DIE NORM ISO 27701

Synergien zwischen Informationssicherheit und Datenschutz für intelligente Dienste schaffen

Smart Service Welt

Eine Publikation im Auftrag des Bundesministeriums für Wirtschaft und Energie im Rahmen der Begleitforschung zum Technologieprogramm „Smart Service Welt II“

IMPRESSUM

Herausgeber
Begleitforschung Smart Service Welt II
Institut für Innovation und Technik (iit)
in der VDI/VDE Innovation + Technik GmbH

Guido Zinke
Steinplatz 1
10623 Berlin
zinke@iit-berlin.de

Redaktion
Dr. Martin Weimer, Institut für Innovation und Technik (iit)

Gestaltung
Loesch*Hund*Liepold Kommunikation GmbH

Bilder
ribkhan – stock.adobe.com

Stand
Juni 2021

INHALT

1 EINLEITUNG

Was braucht es für smarte, intelligente Dienste? Neben Entwickler:innen und finanziellen Mitteln unstrittig auch Daten, intelligente Algorithmen, performante Anwendungen und zuverlässige Dienste, Provider und Dienstleister für Informationssicherheit und Datenschutz.

Ungeachtet einer grundsätzlichen Sensibilisierung für die Themen „Informationssicherheit" und „Datenschutz" haftet beiden nicht der Ruf von Innovationstreibern an: Weder gelten lange Passwörter, zusätzliche Token, Verschlüsselungsverfahren – denkt man an Informationssicherheit – noch Einwilligungsmanagement, Löschkonzepte oder Pseudonymisierungen – denkt man an den Schutz personenbezogener Daten – als unmittelbar nutzbringend. Auch bleibt es eine ständige Herausforderung, wirksame Sicherheitsmaßnahmen und Compliance als Kaufargumente oder gar als Wettbewerbsvorteile zu verstehen und erfolgreich zu kommunizieren. Schon allein die Anforderungen der Datenschutz-Grundverordnung (DSGVO) zum Schutze personenbezogener Daten können mit großen Herausforderungen für Unternehmen, insbesondere bei der Entwicklung neuer Geschäftsfelder wie smarter Dienste, verbunden sein. Konkret kann es für Unternehmen eine Schwierigkeit darstellen, zusätzliche Dienste auf Basis der Analyse personenbezogener Daten zu entwickeln, wenn damit der Zweck der Verarbeitung überdehnt wird. Kommt es zu Verletzungen, drohen Bußgelder und – oft noch schwerwiegender – ein Reputationsschaden. Sanktionen drohen auch von anderer Seite: Bei Verstößen gegen das kommende IT-Sicherheitsgesetz 2.0 können für „Unternehmen von besonderem öffentlichem Interesse"[1] ebenfalls empfindliche Strafen drohen, wobei nur ausgewählte Firmen unter diese Kategorie fallen dürften.

Es gibt jedoch in vielen Organisationen ein gutes Fundament, um diesen Herausforderungen zu begegnen: eine gelebte Sicherheitskultur zum Schutz von Informationen. Die neue ISO 27701 beschreibt, wie bestehende Strukturen, Prozesse und sogar Tools der Informationssicherheit als Basis für eine umfassende Würdigung der DSGVO dienen können – ohne, dass dafür zwei Parallelwelten von Informationssicherheit und Datenschutz mit allen erdenklichen Widersprüchen und Mehraufwänden zu schaffen sind.

Ziel dieser Handreichung ist es zu zeigen, dass sowohl punktuelle wie auch umfassende Zusammenarbeiten zwischen beiden Bereichen möglich sind. Dieses Zusammenwirken zahlt sich auch bei der Entwicklung von smarten Diensten aus. Diese Handreichung ist aus der Sicht eines Anwenders und nicht aus Sicht einer Zertifizierungsstelle geschrieben.

