E3 Vorgenommene Änderungen von SDM-Versionen

E3.1 Änderungen von V1.1 auf V2.0 (Stand 5.11.2019)

Die Version SDM 2.0 umfasst nun fünf Teile:

A – Beschreibung des SDM,
B – Zusammenstellung der Anforderungen der DS-GVO,
C – Systematisierung der Anforderungen der DS-GVO durch Gewährleistungsziele,
D – Praktische Umsetzung,
E – Organisatorische Rahmenbedingungen, Betriebskonzept, History, Referenzmaßnahmen- Katalog.

Der Teil A beschreibt Zweck, Anwendungsbereich und Struktur des Modells, an denen sich gegenüber der Vorversion inhaltlich nichts geändert hat. Das SDM umfasst sieben Gewährleistungsziele, eine Strategie zur Abstufung von Risiken bzw. Schutzbedarfen sowie die drei funktionale Komponenten einer Verarbeitungstätigkeit. Neu ist, dass die in der DS- GVO genannten „Dienste“ die „IT-Systeme“ ergänzen.

Der Teil B stimmt das SDM V2.0 gegenüber der Vorversion noch einmal verstärkt auf die Anforderungen DS-GVO ab. Es sind insbesondere alle einzelnen in der DS-GVO genannten konkreten Maßnahmen zur Umsetzung der Betroffenenrechte berücksichtigt. Ferner ist ein Kapitel zum „Einwilligungsmanagement“ sowie zur „Umsetzung aufsichtsbehördlicher Anordnungen“ hinzugekommen.

Im Teil C werden die Gewährleistungsziele wie bisher den Grundsätzen aus Art. 5 DS-GVO sowie darüber hinaus den vielen vereinzelten rechtlichen Anforderungen aus Teil B zugeordnet. Das SDM 2.0 gewährleistet dadurch sehr viel besser als bislang die vollständige Berücksichtigung operativer Anforderungen der DS-GVO. Dieses Kapitel ersetzt die Zuordnung von Gewährleistungszielen und Artikeln der DS-GVO aus SDM-V1.1/S. 21, Tabelle 1 und 2.

Teil D stellt die praktische Umsetzung dar; hier wurden die größten Änderungen gegenüber der Vorversion vorgenommen. In dem Kapitel zu „Risiko und Schutzbedarf“ besteht die konzeptionelle Neuerung zur V1.1 in einer klaren Darstellung des Verhältnisses von Schutzbedarf und Risiken: Der Schutzbedarf einer Person entsteht aus den Risiken, die eine Verarbeitungstätigkeit mit Personenbezug ohne technische und organisatorische Maßnahmen erzeugen würde. Während der so bestimmte Schutzbedarf der betroffenen Personen konstant bleibt, lassen sich die Risiken - durch die Gestaltung der Verarbeitungstätigkeit sowie durch den Betrieb technischer und organisatorischer Maßnahmen - mindern; diese Minderung muss bis auf ein verantwortbares Schutzniveau bzw. Restrisiko erfolgen.

Neu aufgenommen wurde das Kapitel zu „Datenschutzmanagement“. Ein Datenschutzmanagement (DSM) stellt ein methodisches Bindeglied zwischen den betrieblichen und rechtlichen Anforderungen einer Organisation und den technischen Funktionen und den technischen und organisatorischen Maßnahmen dar. Deshalb sollte die Darstellung eines DSM immer auch Bestandteil der Methodik sein. Dieses Kapitel nimmt Bezug auch auf die Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO und klärt das wechselseitige Verhältnis von Datenschutz-Folgenabschätzung und Datenschutzmanagement. Als wesentliche Komponente enthält es eine knappe Darstellung eines, spezifisch auf die datenschutzrechtlichen Prüfungsanforderungen, angepassten Deming-Zyklus. Die konzeptionelle Neuerung besteht darin, dass der genaue Ort des wechselseitigen Bezugs von Soll-Ist-

Prüfvorgängen, die technische und organisatorische Soll- Werte betreffen, und Bewertungen normativer Soll-Ist-Beurteilungen, ausgewiesen wird. Dabei erzeugt jede der vier Phasen Produkte (Spezifikationen, Dokumentationen, Beurteilungen, Anweisungen des Verantwortlichen) als Output, der jeweils den Input der nachfolgenden Phase bildet. Dieses Kapitel nimmt viele Aspekte aus dem Kapitel SDM- V1.1/S. 34, „Prüfen und Beraten“ auf und ersetzt diese.

