DSK VERÖFFENTLICHT NEUE VERSION DES STANDARD-DATENSCHUTZMODELLS

Martin Rost

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) empfiehlt seit November 2019 die Anwendung des Standard-Datenschutzmodells in der Version 2.0 (SDM-V2).[1] Die Entwicklung einer standardisierten Methode zur Beratung, Prüfung und Umsetzung der Anforderungen des operativen Datenschutzes ist damit nach gut zehn Jahren zum Abschluss gekommen. Fortan können Verantwortliche und Datenschutzbeauftragte, die ohne eine von Datenschutz-Aufsichtsbehörden anerkannte Methode die Anforderungen der DSGVO umzusetzen versuchen, unter Rechtfertigungsdruck geraten.

1. Kontext

Die Befassung mit dem SDM zeigt, dass eine wirksame Umsetzung der DSGVO anspruchsvoll ist. Das SDM zeigt aber auch, wie diese Umsetzung für personenbezogene Verarbeitungstätigkeiten konkret und vollständig zu bewältigen ist. Durch den Ausweis von Standard-Schutzmaßnahmen bietet es zudem eine belastbare Grundlage auch für betriebswirtschaftliche Kalkulationen. Insbesondere die kaufmännische Bewertbarkeit eines vollständigen zumindest generischen Katalogs an Standard-Datenschutzmaßnahmen führte dazu, dass namhafte Versicherungen schon früh das SDM anwandten.

2. Inhalt

Der Text des SDM-V2 wurde vollständig überarbeitet und umfasst nun fünf Hauptkapitel: Kapitel A weist Zweck und Anwendungsbereich aus; die Kapitel B und C versammeln die operativen Anforderungen der DSGVO und bilden diese auf den sieben Gewährleistungszielen ab, während Kapitel D die generischen Maßnahmen zu deren Umsetzung auflistet. Kapitel D bietet außerdem Unterstützung unter anderem darin, Verarbeitungstätigkeiten im Hinblick auf die datenschutzrechtlichen Anforderungen zu beschreiben, weil entgegen vielfacher Annahmen Art. 30 DSGVO nur der formalen ▸

[1] SDM-V2-Methode: https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf, SDM-Newsletter: https://www.datenschutzzentrum.de/mailinglisten/#sdm

Erfassung dient, nicht aber als vollständig prüfbare Beschreibung einer Verarbeitungstätigkeit ausreicht. Außerdem hilft das Kapitel bei der Feststellung der Risikostufe und beim Zusammenstellen der Prozesse für ein DSGVO-bezogenes Datenschutzmanagement(system). In Kapitel E wird unter anderem der methodisch enge Bezug zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) hergestellt.

2.1 Gewährleistungsziele

Am Kern des Modells wurde nichts geändert. Die Gewährleistungsziele – Sicherung der Verfügbarkeit, Integrität und Vertraulichkeit, der Transparenz, Nichtverkettung, Intervenierbarkeit und Datenminimierung – nehmen wie bislang die über das Datenschutzrecht verteilten operativen Anforderungen auf und sind mit konkreten Maßnahmen zur Umsetzung hinterlegt. Verfahrensplaner, Juristen, Techniker und Betriebswirte können in ihren spezifischen Logiken bleiben, müssen ihre Expertise aber auf diese Ziele des Datenschutzes, die den Grundsätzen aus Art. 5 DSGVO entsprechen, beziehen. Das Gewährleistungsziel „Transparenz" (vgl. Art. 5 Abs. 1 DSGVO) sollte nach dem Stand der Technik als „Herstellung von Prüffähigkeit" umgesetzt werden, in Form von „Spezifikation" (Prüffähigkeit relevanter Ereignisse für die Zukunft), „Dokumentation" (Prüffähigkeit aktueller Ereignisse) und „Protokollierung" (Prüffähigkeit vergangener Ereignisse).

2.2 Risiken

Das SDM-V2 unterscheidet nun in Bezug zu Risiken vier Gruppen, zwei Stufen sowie eine *Strategie zur Bestimmung der Wirkintensität von Schutzmaßnahmen*.