1 Vergl. „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, § 8f."

2 MOTIVATION

Informationssicherheit verfolgt als klassische Ziele die Gewährleistung der Vertraulichkeit, der Integrität und der Verfügbarkeit von Informationen. Eine umfassende Betrachtung dieser Ziele und die Verknüpfung mit den eigentlichen Unternehmenszielen kann durch sogenannte Managementsysteme erreicht werden. Eine der wichtigsten Normen zur Einführung, Erhaltung und Verbesserung eines sogenannten Informationsmanagementsystems (ISMS) ist die Norm ISO 27001.

Sie betrachtet keine Produkt- oder Systemsicherheit, sondern Informationssicherheit auf dem Niveau von Organisationen. Smart Services – intelligente Dienste – sind eingebettet in einen technologischen Kontext aus Anwendungen, aus Infrastruktur und Dienstleistern. Sicherheit und Datenschutz auf Produkt- oder Systemebene zu betrachten, würde zu kurz greifen.

Ein ISMS gemäß der Norm ISO 27001 ist zertifizierungsfähig. An die Informationssicherheit in einem Unternehmen bzw. in einer Organisation richten sich Anforderungen, die von außen (Gesellschafter:innen, Aktionär:innen, Bürger:innen, Presse, Legislative etc.) und von innen (Geschäftsführung, Mitarbeitende, Betriebsrat etc.) gestellt werden. Es gilt also, zahlreiche Anspruchsgruppen mit ihren Erwartungen und mit ihrem Einfluss auf das Unternehmen zu betrachten. Dies ist ein wesentlicher Unterschied zum Datenschutz – dem Schutz personenbezogener Daten (pbD). Hier stehen die Anforderungen der Anspruchsgruppe „Betroffene“ klar im Vordergrund. Dies birgt Konfliktpotenzial.

Ein Ausweg kann es sein, die klassischen Informationssicherheitsziele um ein viertes Ziel – den Schutz personenbezogener Daten – zu erweitern und es in allen relevanten Aspekten mit zu berücksichtigen. Dies reicht von Sicherheitspolitik über alle etablierten Sicherheitsprozesse, alle relevanten organisatorischen und technischen Sicherheitsmaßnahmen bis hin zur Ausgestaltung von Vertragsbeziehungen zu Unterauftragnehmern oder Kunden. Wie diese Erweiterung systematisch umgesetzt werden kann und so zur Ausbalancierung der Anforderungskategorien Informationssicherheit und Datenschutz beiträgt, beschreibt die relativ neue[2] Norm ISO 27701.

Eine Zertifizierung des erweiterten Managementsystems nach ISO 27701 auf Basis der ISO 27001/27002 ist mittlerweile auch in Deutschland möglich.[3] Die Zertifizierung soll hier bewusst nicht im Vordergrund stehen.

2 August 2019.

3 Die DSGVO fordert in Artikel 42 von Mitgliedstaaten, Kommission und Aufsichtsbehörden die Förderung und Einführung eines Datenschutzzertifikats. Es gibt jedoch in Deutschland noch keine Zertifizierungsstellen und noch keine DSGVO-Zertifikate im Sinne des Artikels 42. Auch eine Zertifizierung nach der Norm ISO 27701 entspricht nicht der DSGVO.

3 INHALT DER ISO 27701

Der offizielle und übersetzte Titel der Norm ISO/IEC 27701:2019-08 lautet „Informationstechnik – Sicherheitsverfahren – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutzmanagement – Anforderungen und Leitfaden".

Der Titel nimmt viel vom 60-seitigen Inhalt und seiner Zielsetzung vorweg. Die ISO 27701 erweitert ein bestehendes (nicht notwendigerweise zertifiziertes) Informationsmanagementsystem nach ISO 27001 und seine technische und organisatorische Umsetzung nach ISO 27702[4] zur Schaffung eines integrierten Managementsystems für Informationssicherheit und Datenschutz.

Konkret wird in der ISO 27701 sowohl der Managementrahmen in zwei Kapiteln erweitert, zudem erfahren 31 der insgesamt 114 Sicherheitsmaßnahmen der ISO 27001/ISO 27002 Ergänzungen und 49 zusätzliche datenschutzspezifische Maßnahmen werden formuliert. Letztere teilen sich in 31 Maßnahmen für die „verantwortliche Stelle"[5] von pbD und 18 für den sogenannten Auftragsverarbeiter von pbD auf.

