Martin Rost, Aleksandra Sowa

Die ISO 27701 und das SDM-V2 im Lichte der Umsetzung der DSGVO

Dieser Artikel gibt einen kurzen Einblick in die Standards und zeigt auf, welche Hilfestellung man im Datenschutz als Praktiker von ihnen erwarten darf.

1 Einleitung

Es werden nicht viele Modelle auf dem Markt angeboten, die beanspruchen, datenschutzrechtliche Anforderungen in konkrete funktionale Anforderungen zu transformieren. Eine solche Transformation, die bei jeder Prüfung oder aktiven Gestaltung einer Verarbeitungstätigkeit zu bewältigen ist, ist dabei unabweisbar „verlustbehaftet", es bleibt immer Schlupf. Während sich das „Standard-Datenschutzmodell" (SDM) ausschließlich in den Dienst der DSGVO stellt, bemüht sich die ISO 27701 insbesondere um ein Konsistenthalten der ISO-Familie mit Anforderungen aus der DSGVO. Während das SDM den Blick auf die Funktion des Datenschutzes, nämlich eine Verarbeitungstätigkeit grundrechtekonform zu gestalten, fest im Blick zu behalten beansprucht, legt die ISO 27701 besonderen Wert darauf, einen praxisgerechten Kontakt zur Organisation und ihren Prozessen als Ganzes zu halten.

2 Essentials des SDM

Das Standard-Datenschutzmodell in der Version 2.0 (SDM-V2) wurde Anfang November 2019 von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) für Datenschutzprüfungen und Datenschutzberatungen zur Anwendung empfohlen. Das SDM-V2 wurde gegenüber dem SDM-V1.1 noch enger auf die DSGVO abgestimmt[1], mit dem Kurzpapier Nr. 18 „Risiko" der DSK abgeglichen sowie um ein Kapitel zum Datenschutz-Management ergänzt.[2] Anschließend wurde es noch einmal redaktionell überarbeitet (Version SDM-V2a) und im April 2020 dann um einen Absatz im Anhang erweitert, in dem der Grad der Verpflichtung der Anwendung der Maßnahmen dargelegt ist (Version SDM-V2b). Dazu heißt es:

> *„(...) Die Aufzählung von Maßnahmen in den Bausteinen ist nicht abschließend. Durch die Aufnahme einer Maßnahme in einen Baustein trifft die Konferenz keine verbindliche Aussage zur Verpflichtung, sie umzusetzen. Gleichwohl wird eine solche Verpflichtung unter Berücksichtigung der nach gesetzlicher Vorgabe im Einzelfall zu betrachtenden Faktoren vielfach bestehen. (...) Aufgrund der Natur des Anhangs als Referenzkatalog müssen Anwender des SDM jedoch dokumentieren, ob, inwieweit und warum sie sich entschieden haben, Maßnahmen der Bausteine abweichend von den Empfehlungen des SDM umzusetzen."*

Die sehr enge Verzahnung des SDM-V2 mit der DSGVO führte zu einer nochmaligen Reflexion der Ausrichtung des Modells und insbesondere zur noch einmal verstärkten Abgrenzung von Prüf- und Gestaltungs-Modellen der Informationssicherheit. Die DSGVO „schützt die Grundrechte und Grundfreiheiten natürlicher Personen" (Art. 1 Abs.2 DSGVO) und macht deshalb nicht nur besonders schützenswerte „personenbezogene Daten" (vgl. Art. 4 Abs 1 DSGVO) sondern „Verarbeitungen" (Art. 4 Abs. 2 DSGVO) durch „Niederlassungen" (Art. 3 Abs. 1 DSGVO) zum Gegenstand der datenschutzrechtlichen Ausgestaltung. Die Verantwortlichen der „Niederlassungen" müssen dafür sorgen, dass die Datenverarbeitungen der Organisationen den Grundrechten und Grundfreiheiten nicht zuwiderlaufen und dabei den „Grundsätzen" des Datenschutzes (Art. 5 DSGVO) genügen. Die Wirksamkeit der risikomindernden Schutzmaßnahmen muss dabei nachgewiesen werden (vgl. Art. 32, Abs. 1 lit. d DSGVO, Art. 35 Abs. 3 DSGVO). Diese Anforderungen operativ umzusetzen nimmt das SDM in Anspruch.

Dr. Aleksandra Sowa

ist IT-Compliance Manager und Datenschutzauditorin. Sie ist Buchautorin und aktuell als Senior Manager im Bereich Cybersecurity & Privacy einer Wirtschaftsprüfungsgesellschaft tätig.

