CHRISTOPHER ZERRES

MARKETING

Schriftenreihe „Arbeitspapiere für Marketing und Management“

Herausgeber:
Prof. Dr. Christopher Zerres

Hochschule Offenburg
Fakultät Medien

Arbeitspapier Nr. 61

Prinzipien und Elemente eines Datenschutzmanagementsystems

Kling, M., Zerres, T., Zerres, C.

Offenburg, Oktober 2021

ISSN: 2510-4799

Impressum

Prof. Dr. Christopher Zerres
Hochschule Offenburg
Fakultät Medien
Badstraße 24
77652 Offenburg

ISSN: 2510-4799

Inhalt

Ziel dieses neuen Arbeitspapieres ist es, vor dem Hintergrund der Entwicklungslinien des Datenschutzes, eine fundierte und gleichzeitig praxisnahe Darstellung der Prinzipien und der Elemente eines Datenschutzmanagementsystems vorzunehmen.

1 EINFÜHRUNG

Durch die Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung (DS-GVO)), die am 25. Mai 2016 in Kraft getreten ist und nach einer zweijährigen Übergangsfrist seit dem 25. Mai 2018 in Europa unmittelbar gilt, wurden die datenschutzrechtlichen Anforderungen an Unternehmen erhöht[1] und der Bußgeldrahmen für Verstöße gegen die datenschutzrechtlichen Regelungen verschärft.[2] Mit der DS-GVO wurde ein Bußgeldrahmen von bis zu 20 Millionen Euro eingeführt. Für Unternehmen kann das Bußgeld zudem bis zu 4 % des gesamten, weltweit erzielten Vorjahresumsatzes betragen.[3] Diese Art der Bußgeldbemessung ist in Deutschland bereits aus dem Kartellrecht bekannt.[4] Dort setzen die zuständigen Behörden seit langem die Bußgelder auf der Grundlage des Unternehmensumsatzes fest. Zudem fügte der europäische Gesetzgeber dem Erwägungsgrund (ErwG) 150 der DS-GVO noch vor Ende der Trilog-Verhandlungen den Hinweis hinzu, dass bei Geldbußen gegen Unternehmen der Begriff des Unternehmens im Sinne des Artikel 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Anwendung findet.[5] Deshalb gilt bei Sanktionen gegen Unternehmen der kartellrechtliche Unternehmensbegriff, was insbesondere bei Konzernen beziehungsweise Unternehmensverbünden einen signifikanten Einfluss auf die Höhe des Bußgeldes haben kann, da der Konzernumsatz als Berechnungsgrundlage für Bußgelder herangezogen wird.

Mit der DS-GVO wurden zudem die Grundsätze für die Verarbeitung personenbezogener Daten eingeführt, welche in Art. 5 DS-GVO festgelegt sind. Hierzu gehört auch der Grundsatz der Rechenschaftspflicht[6] nach Art. 5 Abs. 2 DS-GVO. Demnach hat der Verantwortliche nicht nur die Einhaltung der Grundsätze sicherzustellen, sondern muss deren Einhaltung auch nachweisen können.[7] Diese Pflicht besteht grundsätzlich bei der Verarbeitung personenbezogener Daten und damit unabhängig von einem konkreten Vorfall oder Verstoß.[8] Auch aus anderen Artikeln der DS-GVO ergeben sich Nachweispflichten für den Verantwortlichen. Zu diesen Vorgaben gehören beispielsweise Art. 24 DS-GVO mit der Verantwortung des für die Verarbeitung Verantwortlichen, Art. 30 DS-GVO über das Führen eines Verzeichnis von Verarbeitungstätigkeiten[9], Art. 33f. DS-GVO über die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde einschließlich deren Dokumentation gemäß Art. 33 Abs. 5 DS-GVO[10], Art. 7 Abs. 1 DS-GVO zur Nachweispflicht für