2.2.1 Risikogruppen

Die *Risikogruppe 1* thematisiert den Grundrechtseingriff einer Verarbeitungstätigkeit. Betroffene unterliegen dem Risiko, dass der Grundrechtseingriff nicht hinreichend milde gestaltet ist, weil nicht legitime Zwecke gesetzt wurden oder weil Zwecke gezielt zu weit formuliert und deren Verständnis in der Praxis gedehnt oder schlicht nicht beachtet wurden. Dieses spezifisch nur im Datenschutz bestehende Risiko kann durch eine umsichtige Verfahrensgestaltung – bei einem hohen Risiko durch eine verarbeitungsspezifische Datenschutz-Folgenabschätzung (DSFA) – verringert werden.

Die *Risikogruppe 2* umfasst unzulängliche Schutzmaßnahmen zur Milderung des Grundrechtseingriffs, wenn diese gar nicht, nicht hinreichend oder falsch bestimmt, betrieben oder überwacht wurden. Dieses Risiko kann insbesondere durch ein organisationsweites Datenschutzmanagement (DSM) verringert werden.

Die *Risikogruppe 3* umfasst die IT-Sicherheit, wenn Schutzmaßnahmen gar nicht, nicht hinreichend oder falsch betrieben und überwacht wurden. Dieses Risiko kann in Zusammenarbeit mit der IT-Sicherheitsabteilung verringert werden.

Zur *Risikogruppe 4* gehören solche Schutzmaßnahmen der IT-Sicherheit, die ihrerseits nicht hinreichend datenschutzgerecht bestimmt, betrieben und überwacht wurden. Dieses Risiko lässt sich durch Szenarien bearbeiten, in denen für klar definierte Ausnahmefälle Verfahren beschrieben werden, bei denen zur Rettung der Organisationen zeitlich beschränkt Maßnahmen der IT-Sicherheit die Maßnahmen des Datenschutz dominieren dürfen. IT-Sicherheits-Vorfälle und derartige kontrollierte Ausnahmen sind zu dokumentieren.

2.2.2 Risikostufen

Weil mit jeder Verarbeitungstätigkeit immer mindestens ein geringes oder normales Risiko für betroffene Personen einhergeht, gilt es zu klären, ob ein hohes Risiko vorliegt.

Zur Klärung der Risikostufe kann im ersten Schritt anhand des *Typs der Verarbeitung* (vgl. Art. 35 DSGVO) oder anhand des *Typs der Daten oder der Betroffenen* (vgl. Art. 9/10 DSGVO) geprüft werden, ob gemäß DSGVO-Definition bereits ein hohes Risiko vorliegt. Im zweiten Schritt kann die *Muss-Liste* der Datenschutz-Aufsichtsbehörden[2] herangezogen werden, die die neun Einträge umfassende Liste der Eigenschaften von Verarbeitungstätigkeiten des *Working Paper 248* der Artikel-29-Gruppe enthält. Eine Übereinkunft unter den Aufsichtsbehörden besagt: Wenn mindestens zwei Eigenschaften aus dieser Liste zutreffen, liegt ein „hohes Risiko" vor. Abschließend sollte geprüft werden, ob Art, Umfang, Umstände oder Zwecke gem. Art. 24 DSGVO (inkl. ErwG 76 DSGVO) der Verarbeitungstätigkeit das Risiko

[2] https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf

für betroffene Personen in Bezug auf spezifische Schäden erhöhen.

Ausgangspunkt für eine Risikobestimmung ist somit die „reine Verarbeitungstätigkeit", die sich aus der „puren" Zwecksetzung und der abstrakten Logik der Verarbeitung ergibt; diese Beiden erzeugen das Ausgangsrisiko für betroffene Personen. Die Höhe des Schutzbedarfs der Betroffenen entspricht der Höhe des Ausgangsrisikos, weitere Risiken der anderen Risikogruppen kommen hinzu. Bei einem normalen Risiko einer Verarbeitungstätigkeit ist der Schutzbedarf der betroffenen Personen somit normal, während ein hohes Risiko entsprechend einen hohen Schutzbedarf erzeugt.

Der Schutzbedarf Betroffener in Bezug auf eine Verarbeitungstätigkeit bleibt konstant, die Risiken der Verarbeitungstätigkeit für Betroffene können, durch eine möglichst eng zweckorientierte Gestaltung der Verarbeitung und durch Schutzmaßnahmen, auf ein gemäß DSGVO ausreichendes Niveau verringert werden.

