E1 Zusammenwirken von SDM und BSI-Grundschutz

Das SDM steht in einer engen Beziehung zur Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Der vom BSI entwickelte IT-Grundschutz ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium konkrete Anforderungen. Bei der Auswahl von Maßnahmen orientiert sich der Grundschutz vorrangig an den aus der IT-Sicherheit bekannten Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit.

Um die Anwendung des SDM zu erleichtern, nutzt die SDM-Methodik vergleichbare Modellierungsmechanismen wie die Grundschutzmethodik. BSI-Grundschutz und SDM basieren auf der gleichen Modellierung einer Verarbeitungstätigkeit. Auch das SDM modelliert die Verarbeitungstätigkeit (Geschäftsprozess) mit ihren Elementen Systeme und Dienste sowie Teilprozesse und betrachtet umfassend das Element der personenbezogenen Daten. Die zu treffenden technischen und organisatorischen Maßnahmen sind abhängig vom Risiko, das von der Verarbeitungstätigkeit und deren Eingriffsintensität ausgeht. Aus diesem Risiko wird der Schutzbedarf bestimmt und ebenfalls in drei Stufen eingeteilt. Es wird ein direkter Zusammenhang zwischen Risiko(höhe) und Schutzbedarf(sstufe) hergestellt (siehe Abschnitt D3). Die empfohlenen Maßnahmen werden im Referenzmaßnahmen-Katalog zusammengestellt.

Die Umsetzung dieser Sicherheitsmaßnahmen ist für den Datenschutz essentiell. Aber die Zielrichtung von BSI-Grundschutz und SDM unterscheiden sich ganz wesentlich. Das SDM nimmt bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen die Perspektive des Betroffenen und dessen Grundrechtsausübung ein und unterscheidet sich daher von der Sicht des IT-Grundschutzes. IT-Grundschutz hat vorrangig die Informationssicherheit im Blickfeld und soll die datenverarbeitende Institution schützen. Für die Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die ein Betroffener durch die Datenverarbeitung der Institution hinnehmen muss. Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen durch verantwortliche Stellen und der von Maßnahmen zur Gewährleistung der Betroffenenrechte zu unterscheiden.

Das SDM betrachtet neben den o. g. aus der IT-Sicherheit bekannten Schutzzielen vorrangig die Gewährleistungsziele mit Datenschutzbezug aus denen – wie im Bereich der IT-Sicherheit – technische und organisatorische Maßnahmen abgeleitet werden. Die Gewährleistungsziele des Datenschutzes erfordern in diesem Sinne im Vergleich zu den Schutzzielen der IT- Sicherheit ein etwas erweitertes Verständnis, denn der Datenschutz nimmt zusätzlich eine darüber hinausgehende, erweiterte Schutz-Perspektive ein, indem er auch die Risiken betrachtet, die von den Aktivitäten der Organisation selbst innerhalb und außerhalb ihrer Geschäftsprozesse für die Rechte und Freiheiten natürlicher Personen bestehen.

Im Rahmen der Modernisierung der Grundschutzmethodik durch das BSI wurde das Verhältnis von Datenschutz und Informationssicherheit neu justiert. Im neuen BSI-Standard 200-2 wird auf das SDM verwiesen, wenn es darum geht, das Risiko eines Grundrechtseingriffs, und daraus folgend des Schutzbedarfs, zu bestimmen. Das neue Grundschutz-Kompendium, das die Grundschutzkataloge ersetzt, enthält im Bereich „CON: Konzeption und Vorgehensweisen“ den neuen Baustein „CON.2 Datenschutz“, der die Abgrenzung zwischen Informationssicherheit und Datenschutz beschreibt. Die Anforderung „CON.2.A1 Umsetzung Standard-Datenschutzmodell“ besagt, dass geprüft werden muss, ob das Standard-Datenschutzmodell angewendet wird und dass eine etwaige Nichtberücksichtigung alle Gewährleistungsziele und eine Nichtanwendung der SDM- Methodik sowie der Referenzmaßnahmen begründet werden müssen.

BSI-Grundschutz und SDM ergänzen sich somit in idealer Weise und liefern gemeinsam die Informationen, die erforderlich sind, um die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen zu können (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO).

E2 Betriebskonzept zum Standard-Datenschutzmodell

E2.1 Einleitung

Das Betriebskonzept verfolgt den Zweck, den Anwendern dieses Modells Handlungssicherheit im Umgang zu geben. Das bedeutet zu klären, wer für das SDM einsteht, welche Version die aktuell gültige ist und zu welchem Zeitpunkt welche Version galt und wo diese aktuelle Version beziehbar ist. Das Betriebskonzept regelt drei Aspekte:

- Klärung der Rollen und Zuständigkeiten in Bezug zum Modell,
- Sicherstellung der Anwendbarkeit des SDM,
- Schaffung von Transparenz hinsichtlich der Veröffentlichung und Weiterentwicklung des Modells.