[1] Vgl. Von Schenck/Mueller-Stöfen, GWR (2017) – S. 171 ff.
[2] Vgl. EP-Ausschuss: Bürgerliche Freiheiten, Justiz und Inneres (LIBE) LIBE-Ausschuss des Europäischen Parlaments (2015) – S. 3; Schrulle, IT-Governance (2019) – S. 25.
[3] Vgl. Art. 83 Abs. 5 DS-GVO.
[4] Vgl. Art. 23 Abs. 1, 2 Satz 2 der VO (EG) Nr. 1/2003 des Rates vom 16.12.2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln.
[5] Vgl. Faust/Spittka/Wybitul, ZD (2016) – S. 120.
[6] In der englischen Fassung: Accountability.
[7] Vgl. Heberlein, in: Ehmann/Selmayr (2018) Art. 5, Rn. 29; Veil, ZD (2018) – S. 9; Schrulle, IT-Governance (2019) – S. 25.
[8] Vgl. Schrulle, in: Sowa (2020) – S. 22.
[9] Auch Verarbeitungsverzeichnis genannt.
[10] Vgl. Art. 28, insbes. Abs. 3, S. 2 lit. h) für den Auftragsverarbeiter.

die Einwilligung[11] sowie zum Nachweis des fehlenden Verschuldens gemäß Art. 82 Abs. 3 DS-GVO. Um nachweisen zu können, dass kein Verschulden seitens des Verantwortlichen vorliegt, muss dieser beweisen, dass die datenschutzrechtlichen Vorschriften eingehalten wurden. Dies setzt voraus, dass die Verarbeitungen dokumentiert wurden, was die Arbeit der Aufsichtsbehörden erleichtert.[12]

Für die Gewährleistung einer umfassenden Dokumentation dieser Vorgänge und den Grundsatz der Rechenschaftspflicht zu erfüllen, ist ein Konzept notwendig, welches sämtliche Verarbeitungen von personenbezogenen Daten berücksichtigt.[13] Innerhalb der DS-GVO ist keine Norm abgebildet, die zur Implementierung eines Datenschutzmanagementsystems (DSMS) verpflichtet[14]. Allerdings erwachsen aus Art. 5 Abs. 2 und Art. 25 Abs. 1 DS-GVO bereits Pflichten[15], die nach Meinungen in der Literatur nur durch das Führen eines ganzheitlichen und nachhaltigen DSMS abgebildet und kontrolliert werden können.[16] Auch aus der Formulierung des Art. 24 DS-GVO lässt sich ableiten, dass für die Umsetzung der Nachweispflicht ein funktionierendes DSMS notwendig ist.[17] Das Führen eines Verarbeitungsverzeichnisses gemäß Art. 30 DS-GVO sowie das bedarfsweise Reagieren kann dem Grundsatz der Rechenschaftspflicht nicht gerecht werden.[18] Ein DSMS kann den Vorwurf der Fahrlässigkeit bei achtlos verursachten Datenschutzverstößen nicht entkräften, die Aufsichtsbehörden berücksichtigen das System jedoch bußgeldmindernd gemäß Art. 79 Abs. 2a lit. m) DS-GVO. Durch ein effizientes DSMS werden eine Verringerung der Anzahl von Datenschutzvorfällen durch eine entsprechende Sensibilisierung der Mitarbeiter, eine schnelle Reaktion auf Datenschutzvorfälle und das Ergreifen von Maßnahmen möglich, um den entstehenden Schaden der betroffenen Personen sowie beim Unternehmen möglichst gering zu halten.[19] Sowohl Gegenmaßnahmen als auch die Kooperation mit der zuständigen Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern, sind nach Art. 83 Abs. 2 lit. c) und lit. f) DS-GVO von den Aufsichtsbehörden zu berücksichtigen.

Für Unternehmen sind die Bündelung und die Überführung von Einzelmaßnahmen in ein DSMS angesichts des gestiegenen Bußgeldrisikos nahezu unumgänglich.[20] Außerdem kann durch die Einführung eines solchen Systems die persönliche Haftung der Vorstände und Geschäftsführer vermieden werden.[21] Allerdings ist die Kenntnis beziehungsweise die Information der Unternehmensleitung über die Wirksamkeit des Systems in angemessener Weise erforderlich.[22] Ein DSMS einzurichten bedeutet deshalb nicht, dass lediglich Planung und Umsetzung durchgeführt werden, sondern auch das System stetig weiterzuentwickeln und an das Unternehmen, dessen Veränderungen und die Veränderungen der Unternehmensumwelt anzupassen.[23] Ein DSMS soll nicht ausschließlich den Datenschutz systematisieren,

