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).