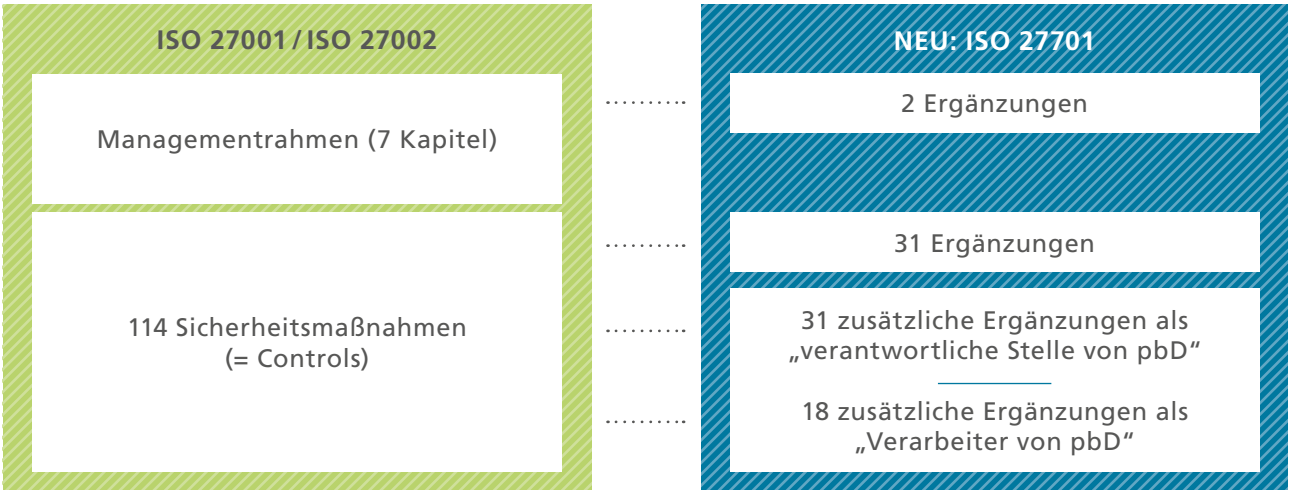

Abbildung 1: Um die Anforderungen zum Schutz personenbezogener Daten in ein bestehendes ISMS zu integrieren, sind zwei Ergänzungen im Managementrahmen nötig; ein gutes Drittel von Sicherheitsmaßnahmen erfährt Erweiterungen und bis zu 49 spezifische Maßnahmen können zusätzlich nötig werden. Muss-Anforderungen finden sich nur im Kern des Managementsystems der ISO 27001. Alle anderen Anforderungen sind Soll-Anforderungen, die bei entsprechender Begründung/mangelnder Relevanz entfallen.

4 Die ISO 27002 stellt eine Detaillierung von 114 im Anhang der ISO 27001 aufgeführten Sicherheitsmaßnahmen (Controls) dar.
5 Art. 4 Nr. 7 DSGVO: Verantwortlicher ist demnach die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

3.1 Synergie in Kernprozessen – allen voran eine einheitliche Risikobewertung

Im Managementrahmen der ISO 27001 werden wie in jeder anderen Norm für Managementsysteme mit einer sogenannten High-Level-Struktur sieben grundlegende Aspekte (Kontext der Organisation, Führung, Planung, Support, Betrieb, Leistungsbewertung und Verbesserung) zwingend gefordert. Die ISO 27701 ergänzt vor allem einen ganz besonderen Kernprozess: den der Planung (Kap. 6 der ISO 27001).