[11] Vgl. hierzu auch ErwG 42.
[12] Vgl. *Albrecht/Jotzo*, in: Albrecht/Jotzo (2017) – S. 56, Rn. 19.
[13] Vgl. Schrulle, IT-Governance (2019) – S. 25.
[14] Vgl. Hansch, ZD (2019) – S. 245.
[15] Veil identifiziert 68 Pflichten für den Datenverarbeiter, vgl. Veil, CR-online (2018) – Nr. 18; Veil, in: Gierschmann/Schlender/Stentzel/Veil (2018) – Art. 24, Rn. 45.
[16] Vgl. Veil, in: Gierschmann/Schlender/Stentzel/Veil (2018) Art. 24, Rn. 7; Schrulle, IT-Governance (2019) – S. 25; Meyer/Struck/Bitsch (2020); Paal, in: Paal/Pauly (2021) – Art. 15, Rn. 15.
[17] Vgl. Meyer/Struck/Bitsch (2020).
[18] Vgl. Jung, CCZ (2018) – S. 224.
[19] Vgl. Faust/Spittka/Wybitul, ZD (2016) – S. 125.
[20] Vgl. Veil, in: Gierschmann/Schlender/Stentzel/Veil (2018) – Art. 24, Rn. 74.
[21] Vgl. LG München I, Urteil vom 10.12.2013 – 5 HK O 1387/10; ausführlich Schmidt, in: Hauschka/Moosmayer/Lösler (2016) – § 45, Rn. 4 ff.; Poppe, in: Inderst/Bannenberg/Poppe (2017) – Kapitel 1.3, Rn. 11.
[22] Vgl. Poppe, in: Inderst/Bannenberg/Poppe (2017) – Kapitel 1.6, Rn. 32 und 35.
[23] Vgl. Jung, CCZ (2018) – S. 224.

sondern auch notwendige Anpassungen innerhalb des Systems frühzeitig identifizieren. Weiterhin soll eine Messung ermöglicht werden, die Rückschlüsse auf die Funktionsfähigkeit erlaubt. Dies ist vergleichbar mit der Nullfehlerquote, welche aus der industriellen Qualitätssicherung bekannt ist.[24]

Richtlinien aufzustellen und Handlungsanweisungen zu erlassen, sind unzureichend. Zusätzlich wird eine Messung des Reifegrads beziehungsweise der Wirksamkeit der Einhaltung datenschutzrechtlicher Normen benötigt, um zu prüfen, ob durch die geschaffene Struktur die gesetzlichen Rahmenbedingungen tatsächlich eingehalten werden können. Bestehende Systeme sollten daher regelmäßig überprüft werden. Dabei kann verifiziert werden, ob die getroffenen Maßnahmen zu einer effektiven Vermeidung von Datenschutzverstößen führen.[25] Sind die getroffenen Maßnahmen nicht effektiv, so ist zu hinterfragen, was geändert werden muss, damit diese effektiv werden. Die Messung, Analyse und Auswertung von Effektivität und Effizienz des Systems zur Schadens- und Bußgeldvermeidung sind notwendige Prozessschritte. DRUCKER stellte bereits fest: „*If you can‘t measure it, you can’t manage it.*“[26]
Entwicklung des Datenschutzes

2 ENTWICKLUNG DES DATENSCHUTZES

2.1 IN DEUTSCHLAND

Der Datenschutz in Deutschland wurde erstmals 1970 kodifiziert, als das Bundesland Hessen das weltweit erste stringent ausformulierte Datenschutzgesetz verabschiedete.[27] Dieses beruhte noch auf einem anderen Verständnis des Datenschutzes, worunter im Wesentlichen der Schutz der Daten selbst zu verstehen war.[28] Den Grundstein für das heute gültige Verständnis des Begriffs Datenschutz lieferte SEIDEL zur selben Zeit, indem er den Datenschutz als Persönlichkeitsschutz an personenbezogenen Daten insgesamt definierte.[29] Sieben Jahre später folgte das erste deutsche Bundesdatenschutzgesetz (BDSG 1977), das bereits auf dem Verbotsprinzip mit Erlaubnisvorbehalt basiert, welches aus der DS-GVO bekannt ist. Somit sind alle Datenverarbeitungen als missbräuchlich qualifiziert, welche auf keiner gesetzlichen Grundlage beruhen.[30] Bis Anfang der achtziger Jahre folgten die restlichen Bundesländer und verabschiedeten eigene Landesdatenschutzgesetze.

