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.