Die Planung der Informationssicherheit basiert auf dem Umgang mit Risiken. Hier setzen die zusätzlichen Datenschutzanforderungen an und dies führt zu maßgeblichen Synergieeffekten. Nahezu jede Entscheidung bezüglich der Informationssicherheit ist eine Abwägung zwischen Risiken und Chancen. Typischerweise wird die Gefährdung von Informationen und ihrer Träger (z. B. IT-Systeme, Anwendungen oder Services) systematisch in einer Risikoidentifikation erfasst, analysiert und bewertet. Das Risikomanagement kann nach der allgemeingültigen Norm ISO 31000, nach einer ihrer Ableitung für die Informationssicherheit gemäß der ISO 27005 oder auch nach dem BSI-Standard 200/3[6] erfolgen. In der Regel werden für eine typische Organisation Hunderte bis Tausende (!) von Einzelrisiken identifiziert und bewertet. Dieses arbeitsintensive Fundament rechtfertigt kein eigenes Risikomanagement für eine Untermenge von Informationen – den personenbezogenen Daten. Ohne Weiteres kann die potenzielle Beeinträchtigung des „vierten" Schutzziels in allen relevanten Assets (Anwendungen, IT-Systeme, Netze, Personal, Gebäude, Compliance etc.) als weitere Komponente ergänzt werden. Zusätzliche Kategorien von Gefährdungen zur Behandlung des Datenschutzes sind zunächst nicht nötig, da sich bereits einschlägige im BSI-Standard 200/3 befinden wie: „Verstoß gegen Gesetz und Regelungen"[7] oder „Missbrauch personenbezogener Daten"[8]. Der Standard ließe jedoch auch weitere Gefährdungen zu, um die Besonderheit von Geschäftsprozessen oder eingesetzten neuen Technologien (z. B. maschinelle Lernverfahren) und Anwendungen zu berücksichtigen.

Das Risiko für Betroffene kann so einfacher identifiziert und auch bewertet werden. Das Schadensausmaß als ein Faktor des Risikowerts kann sich aus Sicht des Unternehmens an potenziellen Bußgeldern[9] orientieren. Das Ergebnis einer konsolidierten Risikobewertung von Informationssicherheit und Datenschutz bietet die Möglichkeit, Risiken wirtschaftlicher zu behandeln. Fehlplanungen werden verringert und begrenzte Ressourcen zielgerichteter eingesetzt. Es können jedoch auch etwaige Zielkonflikte zwischen Maßnahmen zur Erhöhung der Informationssicherheit und des verbesserten Schutzes von pbD vor ihrer Umsetzung im Schritt der Risikobehandlung erkannt werden. Zum Beispiel wird ein verstärktes Logging den betrieblichen Datenschutz und die Mitbestimmung tangieren oder eine integritätsgeschützte digitale Langzeitarchivierung Löschanfragen erschweren. All dies kann früher und umfassender erkannt werden.

6 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html (zuletzt besucht am 25.02.2021).
7 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Elementare_Gefaehrdungen.pdf?__blob=publicationFile&v=4 (zuletzt besucht am 25.02.2021).
8 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Elementare_Gefaehrdungen.pdf?__blob=publicationFile&v=4l (zuletzt besucht am 25.02.20021).
9 Als Quelle kann dienen: https://www.enforcementtracker.com/ (zuletzt besucht am 26.10.2020). Das Berechnungsmodell für Bußgelder ist in https://www.datenschutzkonferenz-online.de/media/ah/20191016_bußgeldkonzept.pdf (zuletzt besucht am 26.10.2020) ausgeführt.

Eine einheitliche Risikobetrachtung beschleunigt auch massiv typische datenschutzrechtliche Herausforderungen wie die Erstellung einer Datenschutz-Folgenabschätzung[10] (DSFA). Diese wird insbesondere bei der Verarbeitung von pbD nötig, die eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen durch eine automatisierte Verarbeitung vorsehen und welche massive Auswirkung auf die Betroffenen haben kann (Stichwort Profiling). Einschlägige Anleitungen zur Erstellung einer DSFA wie der Bitkom-Leitfaden[11], das Whitepaper des Forums