Der Grundstein des heutigen Datenschutzes in Deutschland wurde allerdings erst im Jahr 1983 gelegt, als das Bundesverfassungsgericht im sogenannten Volkszählungsurteil feststellte, dass auch Datenverarbeitungen, die auf einer gesetzlichen Grundlage beruhen, einen unzulässigen Eingriff in die Grundrechte der Betroffenen darstellen können. Dies wurde unter anderem damit begründet, dass bei Unwissenheit von Menschen, was und wann etwas von ihnen aufgezeichnet oder anderweitig dokumentiert wird, sich jede Person unweigerlich anders verhalten und sie somit nicht mehr frei über ihre Handlungen entscheiden würde. Das Volkszählungsurteil prägte das datenschutzrechtliche Verständnis nachhaltig, indem das sogenannte „Recht auf informationelle Selbstbestimmung“ als Grundrecht formuliert wurde,

[24] Vgl. *Faust,* in: Schimansky/Bunte/Lwowski (2017) – § 109, Rn. 124a.
[25] Vgl. *Schrulle*, in: Sowa (2020) – S. 22.
[26] Vgl. Jüttner, CCZ (2018) – S. 169.
[27] Vgl. Dr-Datenschutz.de (2014); Seidel/Seidel, ZD (2020) – S. 109.
[28] Vgl. Seidel/Seidel, ZD (2020) – S. 109.
[29] Vgl. Seidel, NJW (1970) – S. 1581ff.
[30] Vgl. Art. 6 Abs. 1 DS-GVO.

welches sich aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG) i. V. m der Menschenwürde (Art. 1 Abs. 1 GG) ableitet.[31] Als Teil des allgemeinen Persönlichkeitsrechts wird den betroffenen Personen das Recht gewährt, selbst über die Preisgabe und die Verwendung ihrer persönlichen Daten zu entscheiden. Ursprünglich war das Grundrecht jedoch als Abwehrrecht gegen die Datenerhebungen des Staates konzipiert. Das Volkszählungsurteil war der Anstoß, dass Bund und Länder die bestehenden Datenschutzgesetze reformierten und darüber hinaus neue bereichsspezifische Datenschutzgesetze schufen.

2.2 INTERNATIONAL

International wurde bereits vor einigen Jahren die Wichtigkeit des Datenschutzes erkannt, weshalb schon im Jahr 1995 die erste europäische Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Richtlinie 95/46/EG) verabschiedet wurde. Da Richtlinien allerdings keine unmittelbare Rechtswirkung entfalten, musste diese Richtline erst in nationales Recht umgesetzt werden, weshalb dies beispielsweise in Deutschland erst 2001 durch die Novellierung des BDSG erfolgte. In den folgenden Jahren wurden weitere Richtlinien im Datenschutz erlassen. So wurden neue Standards für den Datenschutz in der Telekommunikation 2002 durch die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) gesetzt, welche mit der Novelle des Telekommunikationsgesetzes 2004 in deutsches Recht umgesetzt wurde. Auch 2009 wurde die sogenannte Cookie-Richtlinie (Richtlinie 2009/136/EG) erlassen, welche allerdings nicht rechtzeitig in deutsches Recht umgesetzt wurde, was für eine unklare Rechtslage sorgte.[32]