Martin Rost

ist Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und Leiter der Arbeitsgruppe „Standard-Datenschutzmodell"
E-Mail:
martin.rost@datenschutzzentrum.de

1 Das SDM eignet sich auch zur operativen Umsetzung der Justiz-Richtlinie (vgl. Schlehan 2018).

2 Bezugsquelle des Modells: https://www. datenschutzkonferenz-online.de/media/ah/SDM-Methode_V20b.pdf. Als zentrales Repository der SDM-Arbeitsgruppe dient https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/. Dort finden sich auch Bausteine zu Schutzmaßnahmen. Dass sich das SDM zudem als Grundlage für eine Datenschutz-Folgenabschätzung gem. Art, 35 DSGVO eignet, zeigte sich zuletzt prominent bei der Muster-DSFA zur Corona-Warn-App (vgl. Bock et al. 2020).

Als Zweck weist das SDM die systematische „Transformation gesetzlicher Anforderungen in operativ-funktionale Anforderungen" aus. Denn auch die konkreten, funktionsnah formulierten Anforderungen der DSGVO – wie bspw. „Löschen" (Art. 17 DSGVO) oder „Pseudonymisierung" (Art. 25 DSGVO) – bedürfen einer konkretisierenden Einengung, weisen diese doch eine breite Skala an unterschiedlichen Möglichkeiten zur Implementierung auf. So stellt bspw. ein Löschvorgang (und dessen Transparenz) in Bezug auf ein Datum in einer Datei andere Anforderungen als in Bezug auf eine Datenbank oder auf die Datenbestände eines IT-Systems am Arbeitsplatz oder eines Servers im Rechenzentrum, zudem in Abhängigkeit von der zu beachtenden Risikostufe.

Das SDM besteht aus drei Bestandteilen. Es verdichtet erstens die „Grundsätze" aus Art. 5 der DSGVO – sowie alle weiteren in der DSGVO verstreuten Anforderungen – zu sieben „Gewährleistungszielen", die eine Organisation anstreben und in Schutzmaßnahmen umwandeln muss. Das Modell empfiehlt zweitens, die Verarbeitungstätigkeiten von Organisationen in drei Komponenten – Datenbestände, IT-Systeme/Dienste und Prozesse – zu analysieren, zu prüfen und zu gestalten. Und drittens bietet das SDM eine Strategie an, um die Risiken einer Verarbeitungstätigkeit einer der beiden von der DSGVO vorgegebenen Risikostufen – „gering/ normal" oder „hoch" – zuzuordnen, mit Konsequenzen für die Auswahl und die Wirksamkeit der Schutzmaßnahmen. Auf Basis dieser drei Bestandteile weist das SDM dann generische Referenz- oder Standard-Schutzmaßnahmen sowie ein Framework für ein organisationsweit agierendes Datenschutz-Management aus, das die vier Aktivitäten „Kontrollieren", „funktionales und rechtlichen Prüfen", „rechtliches Beurteilen" und „verantwortliches Entscheiden" unterstützt.[3]

3 Essentials der ISO/IEC 27701

Die ISO/IEC 27701 wurde im August 2019 in der Version 1 publiziert. Im Wesentlichen wird dieser Standard einleitend zunächst in die Systematik der ISO-Familie eingeordnet mit dem Zweck, diese um Maßnahmen für ein „Privacy Information Management System" (PIMS)[4], das für die im Rahmen des Informationssicherheitsmanagementsystems (ISMS) verarbeiteten personenbezogenen Daten gilt, zu erweitern. Referenziert wird in dem ISO 27701 entsprechend auf die relevanten bestehenden, darunter auch zertifizierbaren Standards zum Management der Informationssicherheit:

- ISO/IEC 27000 („Information security management system", overview and vocabulary),
- ISO/IEC 27001:2013 („Information security management system", requirements),
- ISO/IEC 27002:2013 („Code of practice for information security controls", guidelines)
- sowie den ISO/IEC 29100 Information technology — Security techniques — Privacy framework („Rahmenwerk für Datenschutz") aus dem Jahr 2011 (Review im Jahr 2017), in dem erstmalig Terminologie, Verantwortlichkeiten und Rollen der Verantwortlichen für die Verarbeitung personenbezogener Daten definiert wurden.

