Martin Rost[1]

DSK: Standard-Datenschutzmodell V2

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat auf ihrer 98. Konferenz am 06./07. November 2019 eine umfangreich bearbeitete Version des Standard-Datenschutzmodells („SDM-V2") zur Prüfung und Beratung von Verarbeitungstätigkeiten mit Personenbezug nach DS-GVO veröffentlicht.

1 Einleitung

SDM-V2 setzt auf nunmehr 67 Seiten Bewährtes des SDM-V1.1 fort:[2] Die sieben *Gewährleistungsziele* nehmen die normativen Anforderungen mit operativem Bezug der DSGVO auf (vgl. insbes. Art. 5 DSGVO) und weisen diesen generische Referenzschutzmaßnahmen zu. *Schutzbedarfsstufen* sorgen für die Dimensionierung der Schutzmaßnahmen; spezifische Schutzmaßnahmen sind für die *drei Verarbeitungskomponenten* Daten, IT-Systeme und Prozesse vorzusehen.

Einige Details wurden geändert: Die etwas überraschend in Art. 32 der DSGVO aufgetauchte Anforderung der Belastbarkeit von Systemen wurde mit einem eigenen kurzen Kapitel bedacht.[3] Die Einstufungen von Risiken- bzw. Schutzbedarfen Betroffener wurde, abgestimmt mit dem 2018 verabschiedeten Kurzpapier Nr. 18 über „Risiko" (vgl. DSK 2018b), auf zwei Stufen reduziert. Für die Analyse bzw. Gestaltung von Verarbeitungstätigkeiten ist mit „Diensten" zu den bisherigen Komponenten Daten und Prozessen eine weitere Komponente von IT-Systemen (Hardware, Software) hinzugekommen.

2 Verbesserungen gegenüber der V1.1

Das SDM-V2 stellt zunächst einmal klar, dass der Objektbereich der DSGVO, also derjenige, den es datenschutzrechtlich zu gestalten gilt, eine „Verarbeitung" (vgl. Art. 4 Abs. 2 DSGVO) einer Organisation ist, deren Eingriff in die Rechte und Freiheiten natürlicher Personen milde zu gestalten ist.

Eine wesentliche Verbesserung besteht in der hochauflösenden Sichtung der operativen Anforderungen der DSGVO an Verarbeitungen. In dem Kapitel C werden Normen mit Maßnahmen durch Gewährleistungsziele vermittelt, dieses bildet somit das Herzstück des Modells. Hier lassen sich sämtliche funktionale Anforderungen der DSGVO für eine geplante Verarbeitung (Beratung) bzw. sämtliche rechtliche Anforderungen bei einer im Betrieb befindlichen Verarbeitung (Prüfung) zusammenstellen. Der Bezug auf Referenz-Maßnahmen erlaubt zumindest überschlägig auch die betriebswirtschaftliche Kalkulation für die Umsetzung von Datenschutzmaßnahmen.

Beim Thema „Risiko" verfolgen die Autoren zwei Strategien: Eine Typisierung der Risiken hilft einerseits, für Verfahren die geeigneten Schutzmaßnahmen zu treffen (a) und andererseits die benötigte Wirksamkeit der Maßnahmen zu bestimmen (b).

Zu a): Das SDM unterscheidet vier Typen von Risiken:

- *Risikotyp 1*: Der Grundrechtseingriff der Verarbeitungstätigkeit wird nicht hinreichend milde gestaltet.
- *Risikotyp 2*: Schutzmaßnahmen zur Milderung des Eingriffs werden nicht hinreichend betrieben und überwacht.
- *Risikotyp 3*: Schutzmaßnahmen der IT-Sicherheit werden nicht hinreichend oder falsch betrieben und überwacht.
- *Risikotyp 3.1*: Schutzmaßnahmen der IT-Sicherheit werden unzureichend datenschutzgerecht betrieben und überwacht.

Zu b): Das Ausgangsrisiko erzeugt die „reine Verarbeitungstätigkeit", die von einer Organisation, zumeist mit IT-Unterstützung, betrieben wird. Diese VT erzeugt die Risiken für die „Freiheiten und Rechte betroffener Personen". Bei einem hohen Risiko einer VT haben die davon betroffenen Personen einen entsprechend hohen Schutzbedarf. Während der Schutzbedarf der Personen konstant bleibt, können die Risiken der VT durch den Betrieb von Schutzmaßnahmen verringert werden, bis auf ein Schutzniveau, das die Anforderungen der DS-GVO erfüllt. Die Wirkungen der Schutzmaßnahmen müssen bei hohem Risiko bzw. Schutzbedarf intensiver sein, was insbesondere durch die Anwendung der Schutzmaßnahmen auf sich selber (bspw. Verschlüsselung und Zertifizieren von Protokolldaten) sichergestellt werden kann.