Durch den Gestaltungsspielraum, welchen die Mitgliedstaaten bei der Umsetzung der Richtlinien in ihr jeweiliges nationales Recht hatten, unterschieden sich die Datenschutzanforderungen innerhalb der Mitgliedstaaten teilweise stark voneinander. Die DS-GVO verfolgte daher das Ziel, den Datenschutz in allen Mitgliedstaaten zu harmonisieren. Anders als die bisherigen Richtlinien ist die DS-GVO als Verordnung unmittelbar in jedem Mitgliedstaat anwendbar. Nach umfangreichen Verhandlungen legte das europäische Parlament Anfang 2014 seinen Vorschlag der DS-GVO vor, welcher am 14. April 2016 beschlossen wurde.[33] Die DS-GVO trat zum 25. Mai 2016 in Kraft und ist nach einer zweijährigen Übergangszeit seit dem 25. Mai 2018 anzuwenden. Seither wird das Thema Datenschutz in der Allgemeinheit häufig mit hohen Bußgeldern und einem hohen bürokratischen Aufwand verbunden. Die Tatsache, dass die betroffenen Personen durch die DS-GVO weitereichende Rechte erhielten, die Verarbeitungen von personenbezogenen Daten transparenter werden mussten und einige Vorschriften auch betriebliche Erleichterungen und wirtschaftliche Chancen mit sich brachten, ging dabei durch die recht einseitige Berichterstattung oftmals unter.

Auch außerhalb der Europäischen Union und des EWR wurde die Wichtigkeit des Datenschutzes erkannt, weshalb einige Länder durch die Bemühungen der DS-GVO auch ihre Datenschutzgesetze überarbeiteten. So trat beispielsweise das türkische Datenschutzgesetz (Turkish Law on the Protection of Personal Data No. 6698) am 7. April 2016 in Kraft, welches sich an der DS-GVO orientiert und auch bei der Überarbeitung von der EU-Kommission unterstützt wurde.[34] Auch Brasilien, was bis zu dem Zeitpunkt weniger sensibel bezüglich des Datenschutzes ausgerichtet war, verabschiedete am 14. August 2018 ein allgemeines Da-

[31] Vgl. Loomans/Matz/Wiedemann (2014) – S.9.
[32] Vgl. Dr-Datenschutz.de (2012).
[33] Vgl. Dr-Datenschutz.de (2013).
[34] Vgl. SüdWest Datenschutz (2018); Öztürk (2019).

tenschutzgesetz („Lei Geral de Proteção de Dados" – LGPD), welches einige Gemeinsamkeiten mit der DS-GVO aufweist und was die Unternehmen in Brasilien dazu zwang, sich völlig neu aufzustellen, um dem neuen Datenschutz zu entsprechen.[35] Hinzu kommen noch weitere südamerikanische und afrikanische Länder, welche sich intensiv mit der DS-GVO auseinandersetzen, um die eigene Gesetzgebung neu auszurichten.[36]