Im Anhang wird (informativ) von den Maßnahmen und Empfehlungen aus dem ISO 27701 auf die entsprechenden Maßnahmen in anderen ISO-Standards im Kontext des Datenschutzes referenziert:

- ISO/IEC 29100 („Rahmenwerk für Datenschutz")
- ISO/IEC 27018 („public cloud services")
- ISO/IEC 29151 („Leitfaden für den Schutz personenbezogener Daten")

Ebenfalls im Anhang erfolgt schließlich eine tabellarische Zuordnung („Mapping") der Anforderungen an das PIMS aus dem ISO 27701 zu den relevanten Artikeln 5 bis 49 der DSGVO.

3.1 Zielsetzung und Abgrenzung des Geltungsbereichs

Der allgemeine Zweck der ISO 27701 soll darin bestehen, Anforderungen zu spezifizieren und eine Anleitung zur Einrichtung, Implementierung, Wartung und kontinuierlichen Verbesserung eben eines Privacy Information Management System (PIMS) in Form einer Ergänzung der ISO 27001 und ISO 27002 sowie eines Mapping mit Maßnahmen aus anderen ISO-Standards (ISO/IEC 29100, 27018 sowie 29151) und der DSGVO zu bieten.

Der spezifische Zweck besteht darin, PIMS-bezogene Anforderungen zu spezifizieren und eine Anleitung zur Verarbeitung von personenbezogenen Daten sowohl für Verantwortliche („PII-Controller") als auch für Verarbeiter („PII-Processor") zu geben. Der Standard soll dabei für alle Arten und Größen von Organisationen gelten, also einschließlich öffentlicher und privater Unternehmen, staatlicher Einrichtungen und gemeinnütziger Organisationen. Es soll insbesondere auch Anleitung dafür bieten, wenn personenbezogene Daten innerhalb eines „Information Security Management Systems" (ISMS) verarbeitet werden.

3.2 ISO/IEC 27701 versus ISO/IEC 27001

Ein verbreiteter Irrtum, ISO 27701 betreffend, besteht darin, dass es sich dabei um einen sog. Stand-alone-Standard handele, der von Organisationen beim Aufbau eines Datenschutzmanagementsystems isoliert berücksichtigt werden kann. Tatsächlich ist der ISO 27701 nur in Kombination mit dem ISO 27001 anwendbar, d. h., die dort auf ca. vierzig Seiten erfassten Anforderungen an PIMS stellen lediglich eine Ergänzung bzw. Erweiterung der Anforderungen des zertifizierbaren Standards ISO 27001, der im Übrigen zuallererst Anwendung findet und dessen Formulierung an den Stellen, an welchen die Formulierung „Information Security" (Informationssicherheit) verwendet wird, in „Information Security and Privacy" (Informationssicherheit und Datenschutz) umgewandelt wird. So gesehen erinnert der Aufbau des ISO 27701 dem eines Artikelgesetzes, wobei die Erfüllung der Anforderungen aus dem neuen Standard zwingend die Erfüllung der Anforderungen aus dem ISO 27001 voraussetzt.

So ist auch nicht gedacht, eine Stand-alone-Zertifizierung des Datenschutzmanagementsystems gemäß ISO 27701 zu ermöglichen. Vielmehr sollte künftig eine Erweiterung der bestehenden ISMS-Zertifizierung gemäß ISO 27001 um den Themenblock „Datenschutz" möglich sein. Die Voraussetzungen hierfür müssen noch formaltechnisch geschaffen werden.

3 Das SDM-V2 lässt sich problemlos in ein organisationsweit aufgespanntes ITIL-4 Framework einfügen (vgl. Rost/Welke 2020).

4 Auch: Datenschutzmanagementsystem (DSMS)

3.3 Logik und Aufbau

Die thematische Zuordnung der Anforderungen an PIMS richtet sich an der Logik der Control Objectives aus den ISO 27001 und ISO 27002 aus.

So werden die Kontrollen von Organisation, Leadership, Planung, Support, Operationen, Performance-Evaluation und Verbesserung aus der ISO 27001:2013 in den Punkten 5.2–5.8 in dem Dokument adressiert, wobei nur Organisation (5.2) und Planung (5.4) zusätzliche, PIMS-spezifische Anforderungen umfassen.

Die ISO 27701 greift die in ISO 27001 und ISO 27002 angesprochenen Aspekte systematisch „Punkt für Punkt" auf und ergänzt diese um Anforderungen eines besonderen Managements personenbezogener Daten. Vielfach wird dabei robust vorgegangen: So heißt es bspw. im Kapitel 5.1 „Allgemeines": Die Anforderungen der ISO/IEC 27001:2013 in Bezug auf „Informationssicherheit" sollen erweitert werden um den Schutz von Privatheit, die möglicherweise durch das Prozessieren personenbezogener Daten berührt wird.