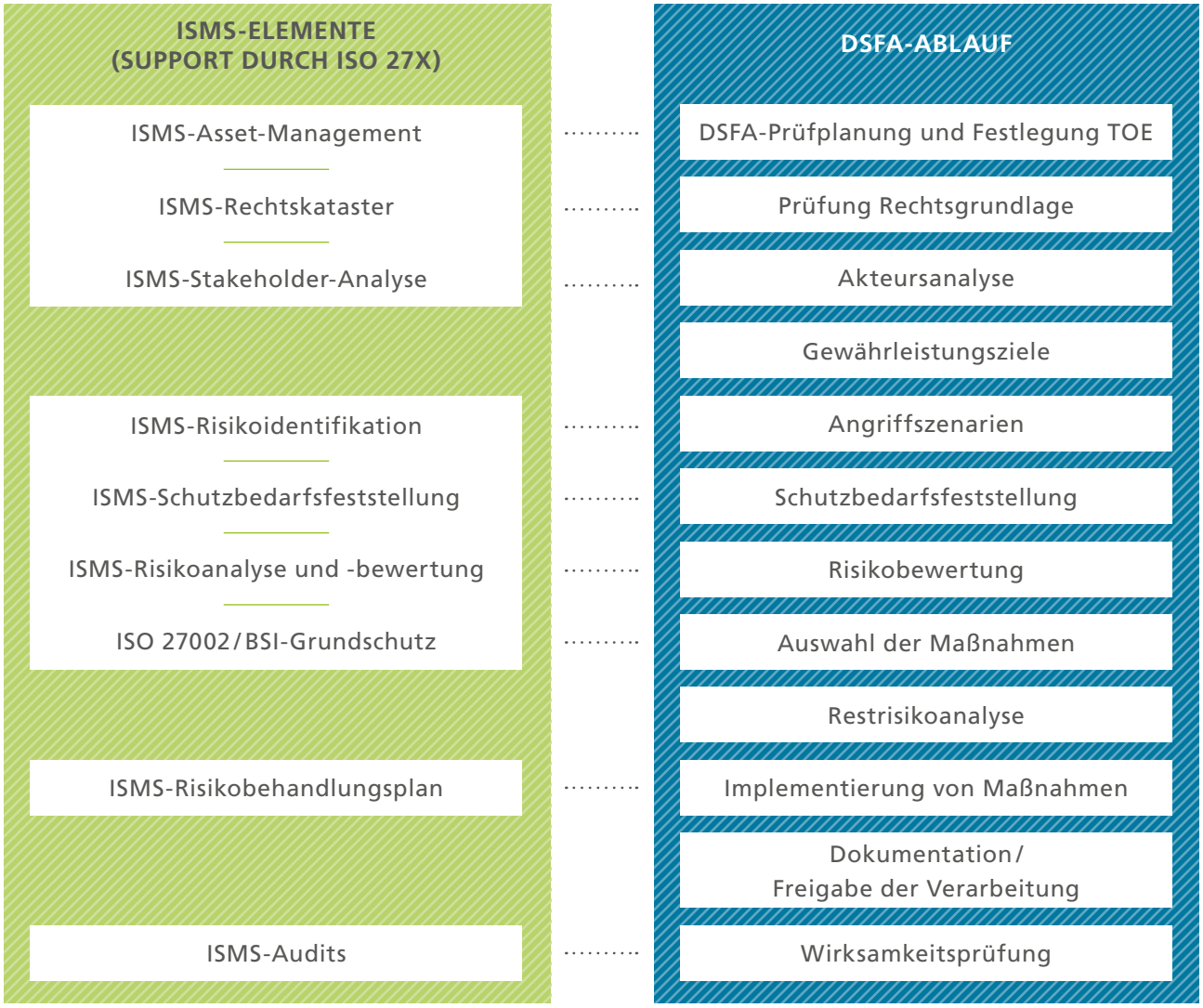

Abbildung 2: Die Schritte einer DSFA (blau) können in ein Flussschema gebracht werden, ein Ansatz ist in dem folgenden „Planspiel" (https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf, zuletzt besucht am 26.10.2020) dargestellt. Dieser wurde hier adaptiert. Die grün hinterlegten Schritte sind Elemente eines ISMS, diese können maßgeblich als Input für die korrespondierenden DSFA-Schritte dienen.

