A1 Zweck des SDM

Mit dem Standard-Datenschutzmodell (SDM) wird ein Werkzeug bereitgestellt, mit dem die Auswahl und Bewertung technischer und organisatorischer Maßnahmen unterstützt wird, die sicherstellen und den Nachweis dafür erbringen, dass die Verarbeitung personenbezogener Daten nach den Vorgaben der DS-GVO erfolgt. Diese Maßnahmen müssen angemessen und geeignet sein, die Risiken für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen soweit einzudämmen, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Für jede Verarbeitung ist also zu prüfen, ob die personenbezogenen Daten durch eine angemessene Auswahl technischer und organisatorischer Maßnahmen so verarbeitet werden, dass die Rechte der Betroffenen gewahrt bleiben und die Sicherheit der Verarbeitung gewährleistet wird (Kapitel III der DS-GVO und die Bestimmungen zur Sicherheit der Verarbeitung gemäß Art. 24, 25 und 32 DS- GVO). Das SDM systematisiert diese Maßnahmen auf der Basis von Gewährleistungszielen und unterstützt somit die Auswahl geeigneter Maßnahmen. Das SDM dient ausschließlich einer datenschutzrechtlich konformen Gestaltung von Verarbeitungstätigkeiten und formuliert keine Anforderungen, die über das Datenschutzrecht hinausgehen.

Voraussetzung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sind das Vorhandensein einer ausreichenden und tragfähigen Rechtsgrundlage (Zulässigkeit der Verarbeitung) und die Gewährleistung der Sicherheit der Datenverarbeitung. Es gelten die Verarbeitungsgrundsätze gemäß Art. 5 DS-GVO und die Bedingungen für die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 DS-GVO. Die Prüfung des Vorliegens einer Rechtsgrundlage als Voraussetzung der Zulässigkeit der Verarbeitung muss vor der Anwendung des SDM erfolgen.

Anschließend ist kumulativ die zweite Voraussetzung der Rechtmäßigkeit der Verarbeitung zu überprüfen – die Frage, ob die Datenverarbeitung minimiert (Art. 25 Abs. 2 DS-GVO) und geeignete Maßnahmen zur Eindämmung des Risikos für die Rechte und Freiheiten der von Verarbeitung Betroffener umgesetzt wurden (Art. 25 Abs. 1 und 32 Abs. 1 DS-GVO). Diese Prüfung setzt als ersten Schritt voraus, dass dieses Risiko der Verarbeitung klar bestimmt wird. Denn die Auswahl geeigneter Maßnahmen ist abhängig von den Risiken.

Insofern ist das SDM Teil eines iterativen Prozesses bestehend aus der rechtlichen Bewertung, der Gestaltung der Verarbeitungsvorgänge sowie der Auswahl und Umsetzung von begleitenden technischen und organisatorischen Maßnahmen. Das SDM bietet mit seinen Gewährleistungszielen eine Transformationshilfe zwischen Recht und Technik und unterstützt damit einen ständigen Dialog zwischen Beteiligten aus dem fachlichen, juristischen und technisch-organisatorischen Bereich. Dieser Prozess läuft während des gesamten Lebenszyklus einer Verarbeitung und kann somit die Forderung der DS-GVO nach regelmäßiger Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen z. B. zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO) unterstützen.

Der oben beschriebene iterative Prozess muss weit vor Beginn der Verarbeitung starten, zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung (Art. 25 Abs. 1 DS-GVO). Bereits bei den ersten Planungen einer Verarbeitungstätigkeit mit personenbezogenen Daten müssen mögliche Risiken identifiziert und bewertet werden, um die Folgen der Verarbeitung beurteilen zu können.

Mit der Datenschutz-Folgenabschätzung (DSFA) verpflichtet die DS-GVO die Verantwortlichen in Art. 35, für besonders risikobehaftete Verarbeitungen die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge einzuschätzen und eine sorgfältige Analyse, Bewertung und Planung der Behandlung der Risiken vorzunehmen (Art. 35 Abs. 7 DS-GVO). Das SDM bietet eine Systematik, um

eine DSFA in strukturierter Form zu erarbeiten.

Das SDM richtet sich sowohl an die Aufsichtsbehörden als auch an die für die Verarbeitung personenbezogener Daten Verantwortlichen. Letztere können mit dem SDM die erforderlichen Funktionen und technischen und organisatorischen Maßnahmen systematisch planen, umsetzen und kontinuierlich überwachen.