Neu aufgenommen wurden Kapitel u.a. zum Einwilligungsmanagement, zur Umsetzung aufsichtsbehördlicher Anweisungen sowie zum Datenschutzmanagement (DSM). Das Datenschutzmanagement(system) ist konventionell in die Phasen des PDCA-Deming-Zyklus gegliedert, bei der jede Phase bestimmte Produkte liefert: *Plan* soll eine Spezifikation insbesondere zur Prüfbarkeit der VT erzeugen. Das *Do* ist gekennzeichnet durch Implementation von Schutzmaßnahmen und der Dokumentation von Prüfaktivitäten. Das *Check* entspricht dem Beurteilen von Prüfergebnissen mit Empfehlungen für Verbesserungen der Compliance; das *Act* dient der Eröffnung von Lösungsräumen mit Anweisungen durch den Verantwortlichen, der über die Mittel und Zwecke entscheidet. Während ein DSM organisationsübergreifend eingerichtet wird, zielt eine Datenschutz-Folgenabschätzung („DSFA", vgl. Art. 35 DSGVO) auf eine einzelne VT. Zur Durch-

1 Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und Leiter der Unterarbeitsgruppe SDM des AK-Technik der deutschen Datenschutzbehörden des Bundes und der Länder (DSK). E-Mail: martin.rost@datenschutzzentrum.de

2 Zentrale Anlaufstelle für Publikation der DSK: https://www.datenschutzkonferenz-online.de/anwendungshinweise.html

SDM mit Links auch auf veröffentlichte Bausteine mit Schutzmaßnahmen: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

3 Vgl. zur Diskussion über Belastbarkeit: Gonscherowski et al. 2018.

führung einer DSFA verweist das SDM auf das DSK-Kurzpapier Nr. 5 (vgl. DSK 2018a).[4]

3 SDM von außen betrachtet

Auch außerhalb der unmittelbaren Entwicklung gibt es interessante Überlegungen zum SDM, auf die hinzuweisen lohnt.

Die Frage, was Gewährleistungsziele bzw. Schutzziele sind, stellen sich die beiden JuristInnen Robrahn/Bock. Sie sprechen im Ergebnis von „Schutzzielen als Optimierungsgeboten" (Robrahn/Bock 2018). Ziele können sowohl NormenexpertInnen als auch TechnikkonstrukteurInnen und OrganisationengestalterInnen den Eindruck vermitteln, in ihren spezifischen Logiken verbleibend einen gemeinsam anzustrebenden Idealzustand anzustreben, der aber nicht im Sinne eines endgültigen Zustands erreicht wird. Letzteres ist angesichts großer gesellschaftlicher Dynamiken sicher eine realistische Annahme.

Der Frage nach dem Verhältnis der Gewährleistungsziele untereinander geht Rost nach (Rost 2018). Unabhängig voneinander sind diese Ziele nicht, weshalb sie nicht unbedacht als „Schutzdimensionen" bezeichnet werden sollten. Die Abhängigkeit der Gewährleistungsziele voneinander zeigt sich in den Maßnahmen: Wenn bspw. ein Datum durch wirksame Verschlüsselung vor unbefugtem Zugriff geschützt ist, sichert das auch die inhaltliche Integrität eines übertragenen Datums. Schutzziele können einander auch widersprechen. Rost untersucht drei Anordnungen der Gewährleistungsziele: Als drei Dualpaare, als selbstbezügliche Anordnung und als Hierarchie. Er vermutet, dass unterschiedliche Organisationstypen, Behörden, Unternehmen, Forschungsinstitute, unterschiedlichen Ziele-Hierarchien unterliegen. Entsprechend könnten Bündel von Schutzmaßnahmen bspw. für öffentliche und nicht-öffentliche Organisationen vorabgestimmt werden.

