Anforderungskatalog an ein SDM-Tool

Unterarbeitsgruppe Standard-Datenschutzmodell, Version 1.0

Mit dieser Übersicht sollen die wesentlichen fachlichen Hauptfunktionen eines SDM-Tools („Tool“) aus Sicht des Datenschutzes dargestellt werden.

0. Prämissen

- Abgrenzung des Tools zur Vorgangsbearbeitung:
  Im Tool sollen grundsätzlich **keine personenbezogenen Daten** verarbeitet werden. Das bedeutet zum Beispiel, dass die Dokumentation der konkreten Ausübungen von Betroffenenrechten im Vorgangsbearbeitungssystem der verarbeitenden Stelle und nicht im Tool dokumentiert wird. Ausnahmsweise kommt die Verarbeitung personenbezogener Daten von fachlichen und administrativen Tool-Benutzern in Betracht (z.B. Berechtigungskonzept, Wiedervorlagen, Aufgabenlisten).
- Ein wesentliches Charakteristikum eines SDM-Tools besteht darin, die normativen Anforderungen der DSGVO auf funktionale Anforderungen mit Hilfe der SDM-Modellierungskomponenten – Mindestbestandteile: sieben Gewährleistungsziele; Verarbeitungsanalyse mit den Komponenten Daten, IT-Systeme und Prozesse; zwei Risikostufen (absehbar: Darstellung der Verarbeitung entlang der Verarbeitungsvorgänge von Art. 4 Nr. 2 DSGVO – für eine Verarbeitung mit Personenbezug abzubilden. Der Zweck der Maßnahmen besteht darin, die Eingriffsintentisität einer Verarbeitung auf das nur erforderliche Maß abzumildern.
- Das SDM-Tool sollte im Kontext eines DSM(S) einen wesentlichen Beitrag leisten können.
- Vernetzung: Die im Folgenden angesprochenen Objekte sollten ihrem Kontext entsprechend im Tool miteinander verknüpfbar sein.

Ein SDM-Tool sollte die folgende Aktivitäten unterstützen: Output-Sicht, Assistenten-Sicht, externe Quellen-Sicht, Schnittstellen-Sicht und „Effizienz“-Sicht. Das kann im Einzelnen bedeuten:

1. Dokumentation datenschutzrechtlicher Nachweise („Output-Sicht“ des Tools)

1.1 Vollständige, aktuelle und rechtskonforme Beschreibung alle relevanten Verarbeitungen

Alle Verarbeitungen, für welche die Tools einsetzende Stelle verantwortlich (Art. 4 Nr. 7 DS-GVO) oder als Auftragsvererbeiter zuständig ist (Art. 4 Nr. 8 DS-GVO), können in dem Tool rechtskonform beschrieben und geeignet ausgegeben werden. Dabei ist insbesondere eine Unterscheidung der Verarbeitung im Rahmen von Verarbeitungstätigkeiten (Art. 30 DS-GVO) und von Betriebsmitteln, die diese Verarbeitungstätigkeiten unterstützen, möglich.

1.2 DSFA-Erforderlichkeitsprüfung

Die durchgeführte Prüfung des Verantwortlichen, ob für eine Verarbeitungstätigkeit eine Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO erforderlich ist, kann mit den gespeicherten Informationen in dem Tool nachgewiesen werden.

1.3 Bericht der Datenschutz-Folgenabschätzung (DSFA)

Die durchgeführten bzw. zu eigen gemachten Datenschutz-Folgenabschätzungen können mit den gespeicherten Informationen in dem Tool nachgewiesen werden (DSFA-Bericht).

1.4 Nachweise für die rechtskonforme Festlegung und Nutzung von Mitteln

Mit den gespeicherten Informationen in dem Tool können Zertifizierungen, datenschutzrechtliche Risikoanalysen usw. als Nachweis für die rechtkonforme „Art und Weise“ der Verarbeitung nachgewiesen werden.

1.5 Erfüllung der Informationspflicht

Mit den gespeicherten Informationen in dem Tool kann die Erfüllung der Informationspflichten (Art. 14, 15 DS-GVO) nachgewiesen werden.

1.6 (...)