10 https://dsgvo-gesetz.de/themen/datenschutz-folgenabschaetzung/ (zuletzt besucht am 25.02.2021).
11 https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html (zuletzt besucht am 26.10.2020).

Privatheit[12] oder die ISO 21943 (Leitfaden zur Datenschutz-Folgenabschätzung) verdeutlichen die Herausforderungen: Ohne tiefgreifende Kenntnis genutzter Anwendungen, IT-Systeme oder den Kreis der Berechtigten lassen sich die geforderten Angriffsszenarien kaum erfassen oder bewerten. Die ISMS-Risikoanalyse, welcher eine umfassende Erfassung aller Assets und damit aller obigen Bausteine zugrunde liegt, hilft an dieser Stelle mit wichtigen Vorarbeiten.

Zwei wichtige Unterschiede zwischen der ISMS-Risikobetrachtung und einer DSFA sind jedoch zu beachten:

- Die DSFA nimmt konsequent den Betroffenen in den Blick. „Angreifer" im Sinne von Dritten mit Einfluss auf die Rechte und Freiheiten natürlicher Personen können auch Innentäter, staatliche Stellen, die Organisation bzw. das Unternehmen selbst, Auskunfteien etc. sein. Im ISMS ist die Risikobetrachtung hingegen auf die Organisation bzw. das Unternehmen ausgerichtet und betrachtet Risiken auf Stakeholder nur mittelbar. Grundsätzlich kann ein ISMS auch die DSFA unterstützen mit einer vorhandenen Stakeholder-Analyse, mit einem Rechtsregister, mit einem dokumentierten Umgang mit diesen Anspruchsgruppen oder auch mit klaren Regelungen im Falle von Hausdurchsuchungen.
- Und auch ein zweiter Unterschied bleibt. Im ISMS besteht die Möglichkeit, Risiken zu akzeptieren und sie bewusst nicht zu behandeln bzw. sie nicht durch weitere Maßnahmen zusätzlich zu reduzieren. Dies ist sinnvoll, wirtschaftlich und je nach Risikoappetit für jede Organisation individuell festgelegt. In einer DSFA identifizierte Risiken, die z. B. nur für eine vergleichsweise kleine Gruppe von Betroffenen bezüglich pbD zutreffen, können nicht gemäß dieser Logik einfach akzeptiert werden. Diese müssen durch geeignete Sicherheitsmaßnahmen behandelt werden. Aber auch hier bietet das ISMS in der Regel Lösungen. Auch wenn Risiken akzeptiert werden, herrscht in Organisationen zumeist eine nachweisbare Basishygiene, die geeignet ist, mit diesen Datenschutzrestrisiken umzugehen: Dazu können Prinzipien wie Need-to-Know, Verschlüsselung von E-Mail-Kommunikation, Festplatten oder Back-ups, sichere Aufbewahrung und viele weitere Maßnahmen, die in der sogenannten Anwendungserklärung[13] eines ISMS festgehalten sind, dienen.

Die zweite Erweiterung durch die ISO 27701 im Managementrahmen wirkt selbstverständlich. Sie fordert, dass der Geltungsbereich aller Bemühungen nicht bewusst die Anforderungen im Umgang mit besonderen personenbezogenen Daten ausklammern darf. Mit anderen Worten: Man kann es sich nicht zu einfach machen und besonders kritische Geschäftsbereiche herausnehmen, um die Aufwände zur Erreichung der Normkonformität künstlich zu senken.

12 https://www.forum-privatheit.de/download/datenschutz-folgenabschaetzung-3-auflage-2017/ (zuletzt besucht am 26.10.2020).
13 Ein ISMS nach ISO 27001 ist verbunden mit einer Erklärung der Anwendbarkeit. Diese ist Ergebnis der Risikoeinschätzung und stellt die Verknüpfung zur Risikobehandlung dar. Sie legt fest, welche Maßnahmen aus dem Anhang der ISO 27001 bzw. aus der ISO 27002 (idealerweise für welche Assets) ergriffen werden und auch auf welche Art und Weise.