E2.2 Auftraggeber, Projektleitung, Anwender

Der Auftraggeber für die Entwicklung und Pflege des SDM sind die Mitglieder der *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK)*. Die DSK ist die Eigentümerin des SDM, das sowohl die Methodik als auch den Referenzmaßnahmen-Katalog umfasst, und gibt dieses heraus.

Die Entwicklung und Pflege des SDM geschieht durch den *Arbeitskreis „Technische und organisatorische Datenschutzfragen“* der DSK (AK Technik). Der AK Technik hat die Projektleitung inne.

Das SDM kann sowohl von den sechzehn Landesdatenschutzbeauftragten, dem Bayerischen Landesamt für Datenschutzaufsicht sowie der Bundesdatenschutzbeauftragte im Rahmen ihrer gesetzlichen Beratungs-, Prüf- und Sanktionstätigkeiten (*Anwendergruppe 1*) als auch von den Verantwortlichen und Auftragsverarbeitern bei der Planung und beim Betrieb der Verarbeitung personenbezogener Daten sowie den Datenschutzbeauftragten im Rahmen ihrer Beratungs- und Prüftätigkeiten (*Anwendergruppe 2*) angewendet werden.

Das Modell wird sowohl im Rahmen der Praxisevaluierung als auch gemäß fachlichen Erfordernissen wie folgt weiterentwickelt:

- Erstellung und Pflege des SDM, das auch den Katalog von Referenzmaßnahmen umfasst;
- Bereitstellung des SDM und des Referenzmaßnahmen-Katalogs;
- Bearbeitung von Änderungsanträgen (Change-Requests, CRs) zum SDM, die von beiden Anwendergruppen eingebracht werden können, über deren Annahme die DSK entscheidet;
- Sicherung der Qualität der Arbeitsergebnisse;
- Versionierung des SDM;
- Projektmanagement, das umfasst
    - Bereitstellung eines Single Point Of Contact (Service Desk);
    - Betrieb von CR-Verfolgung;

    - Moderation von Diskussionen;
    - Verwaltung der nötigen Betriebsmittel (Webseite, Projektplattform);
- Öffentlichkeitsarbeit.

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

E4 Stichwortverzeichnis

E5 Abkürzungsverzeichnis

Abs.	Absatz
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der DSK
Art.	Artikel
Art.-29-Gruppe	Artikel-29-Datenschutzgruppe
BSI	Bundesamt für Sicherheit der Informationstechnik
bzgl.	bezüglich
bzw.	beziehungsweise
CON	Konzeption und Vorgehen (Bausteinbezeichnung im BSI-Kompendium)
CPU	Central Processing Unit (zentrale Verarbeitungseinheit)

CR	Change Request (Änderungsantrag)
d. h.	das heißt
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Datenschutzkonferenz
DSM	Datenschutzmanagement
ErwGr.	Erwägungsgrund
EuGH	Europäischer Gerichtshof
ggf.	gegebenenfalls
i. V. m.	in Verbindung mit
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnik
Kap.	Kapitel
LAN	Local Area Network (lokales oder örtliches Netzwerk)
lit.	Buchstabe
NAS	Network Attached Storage (netzgebundener Speicher)
NEGS	Nationale E-Government-Strategie
Nr.	Nummer
PDCA	Plan Do Check Act (Phasen des Deming-Zyklus)
SAN	Storage Area Network (Datenspeicher-Netzwerk)
SDM	Standard-Datenschutzmodell
SPoC	Sigle Point of Contact (singulärer Kontaktpunkt, zentrale Anlaufstelle)
u. a.	unter anderem
vgl.	vergleiche
WP	Working Paper (der Art.-29-Gruppe)
z. B.	zum Beispiel

E6 Anhang Referenzmaßnahmen-Katalog

Der Referenzmaßnahmen-Katalog wird künftig Bestandteil des SDM, wird aber – in Abhängigkeit der

technischen Entwicklung – in kürzeren Zyklen nach den Vorgaben des Betriebskonzeptes (siehe Kapitel E2) überarbeitet als das SDM selbst.

Der Maßnahmenkatalog ist in einzelne, verabeitungsspezifische Bausteine gegliedert. Jeder Baustein enthält Baustein spezifische Maßnahmen auf der Ebene der Daten, IT- Systeme/Dienste und Prozesse. Dieser Katalog von Bausteinen befindet sich in der Entwicklungs- und Abstimmungsphase und wird ständig weiterentwickelt.

Im Rahmen Erprobung des SDM werden die einzelnen Bausteine des Katalogs zunächst von einzelnen Aufsichtsbehörden veröffentlicht und getestet, um ihre Praxistauglichkeit erproben und nachweisen zu können. Wenn der Nachweis der Praxistauglichkeit dieser Bausteine erbracht ist, werden sie als verbindliche SDM-Bausteine vom AK Technik veröffentlicht.