2. Die Durchführung datenschutzrechtlicher Prozesse („Assistenten-Sicht“ des Tools)

2.1 Erforderlichkeit einer DSFA prüfen

Das Tool unterstützt bei der Durchführung der notwendigen Schritte für die Erstellung einer DSFA-Erforderlichkeitsprüfung inkl. der Durchführung der Schwellwertanalyse (gem. Muss-Liste, Art. 29-WP248, tiefergehende Begründung gem. Kriterien aus Art. 24 DSGVO).

2.2 DSFA durchführen (wenn hohes Risiko)

Das Tool unterstützt bei der Durchführung der notwendigen Schritte für die Erstellung einer DSFA. Dabei werden insbesondere folgende Aspekte berücksichtigt:

- Assistenz bei Durchführung einer DSFA nach Art. 35 (DSK-Kurzpapier Nr. 5, SDM-Baustein "Planen und Spezifizieren")
- grundrechtsorientierte Risikomodellierung mit SDM, die von der Verarbeitung und ihrem Eingriffsrisiko ausgeht (Risiko: Grundrechtseingriff zu intensiv, Risikokriterien: Gewährleistungsziele und "Kap. B", Hauptangreifer: Die eigene Organisation)
- Anbindung von Maßnahmenauswahl entsprechend Risikostufe (SDM: generische Methoden, Bausteine, bei Lücken: ITGS)

2.3 Nachweis erstellen (wenn kein hohes Risiko)

- Unterstützung entsprechend Ablauf nach Baustein "Planen und Spezifizieren", bei Lücken: ITGS
- Anbindung von Maßnahmenauswahl entsprechend Risikostufe (SDM: generische Methoden, Bausteine)

2.4 Datenschutzvorfälle bearbeiten

Das systematische Vorgehen bei Verletzungen des Schutzes personenbezogener Daten (Art. 33, 34 DS-GVO) inkl. ihrer jeweiligen Risikobeurteilung, Meldung sowie ggf. den dadurch verursachten Benachrichtigungen und weitere relevante Datenschutzvorfälle werden durch das Tool unterstützt; der personenbezogene Einzelfall wird nicht im Tool, sondern i.d.R. im Vorgangsverarbeitungssystem der Stelle dokumentiert.

2.5 Herausgabeersuchen von Sicherheitsbehörden bearbeiten

Schrittweise Unterstützung des Prozesses, wenn Sicherheitsbehörden die Herausgabe personenbezogener Daten fordern; Dokumentation nach Abschluss dieses Prozesses entlang „lessons learned“.

2.6 Auskunftsersuchen beantworten

Das Tool unterstützt bei der Durchführung der notwendigen Schritte für die Beantwortung eines Auskunftsersuchens, ohne jedoch den einzelnen Vorgang personenbezogen zu dokumentieren.

2.7 (…)

3. Anforderungsbereich: Externe Bausteine werden im Tool bereitgestellt („Externe Quellen-Sicht“ des Tools)

- Schnittstelle zu den SDM-Bausteinen vorhalten
- Schnittstelle zum Maßnahmen-Katalog des IT-Grundschutzes vorhalten
- Schnittstellen zu Rechtsgrundlagen vorhalten
- (…)

4. Anforderungsbereich: Schnittstellen zu anderen Fachverfahren werden bereitgestellt („Schnittstellen-Sicht“ des Tools)

- Schnittstelle zu einem Maßnahmenmanagement-System vorhalten
- Schnittstelle zu einem DSMS vorhalten
- Schnittstelle zu einem ISMS vorhalten.
- Schnittstelle zu einem Wissensmanagement-System (z.B. Literaturfundstellen)
- (…)

5. Anforderungsbereich: Weitere, allgemeine Anforderungen werden angeboten („Effizienz-Sicht“ des Tools)

5.1 Arbeitstabellen erstellen und abarbeiten („ToDo-/ Aufgaben-Liste)

5.2 Wiedervorlagen erstellen

5.3 Kommentierung/Rückmeldung zu Entwürfen abhandeln und dokumentieren

5.4 Verwaltung von Konzepten

- IT-Konzept,
- Datenschutzkonzept,
- Sicherheitskonzept,
- Betriebskonzept

6. Wünschbare nicht-funktionale Eigenschaften

6.1 Betrieb: Mobile- und Offline-Fähigkeit

6.2 Zusatzfunktionen: Benutzerverwaltung

6.3 Technik: betriebssystemunabhängig (generell geringe Abhängigkeiten), gute Code-Qualität, Open-Source, ressourcenschonend, kompatibel mit älteren Systemen