In den USA, welche allgemein weniger mit einem starken Datenschutz in Verbindung gebracht werden[37], wurde bereits 1972 das Recht auf Privatsphäre durch eine Volksinitiative zu der Liste der Grundrechte hinzugefügt und 1974 in der Verfassung verankert.[38] Seither hat der kalifornische Bundesstaat stets zeitnah auf neue Gefahren aus dem Datenschutz reagiert und in Spezialgesetzen reguliert.[39] Bereits seit 2003 sind in Kalifornien Sicherheitsverstöße von Unternehmen zu melden und seit 2004 sind Datenschutzrichtlinien auf Webseiten vorgeschrieben.[40] Am 01. Januar 2020 trat mit dem California Consumer Privacy Act (CCPA) das bisher stärkste „Datenschutzgesetz" in den USA in Kraft.[41] Zwar liegt in dem Gesetz der Fokus auf dem Verbraucherschutz und weniger auf dem Datenschutz, trotzdem stellt das CCPA ein Vorstoß dar, da die personenbezogenen Daten von kalifornischen Verbrauchern geschützt und diesen, wie die DS-GVO, umfangreiche Rechte eingeräumt werden.[42] Weitere Parallelen zur DS-GVO sind beispielsweise die weit gefasste Definition von personenbezogenen Daten sowie die exterritoriale Wirkung des Gesetzes. Mit den US-Wahlen im November 2020 wurde einer Volksinitiative zur Konkretisierung des CCPA, dem California Privacy Rights Act (CPRA), zugestimmt. Durch den CPRA sollen die bestehenden Regelungen des CCPA ausgeweitet werden, wodurch eine weitere Annäherung an die DS-GVO stattfindet.[43] So sind ab dem 01. Januar 2023 bei Verletzungen mit erheblichen Geldstrafen und auch Schadensersatzansprüchen zu rechnen.[44] Außerdem müssen die Anbieter vernetzter Geräte seit dem 01. Januar 2020 in Kalifornien die Produktsicherheit im Hinblick auf den Datenschutz sicherstellen.[45] Dieser Bereich des Datenschutzes ist von der DS-GVO bisher noch nicht berücksichtigt.[46] Auch außerhalb Kaliforniens sind Vorstöße zu beobachten, um ein Datenschutzgesetz in den USA zu etablieren.[47] So stellte der demokratische US-Senator Ron Wyden Mitte April 2021 den „Protecting Americans' Data from Foreign Surveillance Act" vor.[48] Dieser umfasst einen Gesetzesentwurf, der die Weitergabe personenbezogener Daten von US-Bürgern in Länder mit einem unzureichenden Datenschutz beziehungsweise einer unzureichenden Durchsetzung des Datenschutzes beschränken soll, was in ähnlicher Form auch in der DS-GVO integriert ist.[49] Zwar ist davon auszugehen, dass der Gesetzesentwurf nicht in der vorgelegten Form den Senat passieren wird, allerdings wird dadurch deutlich, dass in den USA der Datenschutz und die Privatsphäre verstärkt Bedeutung und Aufmerk-

[35] Vgl. Rödl & Partner (2019).
[36] Vgl. Kranig/Sachs/Gierschmann (2019) – S. 5.
[37] Vgl. Schewior (2021).
[38] Vgl. Kelso (1992) – S. 328; Determann, ZD (2021) – S. 69
[39] Vgl. Determann, ZD (2021) – S. 69.
[40] Vgl. Determann (2020) – Kapitel 1 und 2.
[41] Vgl. Scheben (2021).
[42] Vgl. Figas (2021).
[43] Vgl. Dr-Datenschutz.de (2020).
[44] Vgl. Determann, ZD (2021) – S. 69.
[45] Vgl. California Civil Code § 1798.91.04(a).
[46] Vgl. Determann, ZD (2021) – S. 69.
[47] Vgl. Kleinz (2021); Schewior (2021).
[48] Vgl. Pressemitteilung Ron Wyden: https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments.
[49] Vgl. Art. 45 Abs. 1 DS-GVO.

samkeit erhalten.[50] Die Rolle des Datenschutzes kann dabei sehr unterschiedlich ausfallen. Während in der EU mit der DS-GVO die Privatsphäre der betroffenen Personen im Mittelpunkt steht, wird der Datenschutz in den USA vielmehr als eine Art Handelsgegenstand angesehen und somit eine ökonomische Sichtweise auf den Datenschutz und die personenbezogenen Daten eingenommen. Ebenso wird in den USA der Datenschutz auch oftmals mit der nationalen Sicherheit in Verbindung gebracht.

2.3 Ziele und Aufgaben des Datenschutzes

Durch die wirtschaftlichen und gesellschaftlichen Veränderungen, der immer steigenden Relevanz von Daten, der exponentiell steigenden Datenmenge und der Entwicklung hin zur Informationsgesellschaft erhält der Datenschutz eine steigende Relevanz.[51] Seidel und Seidel gehen davon aus, dass durch die datenintensiven Bereiche, wie Internet of Things (IoT) und künstliche Intelligenz, der Grundsatz der Datensparsamkeit bereits ausgehebelt wurde.[52] Insbesondere durch die technische Entwicklung, wie Big-Data-Anwendungen und neuen Analysetools, kann der Bezug zu einzelnen Personen vereinfacht hergestellt werden. Der gläserne Konsument ist deshalb bereits zur Realität geworden. Im Mittelpunkt des Datenschutzes stehen daher die betroffenen Personen und deren personenbezogene Daten, welche vor einer missbräuchlichen Verwendung und Verarbeitung zu schützen sind.[53] Somit soll die Privatsphäre geschützt und das Recht auf informationelle Selbstbestimmung durch die Einhaltung der Datenschutzgrundsätze sichergestellt werden (siehe Abb. 1).