2.2.3 Schutzmaßnahmen

Allein weil alle Grundsätze des Art. 5 DSGVO zu beachten sind, sind auch alle Maßnahmen des *SDM-Referenzmaßnahmen-Katalogs* für ein normales Ausgangsrisiko der Verarbeitungstätigkeit umzusetzen.

Abhängig von der Spezifik der Verarbeitungstätigkeit sind zusätzlich *individuelle Maßnahmen* auszuwählen. Ein Beispiel dafür wäre, dass bestimmte Vorgänge einer Verarbeitungstätigkeit nur auf Antrag oder nach einer Prüfung freigegeben und der Betrieb gesondert überwacht wird, so dass bei Abweichungen sofort ein Abbruch oder eine Korrekturmaßnahme ausgelöst werden kann. Vielfach lassen sich Maßnahmen nutzen, die auch für die Informationssicherheit des IT-Grundschutzes verwendet werden; mit dem wichtigen Unterschied, dass der unmittelbare Schutz den von der Verarbeitungstätigkeit betroffenen Personen gilt, nicht den Geschäftsprozessen.

Die wichtigste Strategie zur Intensivierung der Maßnahmen bei einem hohen Risiko besteht darin, die technisch-organisatorischen Maßnahmen des Datenschutzes ihrerseits durch die gleichen technischen und organisatorischen Maßnahmen zu sichern. Das mag kompliziert klingen, ist aber einfach und elegant, um Schutzmaßnahmen effektiv und vollständig – gemessen am Katalog der Gewährleistungsziele beziehungsweise der Grundsätze gemäß Art. 5 DSGVO – zu bestimmen. So sollten bei einer Verarbeitung mit hohem Risiko die Protokolldaten auf ihren Prüfzweck hin geprüft werden, ob sie effektiv nützlich sind, Datenschutz-Konflikte zu lösen und zugleich keine Leistungskontrolle und nur wenige beschränkte Verhaltenskontrollen von Mitarbeitern zuzulassen. Zu prüfen ist, ob es weiterer Protokolldaten bedarf oder ob vorhandene Protokolldaten aus Datenschutzsicht verzichtbar sind und gar nicht erst erzeugt werden dürfen.

Protokolldaten sind bei hohem Risiko zu verschlüsseln und sie sollten nur für den Kreis der Befugten, der in einem Rollen- und Berechtigungskonzept zu definieren ist, zugänglich sein. Die Revisionsfestigkeit ist durch integritätssichernde Maßnahmen sicherzustellen. Es müssen Regeln der Auswertung und des Löschens sowie zusätzlich Verfahren zur Annotation bei zu klärenden oder von Betroffenen bestrittenen Einträgen festgelegt werden.

2.3 Verarbeitungskomponenten

Neben Gewährleistungszielen und Risikobestimmung empfiehlt das SDM-V2 als dritte Modellierungskomponente, die erforderlichen *Daten, die IT-Systeme und Dienste* sowie die einzelnen *Prozesse* der Verarbeitungstätigkeiten zu unterscheiden. Alle Maßnahmen sollten entsprechend ihrer Risikogruppe und Risikostufe auf jeweils diese Komponenten spezifisch bezogen werden. So sollten beispielsweise Programme der Verarbeitung der Daten und die dafür verwendeten IT-Systeme sowie die unterschiedlichen Teilprozesse (wie das Erheben, Verarbeiten, Übermitteln, Löschen) zur Herstellung der Prüfbarkeit protokolliert werden.

Um die Verarbeitungskomponenten vollumfänglich zu erfassen, ist eine vollständige Beschreibung der „personenbezogenen Verarbeitung" mit ihren 14 Subprozessen (vgl. Art. 4 Abs. 2 DSGVO) Voraussetzung. Wesentlicher Ausgangspunkt zur Beschreibung einer Verarbeitungstätigkeit ist die Bestimmung des Zwecks. Mit Bezug zum Zweck sind mindestens vier Aspekte zu unterscheiden: Die *Zwecksetzung* einer Verarbeitung muss legitim sein. ▸

Die *Zweckbeschreibung* muss eng sein, bereits Maßnahmen zum Erreichen der Rechtskonformität ausweisen und sollte dafür auf die vollständige Umsetzung der Grundsätze aus Art. 5 DSGVO bezogen sein. Die Ausführungen zur *Zwecktrennung* sollten die absehbaren zweckändernden oder zweckdehnenden Begehrlichkeiten aus benachbarten Bereichen der Verarbeitung abwehrend ansprechen. Abschließend sollte in Bezug zur *Zweckbindung* ausgeführt werden, wie trotz der Nutzung von (oftmals extern betriebenen) IT-Komponenten der beschriebene Zweck und die Schutzwirkungen von Maßnahmen nicht unterlaufen werden.