Abbildung 1 | Auszug aus: ISO 27701:2019, S. 65, entspricht ISO 27001, Ziffer 6.1.2

6.1.2 Information security risk assessment

The organization shall define and apply an information security and privacy risk assessment process that:

a) establishes and maintains information security and privacy risk criteria that include:
   1) the risk acceptance criteria; and
   2) criteria for performing information security and privacy risk assessments;
b) ensures that repeated information security and privacy risk assessments produce consistent, valid and comparable results;
c) identifies the information security and privacy risks:
   1) apply the information security and privacy risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security and privacy information management system; and
   2) identify the risk owners;
d) analyses the information security and privacy risks:
   1) assess the potential consequences that would result if the risks identified in 6.1.2 c) were to materialize;
   2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and
   3) determine the levels of risk;
e) evaluates the information security and privacy risks:
   1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and
   2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security and privacy risk assessment process.

3.3.1 Ergänzung des ISO 27001

Ausgewählte Kontrollen gelten nur mit entsprechenden Erweiterungen gegenüber der Formulierung in der ISO 27001. Dies gilt bspw. für den Bereich „Information security risk assessment" (Bewertung der Informationssicherheitsrisiken), der unter Ziffer 5.4.1.2 des ISO 27701 PIMS-relevante Erweiterungen erfährt: Die Formulierungen aus 6.1.2 c) 1) sowie 6.1.2 d) 1) der ISO 27001 ändern sich entsprechend. Konkret bedeutet dies:

- Organisationen müssen den Prozess zur Bewertung der Informationssicherheitsrisiken im Bereich des PIMS anwenden, um Risiken des Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit zu identifizieren.
- Organisationen müssen den Prozess zur Bewertung der Informationssicherheitsrisiken im Bereich des PIMS anwenden, um Risiken zu identifizieren, die mit der Verarbeitung personenbezogener Daten (PII) verbunden sind.
- Organisationen müssen entlang des Prozesses zur Bewertung der Informationssicherheitsrisiken sicherstellen, dass das Verhältnis zwischen Informationssicherheit und Schutz personenbezogener Daten adäquat gemanagt wird. (ISO 27701:2019, S. 6, entspr. ISO 27001 6.1.2 c) 1))

Dabei stellt es der Standard den Organisationen frei, ob die relevanten Risiken im Rahmen eines integrierten Risikobewertungsprozesses berücksichtigt werden oder zwei separate Prozesse zur Bewertung der Risiken der Informationssicherheit und Bewertung der Risiken, die mit der Verarbeitung personenbezogener Daten verbunden sind, Anwendung finden.

Im Ergebnis, unter Berücksichtigung der „Refinements" und Ergänzungen aus dem ISO 27701, sieht der entsprechende Bereich des ISO 27001 – 6.1.2 „Information security risk assessment" wie in Abbildung 1 dargestellt aus.

3.3.2 Ergänzung des ISO 27002 Sicherheitsvorfälle und Data Breaches

Unter den Ziffern 6.2–6.15 der ISO 27701 finden sich die PIMS-relevanten Ergänzungen der Guidelines zur Umsetzung der Sicherheitskontrollen aus der ISO 27002. Bis auf Business Continuity Management erfahren alle Kontrollen aus dem Sicherheitsstandard PIMS-relevante Erweiterungen und Ergänzungen.

Umfangreiche Ergänzungen betreffen bspw. die Kontrollen „Information security incident management", die unter der Ziffer 6.13 der ISO 27701 subsumiert wurden. In diesem Bereich wird auf die regulatorischen Anforderungen aus der DSGVO zur Identifizierung und Meldung von sog. „data breaches" eingegangen. Die Ziffer 16.1.1 wird insoweit ergänzt, dass Organisationen im Rahmen ihrer Prozesse zum Management von IT-Sicherheitsvorfällen Verantwortlichkeiten und Prozesse etablieren, die die Aufnahme und Identifizierung von Data Breaches (personenbezogene Daten betreffend) sowie Prozesse zur Benachrichtigung Betroffener und relevanter Beteiligter und Meldungen an die Behörden etablieren sollten.