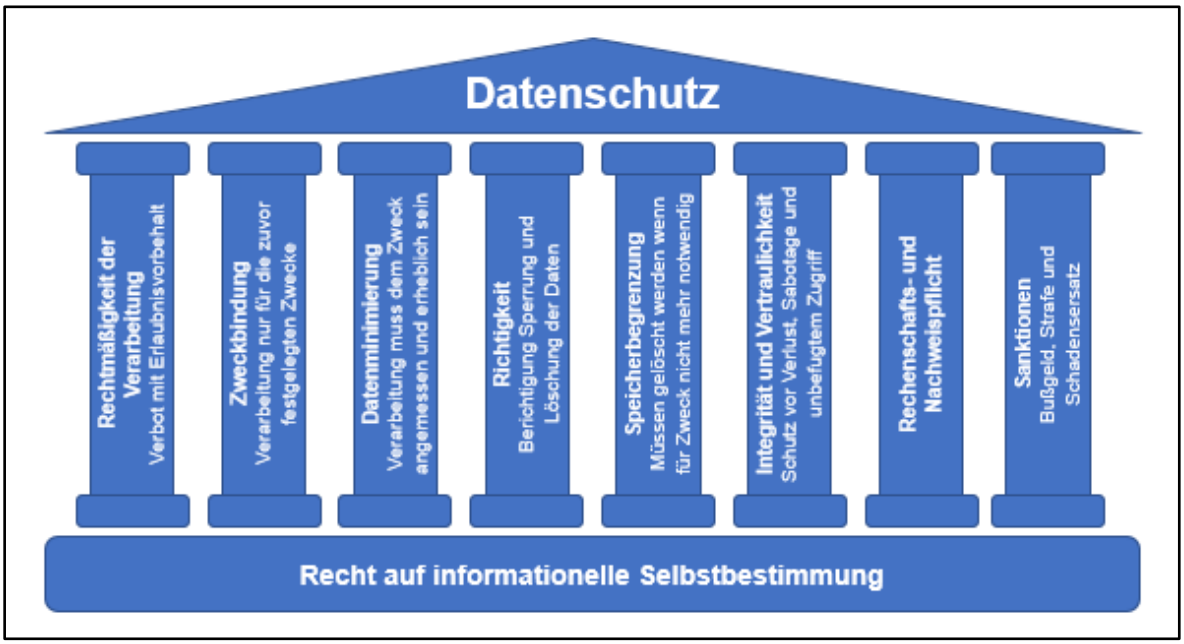

Abb. 1: Ziel und Grundsätze des Datenschutzes[54]

Primäres Ziel des Datenschutzes in einem Unternehmen ist dagegen vorallem die Vermeidung von Datenschutzvorfällen, da diese einen signifikanten Risikofaktor darstellen. Neben finanziellen Belastungen durch mögliche Bußgelder, Schadensersatzforderungen der Be-

[50] Vgl. Schewior (2021).
[51] Vgl. Loomans/Matz/Wiedemann (2014) – S. 7f.
[52] Vgl. Seidel/Seidel, ZD (2020) – S. 109.
[53] Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2020) – S. 5.
[54] Eigene Darstellung.

troffenen und dem internen Aufwand zur Beseitigung des Datenschutzvorfalls, kann ein Datenschutzvorfall zu einem Reputationsschaden werden, von welchem sich das Unternehmen oft lange nicht erholt.[55] Zudem kann eine Datenpanne einen negativen Einfluss auf die Unternehmenskultur und das Vertrauen der Beschäftigten und Kunden haben.[56] Auch im geschäftlichen Verkehr mit anderen Unternehmen können negative Schlagzeilen durch Datenschutzverstöße dazu führen, dass Aufträge an Konkurrenten vergeben werden oder das Unternehmen bei Ausschreibungen nicht berücksichtigt wird. Deshalb ist die Einhaltung der geltenden Datenschutzgesetze und -normen sowie deren Grundsätze für Unternehmen von großer Bedeutung.