3.2 Synergien bei umgesetzten Sicherheitsmaßnahmen – einige Beispiele

Die eigentliche Umsetzung von Informationssicherheitsmaßnahmen erfolgt nach 114 Sollvorgaben im Anhang der ISO 27001 oder ihrer detaillierten Ausführung in der ISO 27002. Gut ein Viertel dieser Maßnahmen ergänzt die ISO 27701, zum Beispiel:

- Vorhandene Richtlinien, Leitfäden und Sicherheitskonzepte der Informationssicherheit können um das Schutzziel und die Aspekte des Datenschutzes erweitert werden. Widersprüchliche Anweisungen und kollidierende Umsetzungen entfallen. Z. B. bietet es sich an, in einem bestehenden Kryptografiekonzept auch den Schutz von (besonders kritischen) pbD mit zu berücksichtigen. So können die Gesamtheit aller eingesetzten kryptografischen Verfahren und damit verbundene Maßnahmen (z. B. Handhabung von Schlüsseln) einheitlich und umfassend betrachtet werden.
- Bewusstsein der Mitarbeitenden: Die Sensibilisierung für den richtigen Umgang mit Informationen kann ohne Weiteres den Umgang von personenbezogenen Daten mit beinhalten. Die Unterstützung bei der Meldung von Vorfällen gilt allgemein und ist oft essenziell für das Security-Incident-Management bzw. für die Meldung von Datenschutzvorfällen.
- Die Erstellung eines Löschkonzepts personenbezogener Daten, z. B. nach DIN 66398, setzt unter anderem die Identifikation von Datenarten voraus, um Löschklassen zu bilden, Löschregeln gemäß gesetzlichen Vorgaben zu formulieren und Umsetzungsvorgaben in Anwendungen und Prozessen zu implementieren. Bei dieser vielschichtigen Inventarisierungsaufgabe unterstützt eine Übersicht über alle im Unternehmen eingesetzten Anwendungen und IT-Systeme die unterstützten Geschäftsprozesse und die jeweiligen Ansprechpartner:innen und Lieferant:innen. Diese Übersicht leistet eine „Inventur der Informationswerte“ – also das Asset-Management im ISMS.
- Die ISO 27001 stellt unter anderem bei der sicheren Softwareentwicklung auf die Berücksichtigung von Sicherheitsanforderungen oder die Handhabung von Test- und Entwicklungsdaten ab. Anforderungen eines Privacy-by-Designs können zusätzlich mitbeachtet werden oder auch die Erstellung von Test- und Entwicklungsdaten kann zusätzlich datenschutzkonform gestaltet werden.

Diese und weitere zusätzliche Anforderungen wirken beim Lesen aus zwei Gründen vertraut: Typische Sicherheitsmaßnahmen werden zum einen erweitert, zum anderen werden unmittelbar Forderungen der DSGVO bedient. Alle Forderungen der Verordnung lassen sich jedoch nicht in etablierten Sicherheitsmaßnahmen als Ergänzung unterbringen. Die ISO 27701 formuliert aus diesem Grund zusätzliche Anforderungen, die sich speziell an die verantwortliche Stelle oder speziell an den Auftragsverarbeiter von personenbezogenen Daten richten. Aber auch hier können Prozesse und Maßnahmen eines ISMS helfen, schneller und besser zum Ziel zu kommen.

3.3 Zusätzliche Anforderungen

Die verantwortliche Stelle entscheidet über die Zwecke und Mittel der Verarbeitung personenbezogener Daten. Die Verantwortung kann durchaus geteilt werden und bei mehreren Organisationen liegen, hier spricht man von gemeinsamer[14] verantwortlicher Stelle. In diesem Normabschnitt werden Anforderungen formuliert, die sich wie oben schon angedeutet nicht unmittelbar mit bestehenden Sicherheitsmaßnahmen verknüpfen lassen.