3. Neuerungen

Der Katalog mit „generischen Maßnahmen" wurde gegenüber dem SDM-V1.1 um weitere Maßnahmen ergänzt.[3]

Das Kapitel zum „Einwilligungsmanagement" erinnert daran, dass Einwilligungen einzuholen und diese organisiert zu speichern sind, dass sie dem Nachweis dienen und vor allem, dass sie von den Betroffenen widerrufen werden können. Das neue Kapitel zu „Anordnungen aus der aufsichtsbehördlichen Praxis" weist darauf hin, dass die Anordnung einer Aufsichtsbehörde etwa zum Sperren von bestimmten Datenfeldern, von einer Fachapplikation umsetzbar sein muss.

Neu ist auch das Kapitel zum „Datenschutzmanagement". Es verweist zur Begründung des Betreibenmüssens unter anderem auf Art. 32 Abs. 1 lit. d DSGVO. Es werden darin die vier Phasen eines kontinuierlichen Verbesserungsprozesses entsprechend dem PDCA- beziehungsweise dem Deming-Zyklus des Qualitätsmanagements beschrieben:

In der *Plan-Phase* ist die Verarbeitung gemäß Art. 25 DSGVO datenschutzgerecht zu planen, einschließlich der Bestimmung der risikenmindernden Schutzmaßnahmen für die relevanten Verarbeitungskomponenten. Insbesondere ist deren Prüffähigkeit zu spezifizieren. Das Produkt dieser Phase besteht in einer Spezifikation, wobei beispielsweise ein Lastenheft die Sicht des Auftraggebers (Verantwortlicher), ein Pflichtenheft die Sicht des Auftragnehmers (Projektleiter, externe Auftragnehmer) wiedergeben könnte. In diese Phase fällt gegebenfalls auch der erste Teil der Umsetzung von Art. 35 DSGVO mit der Durchführung einer Datenschutz-Folgenabschätzung.

In der *Do-Phase* wird die Verarbeitungstätigkeit anhand der geplanten Komponenten und Aktivitäten gestaltet. Aus Datenschutzsicht sind die Funktionen der Verarbeitung mit den von den Gewährleistungszielen adressierten Schutzmaßnahmen inklusive deren Prüfbarkeit zu implementieren. In diese Phase fällt der zweite Teil des Art. 35 DSGVO sowie die Erzeugung von Prüfergebnissen der Verarbeitungstätigkeit.

Die *Check-Phase* sollte in zwei Unterphasen unterteilt werden. In der Check-Phase 1 werden die funktionalen Prüfergebnisse als Soll-Ist-Differenzen so aufbereitet, dass sie rechtlich beurteilt werden können. In der Check-Phase 2 dann müssen insbesondere Abweichungen rechtlich beurteilt werden, um datenschutzrechtlich begründete „Änderungsbedarfe" zu formulieren.

In der *Act-Phase* sind dann funktionale Lösungsräume zu erarbeiten, deren Umsetzung durch den Verantwortlichen dokumentiert anzuweisen ist, so dass zyklisch wieder in die konkrete Planung von Verarbeitungstätigkeiten eingestiegen werden kann.

4. Fazit

Wer schon mit SDM-V1.1 gearbeitet hat muss nicht umdenken und findet mit dem SDM-V2 eine weitergehende Unterstützung der Arbeit. Man darf allerdings nicht erwarten, dass sich das SDM nach einer einmaligen Lektüre erschließt. Jede Methode, gerade im komplexen Kontext Datenschutz, erschließt sich vollständig erst unter Anleitung methodisch erfahrener PraktikerInnen.

Über den Autor

Martin Rost
arbeitet beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein und leitet die Unterarbeitsgruppe „Standard-Datenschutzmodell" des Arbeitskreis Technik der DSK.

Kontakt: 0431 9881391

martin.rost@datenschutzzentrum.de

▶ www.datenschutzzentrum.de/

[3] Einige deutsche Datenschutzaufsichtsbehörden haben für einige Bausteine höher auflösende Anleitungen unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell publiziert.