A2 Anwendungsbereich des SDM

Die Anwendungsbereiche des Standard-Datenschutzmodells sind Planung, Einführung und Betrieb von Verarbeitungstätigkeiten mit denen personenbezogene Daten verarbeitet werden (personenbezogene Verarbeitungen) sowie deren Prüfung und Beurteilung. Solche Verarbeitungstätigkeiten sind dadurch gekennzeichnet, dass sie sich auf einen konkreten, abgrenzbaren und rechtlich legitimierten Verarbeitungszweck (im öffentlichen Bereich eine Ermächtigungsgrundlage) und auf die diesen Zweck verwirklichenden Geschäftsprozesse gerichtet sind (siehe Kapitel D2).

Die DS-GVO fordert, für jede Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen auszuwählen und umzusetzen, die nach dem Stand der Technik und nach dem Risiko der Rechte und Freiheiten natürlicher Personen erforderlich und angemessen sind. Diese Maßnahmen werden als Teil der Datenverarbeitung betrachtet, einschließlich der mit ihnen selbst möglicherweise verbundenen Verarbeitung personenbezogener Daten, und können ggfs. zu einer eigenen Verarbeitungstätigkeit werden. Dass es sich vielfach so verhalten kann, zeigt sich am Beispiel der Protokollierung, die in der Regel als ein unmittelbarer Bestandteil einer Verarbeitung gilt, aber unter Aspekten des Beschäftigtendatenschutzes zusätzlich beurteilt werden muss.

Die Rechtsgrundlage kann konkrete Maßnahmen vorschreiben, die verarbeitungsspezifisch umzusetzen sind, z. B. eine Anonymisierung erhobener personenbezogener Daten, sobald ein bestimmter Zweck der Verarbeitung erreicht wurde. Außerdem kann es Fälle geben, in denen besondere Maßnahmen ergriffen werden müssen, die als Ergebnis einer gesetzlich erforderlichen Interessensabwägung geboten sind, um eine rechtskonforme Verarbeitung zu ermöglichen.

A3 Struktur des SDM

Das Standard-Datenschutzmodell

- systematisiert datenschutzrechtliche Anforderungen in Gewährleistungszielen,
- leitet aus den Gewährleistungszielen systematisch generische Maßnahmen ab, ergänzt um einen Referenzmaßnahmen-Katalog,
- modelliert die Verarbeitungstätigkeit (Geschäftsprozess) mit ihren Elementen Daten, Systemen und Diensten sowie Teilprozessen,
- systematisiert die Identifikation der Risiken zur Feststellung des Schutzbedarfs einer Verarbeitung und
- bietet ein Vorgehensmodell für eine Modellierung, Umsetzung und kontinuierliche Kontrolle und Prüfung von Verarbeitungstätigkeiten.

A4 Funktion der Gewährleistungsziele des SDM

Das SDM verwendet zur Systematisierung datenschutzrechtlicher Anforderungen

„Gewährleistungsziele“. Die datenschutzrechtlichen Anforderungen zielen auf eine rechtskonforme Verarbeitung, die durch technische und organisatorische Maßnahmen gewährleistet werden muss. Die Gewährleistung besteht darin, das Risiko des Eintretens von Abweichungen von einer rechtskonformen Verarbeitung hinreichend zu mindern. Die zu vermeidenden Abweichungen schließen die unbefugte Verarbeitung durch Dritte und die Nichtdurchführung gebotener Verarbeitungen ein. Die Gewährleistungsziele bündeln und strukturieren die datenschutzrechtlichen Anforderungen und können durch mit ihnen verknüpfte, skalierbare Maßnahmen operationalisiert werden. Auf diese Weise wird die Beeinträchtigung der betroffenen Personen durch die Verarbeitung minimiert und ein wirksamer Schutz betroffener Personen durch die Minderung von Risiken für die Rechte und Freiheiten natürlicher Personen prüfbar sichergestellt. Die Vorteile in der Arbeit mit Gewährleistungszielen liegen in der vereinfachten Modellierung von funktionalen Anforderungen in praktischen Anwendungsfällen und der einfachen Visualisierung von Konflikten. Die Gewährleistungsziele unterstützen die systematische Umsetzung rechtlicher Anforderungen in technische und organisatorische Maßnahmen und können somit als „Optimierungsgebote“ aufgefasst werden.

Das SDM benennt sieben Gewährleistungsziele des Datenschutzes, welche für die Anwendung des SDM von elementarer Bedeutung sind [1)]. Im Einzelnen sind dies:

- Datenminimierung
- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,
- Nichtverkettung,
- Transparenz und
- Intervenierbarkeit.