Zusätzliche Anforderungen sind z. B. die Erstellung und Pflege der Verfahren der Verarbeitungstätigkeiten, angemessene Reaktion auf Änderungen im Umgang mit dem Zweck der Verarbeitung, die transnationale Übertragung von Informationen (Cloud) oder die Kenntnis von Flüssen personenbezogener Daten (data flow/data maps). Ein etabliertes Asset- und Änderungsmanagement vereinfacht bzw. ermöglicht diese Punkte. Andere Anforderungen bedienen den Einsatz von Verfahren zur automatisierten Entscheidungsfindung oder die Zerstörung von Informationsträgern. Auch hier kann ein Anforderungs- und Risikomanagement im Rahmen des ISMS helfen bzw. die nachweisliche Zerstörung von Informationen nach DIN 66399.

Um die DSGVO voll abzudecken, richten sich schließlich 18 zusätzliche Anforderungen an Auftragsverarbeiter von personenbezogenen Daten. Diese reichen von der Vertragsgestaltung zwischen Verarbeiter und Kunde über die Trennung von Mandaten bis zum Umgang mit weiteren Unterauftragnehmern. Und auch hier ist das ISMS eine Möglichkeit, ergriffene technisch-organisatorische Maßnahmen als Vertragsbestandteil aus etablierten Sicherheitsmaßnahmen abzuleiten. Die Trennung von Mandaten kann beliebig komplex sein, hier können typische Sicherheitsmaßnahmen – z. B. Verfahren zur Trennung von Systemen, Anwendungen, Rollen, Netzen etc. – Ansätze liefern.

Es gibt einige Anforderungen der ISO 27701, die weder eine direkte Entsprechung in ISO 27001/27002 aufweisen, noch unmittelbar durch das ISMS unterstützt werden können. Beispielhaft sei die Anfertigung von Datenauszügen von Betroffenen oder die Umsetzung von Transparenz- und Informationspflichten oder das Management von Einwilligungen/Änderungen von Einwilligungen genannt.

14 Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche.

4 FAZIT

Der Anhang der ISO 27701 enthält mehrere Zuordnungstabellen zwischen den in der Norm aufgeführten Controls/Maßnahmen und den Anforderungen der ISO 29100 (Rahmenwerk Datenschutz), relevanten Anforderungen der ISO 27018 (Standard für Datenschutz im Cloud-Bereich) und relevanten Anforderungen der ISO 29151 (Leitfaden für den Schutz personenbezogener Daten). So können bereits unternommene Anstrengungen auf Basis dieser Leitlinien zeitsparend identifiziert und übernommen werden.

Das wichtigste Mapping besteht jedoch zwischen den Maßnahmen der ISO 27701 und ihren Bezügen zu den Artikeln der DSGVO. Dies gestattet eine Standortbestimmung bezüglich der „Compliance-Reife"; dies unterstützt aber auch bei Auskünften gegenüber Kunden oder dem Nachweis gegenüber Aufsichtsbehörden.

Die ISO 27701 ändert nichts an der Tatsache, dass Managementsysteme in der Initiierung und auch in der Pflege aufwendig sind. Die neue Norm spielt ihre Vorteile jedoch nicht erst bei ihrer vollen und nachweisbaren Umsetzung aus. Sie kann durchaus auch peu à peu oder auch nur punktuell angewandt werden. Viele Ergänzungen zur Informationssicherheit führen zu schnellen Ergebnissen und bedürfen nur geringer Anpassungen in Prozessen, Konzepten, Richtlinien oder der Kommunikation. Der Nutzen tritt schnell und vielfältig zutage. Dies reicht von Verbesserungen im Umgang mit Anfragen Betroffener, bei internen Schulungen, in Beschaffungsprozessen, in der Entwicklung von Produkt- und Dienstleistungen, in der Vorfallsbehandlung oder im Vertragsmanagement.

Das ist auch der Grund, warum eine Zertifizierungsfähigkeit im Sinne der DSGVO zweitrangig ist; die ISO 27701 ist vielmehr eine wichtige Richtschnur zur Würdigung und rechtssicheren Umsetzung der DSGVO und zwar mit geringerem Einsatz, insbesondere bei der Entwicklung neuer digitaler Produkte.

www.smartservicewelt.de