Die Risikomodellierung des SDM-V2 war beeinflusst durch Bieker (Bieker 2018). Die Messbarkeit bzw. Skalierbarkeit von Schutzmaßnahmen bei dualen Anordnungen der Schutzziele (Verfügbarkeit-Vertraulichkeit, Intervenierbarkeit-Integrität, Transparenz-Nichtverkettung) wurde durch Jensen angeregt (Jensen 2018). Dass die Methodik des SDM auch im Kontext der JI-Richtlinie angewandt werden kann, weist Schlehan nach (Schlehan 2018).[5] Dass die Schutzziele und das SDM in einer Tradition des deutschen Datenschutzes stehen, der Datenschutz nie mit Datenschutzrecht gleichsetzte, zeigt Pohle auf (Pohle 2018).

Im Kontext der Informationssicherheit verweist das BSI seit 2018 zur Umsetzung von Grundschutzanforderungen unter Konzepte („CON.2"), dass Anforderungen des Datenschutzes mit dem SDM umzusetzen sind. In der aktuell anstehenden Überarbeitung der Grundschutztexte wird die Anwendung des SDM, insbesondere für Bundesbehörden, weiterhin empfohlen. Im Kontext der Datenschutz-Folgenabschätzungen verweist die Art. 29-Gruppe im WP als eine Methode auf das SDM (Artikel-29-Datenschutzgruppe 2017: S. 20). Eine Übersetzung des SDM-V1 liegt vor, für SDM-V2 befindet sie sich in der Planung.

4 Fazit

Wer bislang schon mit den Versionen SDM-V1 und SDM-V1.1 Datenschutz methodisch geplant und um Wirksamkeit bemüht umgesetzt hat, muss sich mit SDM-V2 nicht umstellen. Das SDM-V2 gibt allerdings weitergehende methodische Hilfestellungen zur Umsetzung der DSGVO.

5 Literatur

DuD 2018/01: Datenschutz-Schutzziele, mit den Beiträgen von: Bieker, Felix (S. 27-31); Jensen, Meiko (S. 23-26); Robran, Rasmus (S. 7-12); Rost, Martin (S. 13-18); Schlehan, Eva (S. 32-26).

Bieker, Felix (S. 27-31); Jensen, Meiko (23 – 26); Robran, Rasmus et.al. (S. 07-12); Rost, Martin (S. 13 – 18); Schlehan, Eva (S. 32-36)

Artikel-29-Datenschutzgruppe, 2017: "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679". 17/EN, WP 248. Brüssel. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 .

Bock, Kirsten / Gonscherowski, Susan / Schlehan, Eva, 2019: „Das PIA-Tool der CNIL im aufsichtsbehördlichen Praxistest"; in: PinG - Privacy in Germany, Ausgabe 03; S. 138-144.

DSK, 2018a: Kurzpapier Nr. 5, „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO", https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf .

DSK, 2018b: Kurzpapier Nr. 18, „Risiko für die Rechte und Freiheiten natürlicher Personen", https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

Engeler, Malte, 2019: „Datenschutz in der Justiz"; in: Specht / Mantz: Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage; S. 623-645.

Forum Privatheit 2017: Datenschutzfolgenabschätzung, 3. Verb. Aufl., https://www.forum-privatheit.de/wp-content/upload/Forum- Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf.

Gonscherowski, Susan / Hansen, Marit / Rost, Martin, 2018: „Resilienz - eine neue Anforderung aus der Datenschutz-Grundverordnung", in: DuD - Datenschutz und Datensicherheit 2018/07; S. 442-446.

Pohle, Jörg, 2018: „Datenschutz und Technikgestaltung, Geschichte und Theorie des Datenschutzes aus informatischer Sicht", https://edoc.huberlin.de/bitstream/handle/18452/19886/ dissertation_pohle_joerg.pdf.

4 Das Kurzpapier Nr. 5 basiert auf dem „Whitepaper V3.0" des Forums Privatheitheit, das mit Rückgriff auf das SDM formuliert wurde (Forum Privatheit 2017). Das Paar „Kurzpapier Nr. 5/SDM" zu verwenden hat sich bei vielen Datenschutz-Folgenabschätzungen gem. Art. 35 DSGVO bewährt. Kritisch bzgl. der Qualität des CNIL-Tools für Durchführung einer DSFA siehe Bock et. al. 2019.

5 Siehe darin die Tabelle auf S. 34. Zur oft überraschend schwierigen Entscheidung, ob im Justiz-Kontext DSGVO oder JRL/BDSG-Teil3 gilt und anzuwenden ist, siehe Engeler 2019.