In diesen Gewährleistungszielen finden sich die seit vielen Jahren in der Praxis bewährten Schutzziele der Informationssicherheit wieder. Die Ziele Verfügbarkeit, Integrität und Vertraulichkeit dienten bisher vorrangig der Gewährleistung der Informationssicherheit in Behörden und Unternehmen, also der Absicherung und dem Schutz der Daten einer Organisation. Für Fachleute aus dem Bereich der Informationssicherheit, die mit dem Grundschutzkonzept des BSI [2)] vertraut sind, stellen Gewährleistungsziele somit ein bekanntes Konzept dar. Ihnen wird die Anwendung des SDM leicht fallen, weil die Methode sich an den IT-Grundschutz anlehnt und sich dort bereits bewährt hat. Fachleute aus dem Datenschutzrecht können die Kontinuität der Entwicklung des Datenschutzrechts nachvollziehen und den praktischen Nutzen von Gewährleistungszielen beurteilen.

Datenschutz interpretiert Gewährleistungsziele jedoch nicht aus der Perspektive der Organisation, sondern aus der Perspektive der Betroffenen und umfasst die Erfüllung der Gesamtheit der datenschutzrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten. Das SDM betrachtet daher die o. g. Gewährleistungsziele in ihrer Gesamtheit und erfüllt somit auch die Funktion, die bekannten Schutzziele der Informationssicherheit und die datenschutzrechtlichen Anforderungen für die Verarbeitung personenbezogener Daten als Gewährleistungsziele zusammenzuführen.

Das Konzept der Gewährleistungsziele ist im Kontext des Datenschutzrechts nicht neu. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrem Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ bereits im März 2010 eine grundsätzliche Reform der Regeln des technischen und organisatorischen Datenschutzes vorgeschlagen und gefordert, die o. g. Gewährleistungsziele in das künftige Datenschutzrecht aufzunehmen. [3)] Die Gewährleistungsziele waren auch schon in einigen Landesdatenschutzgesetzen der alten Fassung verankert. [4)] Sie dienen daher schon seit vielen Jahren bei der Umsetzung von Gesetzen und Normen

in komplexen Umgebungen mit mehreren zum Teil in Konkurrenz stehenden Zielvariablen und Anforderungen.

Der europäische Gesetzgeber hat in der Datenschutz-Grundverordnung das Konzept der Gewährleistungsziele aufgegriffen und setzt somit die kontinuierliche Weiterentwicklung des technischen Datenschutzes von den ehemaligen Kontrollzielen des ersten Bundesdatenschutzgesetzes zu technologieneutralen Gewährleistungszielen fort. Die DS- GVO regelt in Art. 5 DS-GVO sogenannte Grundsätze der Verarbeitung, die nunmehr im Anwendungsbereich der DS-GVO allgemeine Geltung beanspruchen. Neu ist nur die Tatsache, dass diese übergeordneten Grundsätze ausdrücklich und allgemeingültig im Gesetzestext festgeschrieben worden sind. Die zentralen datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung (siehe Abschnitt B2) lassen sich mit Hilfe der Gewährleistungsziele vollständig systematisieren (siehe Abschnitt C). Die bereits bekannten und bewährten Gewährleistungsziele mussten dafür nicht grundsätzlich geändert werden, sondern in ihrem konkreten Verständnis auf die Datenschutz-Grundverordnung angepasst werden.

Folgerichtig ist zu konstatieren, dass alle im SDM beschriebenen Anforderungen vollständig aus der DS-GVO abgeleitet sind und sich mit Hilfe der Gewährleistungsziele strukturieren lassen. Das SDM stellt keine über das geltende Datenschutzrecht hinausgehenden Anforderungen. Die Gewährleistungsziele und ihr konkretes Verständnis werden deshalb bei künftigen Änderungen des Datenschutzrechts evaluiert und gegebenenfalls angepasst. Die aufsichtsrechtliche Tätigkeit der Datenschutzaufsichtsbehörden orientiert sich ausschließlich an der DS-GVO. Das im SDM abgebildete Konzept der Gewährleitungsziele fördert den grundrechtsorientierten Datenschutz und unterstützt Verantwortliche und Datenschutzaufsichtsbehörden insbesondere bei der Systematisierung der Anforderungen der DS-GVO (siehe Abschnitt C2).

---

1) Um Redundanzen zu vermeiden, werden die einzelnen Gewährleistungsziele nicht in diesem Abschnitt des SDM erläutert, sondern im Zusammenhang mit ihrer Zuordnung zu den rechtlichen Anforderungen der DS-GVO im Abschnitt C2 detailliert beschrieben.

2) https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

3) https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/Eckpunkte.pdf

4) S. z. B. §§ 4, 5 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -) vom 9. Februar 2000 gültig bis zum 24.5.2018.