Diese Herangehensweise bricht mit dem üblichen Silodenken in den Organisationen, sicherheitstechnische und datenschutzrechtliche Aspekte der Organisation und des Managements in verschiedenen Organisationsbereichen zu etablieren und prozessual voneinander zu trennen. Es entspricht der Empfehlung zur Umsetzung der Anforderungen aus den Art. 33 und 34 DSGVO, dass der Verantwortliche sicherstellen sollte, „*dass IT-Sicherheitslücken zentral gemeldet und auf eine Meldepflicht hin bewertet werden, z. B. unter Einbeziehung des Datenschutzbeauftragten und der Rechtsabteilung*" (Gierschmann et al., S. 886). Kein Verantwortlicher sei davor gefeit, dass es zu einer Verletzung der Sicherheit, z. B. durch einen „bösartigen Hacking-Angriff" kommt, doch für die Bemessung der etwaigen Bußgelder sei es wesentlich, ob der Angriff rechtzeitig erkannt wurde und ob es trotz angemessener Sicherheitsmaßnahmen geschah. Zu den Nachweisen, die gemäß EG 87 von der Aufsicht zwecks Prüfung des Data Breach angefordert werden, gehört lt. Gierschmann et al. auch, ob im Rahmen der technisch-organisatorischen Maßnahmen ein Security Incident Response System etabliert wurde, das nicht nur IT-Sicherheitsvorfälle, sondern auch Data Breaches erkennt, ob Melde- und Kommunikationswege definiert und etabliert sind, die bei Verletzung der Sicherheit personenbezogener Daten „In Place" sind, gelebt werden und klar definieren, wann, was und an

wen berichtet werden soll, welche Informationen erfasst und welche weiteregegeben werden.

Diese Empfehlung findet sich auch in der ISO 27701 im Rahmen der Ergänzung des Information Security Incident Management. Definiert werden u. a. unter der Ziffer 6.13.1.5 die Modalitäten der Reaktion (response) auf die Sicherheitsvorfälle, die Leitfäden für sowohl PII-Controller (Verantwortliche) als auch PII-Processor (Verarbeiter) umfassen und detailliert die Anforderungen aus den Art. 33 und 34 DSGVO als Standardvorgaben berücksichtigen, inkl. Definition von Inhalten der Meldung an die Aufsicht oder die Betroffenen (vgl. ISO 27701:2019, S. 24–26). Es wird explizit darauf hingewiesen, dass sowohl Meldungen von IT-Sicherheitsvorfällen als auch Data Breaches unterschiedlichen nationalen Regulierungen und Normen unterliegen können und diese zu berücksichtigen sind. In Deutschland gilt bspw. neben der Meldepflicht für Verletzungen der Sicherheit personenbezogener Daten nach DSGVO auch Meldepflicht für (wesentliche) Sicherheitsvorfälle im Bereich der kritischen Infrastrukturen nach IT-Sicherheitsgesetz (ITSiG) bzw. BSI-Gesetz (BSIG) (vgl. Hanßen/Sowa 2018).

3.4 Zusätzliche Kontrollen für Verantwortliche und Verarbeiter personenbezogener Daten

Unter den Ziffernummern 7 und 8 des ISO 27701 werden zusätzliche Kontrollen und Kontrollziele für die PII-Controller (Verantwortliche, ad A.7) und PII-Processor (Verarbeiter, ad B.8) erfasst. Es geht um die Ergänzung der Anleitung aus ISO 27002 um relevante, zusätzliche und bisher in dem Standard nicht berücksichtigte Aspekte und Themen der Verarbeitung personenbezogener Daten. So werden unter Ziffer 7.2. Kontrollen erfasst, die Rahmenbedingungen des Sammelns und Verarbeitung personenbezogener Daten adressieren, und 7.3. Pflichten der Verarbeiter gegenüber den Betroffenen (PII-Principals) umfassen, u. a. Auskunfts- und Informationsrechte gemäß Art. 13–15 DSGVO betreffend. Privacy by design und Privacy by default wurden unter Ziffer 7.4 berücksichtigt, darunter Datenminimierung als Kontrollziel, Löschen oder Re-Identifizierung von Daten. Unter 7.5 wurden Kontrollen für Datentransfer (an Dritte u./o. andere Länder und Organisationen) berücksichtigt.

Unter den Ziffern 8.2–8.5 werden die gleichen Aspekte und Kontrollen berücksichtigt, allerdings aus der Perspektive des PII-Processor (Verarbeiter) betrachtet und unter Berücksichtigung besonderer Aspekte der Datenverarbeitung. Umfangreich fallen die Ergänzungen im Bereich des Datentransfers aus, die sich u. a. auf Kontrollen und Möglichkeiten des Engagements von Subunternehmen beziehen und bspw. Die Anleitung zur Prüfung der Zulässigkeit solcher Engagements berücksichtigen.

