechte und Freiheiten natürlicher Personen gem. Art. 35 Abs. 1 DSGVO
- Identifikation und Beschreibung der Risikoquellen (menschlich und nicht-menschlich)
 - Risikoanalyse: besteht durch Art, Umfang, Umstände und Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen
 - Risikobeurteilung (Risikomatrix aus Schwere des Schadens vs. Eintrittswahrscheinlichkeit)
- Abhilfemaßnahmen zur Reduktion der Risiken für die Rechte und Freiheiten natürlicher Personen in Form der Verarbeitung personenbezogener Daten und zur Einhaltung der DSGVO
- Festlegung der Maßnahmen, Garantien, Vorkehrungen und Verfahren

III. Vorgehen nach dem Abschluss der DSFA

- Umsetzung der Abhilfemaßnahmen
- Erstellung eines DSFA-Berichts gem. Art. 5 Abs. 2 DSGVO
- Regelmäßige Evaluation und ggf. Wiederholung des DSFA