Ein besonderes Augenmerk wurde auf eine konsistentere Nutzung des für die DS-GVO zentralen Begriffs der „Verarbeitungstätigkeit“ (vormals „Verfahren“) gelegt. Während der Begriff „Verarbeitung“ in Art. 4 Abs. 2 DS-GVO definiert ist, wird der Begriff „Verarbeitungstätigkeiten“ in Art. 30 Abs. 1 verwendet. Im SDM V2.0 wird nun als Oberbegriff „Verarbeitungstätigkeit“ genutzt, mit „Verarbeitungen“ (wie bspw. Erheben, Speichern, Abfragen) als Bestandteile. Um derartige Teilprozesse einer Verarbeitungstätigkeit zu bezeichnen, kann auch der Begriff des „Verarbeitungsvorgangs“ verwendet werden.

E3.2 Änderungen von V1.0 auf V1.1 (Stand 26.4.2018)

Die folgenden Änderungen betreffen den gesamten Text:

- Das SDM referenziert in der vorliegenden Version ausschließlich auf die DS-GVO; die Bezüge zum BDSG und zu den Landesdatenschutzgesetzen wurden herausgenommen. Möglicherweise müssen Bezüge zum BDSGneu und zu den novellierten Landesdatenschutzgesetzen neu hergestellt werden. Diese Bezüge herzustellen bleibt einer weiteren Fortschreibung des SDM vorbehalten.
- Der Begriff „Verfahren“ wurde an vielen Stellen ersetzt durch den in der DS-GVO verwendeten Begriff der „Verarbeitung“ oder der „Verarbeitungstätigkeit“, ebenso wurde der Begriff „Grundrecht“ oder „grundrechtlich“ auf die DS-GVO-Formel „Rechte und Freiheiten von Personen“ umgestellt.
- Es wurde darauf geachtet, dass das SDM insgesamt auch international anschlussfähig ist, wobei Bezüge zu Urteilen des BVerfG erhalten blieben.
- Ergänzung dieses Kapitels, das die Änderungen zur vorigen Version auflistet.

Wesentliche Änderungen in den einzelnen Kapiteln:

„Kap. 1 Einleitung“ wurde vollständig überarbeitet; neu ist der ausschließliche Bezug zur DS- GVO.

„Kap. 2 Der Zweck des Standard-Datenschutzmodells“ wurde vollständig überarbeitet; herausgestellt wurde deutlicher als bislang, dass vor dem Einsatz des SDM zur Auswahl und Konfiguration von technischen und organisatorischen Maßnahmen die rechtlichen Abwägungs- und Erforderlichkeits-Prozesse sowie eine erste Risikoanalyse durchgeführt sein müssen.

„Kap. 5.5 Weitere abgeleitete Gewährleistungsziele“ wurde ersatzlos gelöscht.

„Kap 6.2 Verankerung der Gewährleistungsziele im BDSG“ und „Kap. 6.3 Verankerung der Gewährleistungsziele in den Landesdatenschutzgesetzen“ und jeweils alle Unterkapitel wurden gelöscht. Ergänzt wurde in „Kap. 6.2 Verankerung der Gewährleistungsziele in der DS-GVO“ der Passus: „In einer Fortschreibung des Handbuchs ist geplant, die Verankerung der Gewährleistungsziele in der EU-Richtlinie für den Datenschutz bei Polizei und Justiz und der in Abstimmung befindlichen ePrivacy-Verordnung der EU zu ergänzen.“

„Kap. 8 Die Verfahrenskomponenten“ wurde vollständig überarbeitet. Zum einen musste auf den Begriff der „Verarbeitung“ bzw. „Verarbeitungstätigkeit“ umgestellt werden, zum anderen hat sich in der Praxis gezeigt, das Bedarf daran besteht, die verschiedenen Ebenen der Vorstellungen zum Begriff „Verarbeitung“ zu klären und welche Aspekte bei einer Zweck- oder Zweckebestimmung und Zweckbindung bedacht werden sollten.

„Kap. 9 Der Schutzbedarf“ wurde vollständig überarbeitet. Die DS-GVO enthält bereits ein gewisses Maß an methodischer Anleitung zur Risikoermittlung, weshalb eine Anleitung zur methodischen Ermittlung von Risiken bzw. des Schutzbedarfs entbehrlich wurde.

Die vorgenommenen Änderungen von SDM 1.1

Kapitel 1 - 3 wurden angepasst

Kapitel 4 an die Sprachregelung der DS-GVO angepasst Kapitel 5 komplett überarbeitet

Kapitel 6.1 gelöscht

Kapitel 6.2 in Kapitel 5 überführt