4 Zusammenschau

Für eine Methode zur Umsetzung gesetzlicher Datenschutzanforderungen an eine Verarbeitung muss man verlangen, dass sie dem Zweck des Gesetzes folgt. Und daraus abgeleitet muss man für die betriebliche Praxis von Schutzmaßnahmen wiederum verlangen können, dass diese nicht nur dem Schutz personenbezogener Daten dienen, sondern zuvorderst die Risiken bzgl. der Intensität von Eingriffen in die Selbstbestimmung von Personen, die von der Verarbeitung selber ausgehen, minimieren. Diesen Anforderungen genügt das SDM ungleich besser als die ISO 27701.

Die ISO 27701 verfolgt den an Risiken orientierten Ansatz wie bereits die ISO 27001. Man geht weg von den starren, auf Prüf- bzw. Maßnahmenkatalogen basierenden Vorgaben zur Umsetzung der Anforderungen an das Informationssicherheits- bzw. Datenschutzmanagement und definiert stattdessen Ziele und Kontrollen, die Organisationen – risikoorientiert, gemäß ihrer speziellen Risikosituation und Gefahrenlage – selbstverantwortlich mit Maßnahmen und Aktivitäten füllen müssen. Entscheidungen und Prozesse müssen belegt bzw. dokumentiert sein, sobald die Organisationen bspw. eine Zertifizierung ihrer Systeme (ISMS oder PIMS/DSMS) anstreben.

5 Fazit

Das SDM stellt sich in den Dienst der Umsetzung der DSGVO. Die ISO 27701 verweist selbstreferenziell vor allem auf andere ISO-Standards; einzig das Mapping im Anhang D stellt einen direkten Bezug zwischen ISO 27701 und DSGVO her. Die relativ starke Anlehnung des weltweit geltenden Standards ISO 27701 an Anforderungen aus der DSGVO könnte als Bestätigung dafür gedeutet werden, wie stark der Einfluss der DSGVO inzwischen auch international geworden ist. Gleichwohl wird in der ISO 27701 darauf hingewiesen, dass die nationalen und lokalen Normen und Regelungen ebenfalls hinreichend zu berücksichtigen seien.

Ein konkret die Umsetzung der DSGVO prüfender oder an der Verfahrensgestaltung beteiligter Datenschutzbeauftragter sollte keine unmittelbar nützlichen Werkzeuge und Arbeitshilfen von der ISO 27701 erwarten. Auf der Ebene der Auflistung von Schutzmaßnahmen der IT-Sicherheit hat der IT-Grundschutz aus unserer Sicht zudem mehr und zumeist Detaillierteres zu bieten.

Eine Stärke der ISO 27701 besteht darin, dass sie die Organisation selber in den Blick nimmt („5.1 Understanding the organization and its context"). Dadurch kann man erkennen, wo es in einer Organisation strukturell und prozessual hapert, um Änderungen herbeizuführen. Über diese insbesondere das Datenschutzmanagement berührende Stelle sieht das SDM zu großzügig hinweg.

6 Literatur

Bock, Kirsten et al. 2020: Datenschutz-Folgenabschätzung (DSFA) für die Corona-App, V1.6, https://www.fiff.de/dsfa-corona-file/at_download/file

DuD-Spezial, 2018: Datenschutz-Schutzziele, DuD – Datenschutz und Datensicherheit, 42. Jahrgang, Heft 1.

Gierschmann, S., Veil, W., Schlender, K. und Stentzel, R. (Hrsg.) 2017. Kommentar Datenschutz-Grundverordnung (1. Auflage), Reguvis Fachmedien

Hanßen, H. und Sowa, A. 2018. „Meldepflichten nach DSGVO, ITSiG und NIS-Richtlinie". In <kes> 4/2018 (36), S. 20-28.

Rost, Martin / Welke, Sebastian, 2020: SDM 2.0 und ITIL 4 „verschränkt", in: DuD – Datenschutz und Datensicherheit, 44. Jahrgang, Heft 4: 258-262.

Schlehan, Eva, 2018: Die Methodik des Standard-Datenschutzmodells im Bereich der öffentlichen Sicherheit und Justiz, in DuD – Datenschutz und Datensicherheit, 42. Jahrgang, Heft 1: 32-36.