3 DATENSCHUTZMANAGEMENTSYSTEM

3.1 BEGRIFF

Aus vielen Bereichen der Unternehmensorganisation ist der Begriff des Managementsystem geläufig. So sind beispielsweise Managementsysteme für die Informationssicherheit[57] (ISO 27001), den Umweltschutz (ISO 14001), den Arbeitsschutz (OHSAS 18001) oder die Compliance (IDW PS 980) bereits etabliert.[58] Hauptmerkmal solcher Managementsysteme ist, dass diese nicht nach der Planung und Durchführung enden, sondern anschließend eine Überprüfung und Verbesserung des Geleisteten stattfindet.[59] Wird ein neues Managementsystem entwickelt, so erfolgt meistens eine Orientierung an vorhandenen Ansätzen für Managementsysteme von internationalen Standards.[60] Bei dem Begriff des Datenschutzmanagement ist deshalb kein System im technischen Sinne gemeint, wie bei einer Software, die beim Management des Datenschutzes unterstützt, sondern vielmehr ein Rahmenwerk, welches die Ziele festlegt und bei der Auswahl der dazu benötigten Werkzeuge unterstützt.[61] Zu einem Managementsystem gehören i. d. R. die nachfolgenden Punkte:

- Richt-, Leitlinien und Arbeitsanweisungen
- Verfahren, Prozesse und Methoden
- Dokumente, Aufzeichnungen und weitere Dokumentation
- Regelmäßige Überprüfungen

Ein DSMS bezeichnet somit die Gesamtheit der Maßnahmen eines Unternehmens, um den Datenschutz des Unternehmens steuern, unterstützen und kontrollieren zu können, mit der Ausrichtung, die Unternehmensziele des Datenschutzes (Datenschutz-Ziele) zu erreichen.[62] Zudem wird unter einem DSMS ein Konzept verstanden, das auf eine kontinuierliche Leistungsverbesserung ausgerichtet ist und zur systematischen Steuerung des Datenschutzes notwendig ist.[63] Einem Unternehmen wird dadurch ein datenschutzkonformes Handeln und

[55] Vgl. Loomans/Matz/Wiedemann (2014) – S. 15f.; *Sowa*, in: Sowa (2020) – S. 17.
[56] Vgl. Loomans/Matz/Wiedemann (2014) – S. 16; Scheben (2019).
[57] Auch Informationssicherheits-Managementsystem (ISMS) genannt.
[58] Vgl. Gabel (2019).
[59] Vgl. Loomans/Matz/Wiedemann (2014) – S. 22.
[60] Vgl. Kranig/Sachs/Gierschmann (2019) – S. 201.
[61] Vgl. Gabel (2019); *Haag*, in: Forgó/Helfrisch/Schneider (2019) Teil II, Kapitel 2, Rn. 47; Meyer/Struck/Bitsch (2020).
[62] Vgl. Kranig/Sachs/Gierschmann (2019) – S. 204; Korge (2020) – S. 31; Wichtermann, ZD (2016) – S. 422; *Haag*, in: Forgó/Helfrisch/Schneider (2019) Teil II, Kapitel 2, Rn. 47; Wybitul (2016) – S. 140.
[63] Vgl. Loomans/Matz/Wiedemann (2014) – S. 21f.

effektives Betreiben des Datenschutzes ermöglicht. Grundsätzlich kann zwischen zwei Methoden beim Aufbau eines DSMS unterschieden werden. So kann ein DSMS entweder anhand eines Schutzstandards oder risikobasiert aufgebaut werden. Dabei bietet der risikobasierte Ansatz, eine individuell auf das Unternehmen zugeschnittene Organisation der Datenschutzaktivitäten.[64] Die Gemeinsamkeiten und Unterschiede der Vorgehensweisen sind in Tab. 1 dargestellt.

	Schutzstandards z. B. IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI)	**Risikobasiertes DSMS**
Übergeordnetes Ziel des Management-systems	- Erreichen eines unternehmensunabhängigen Sicherheitsniveaus	- Erreichen der unternehmensindividuellen Datenschutz-Ziele
Vorgehensweise	- Vorgegebene Sicherheitsziele werden durch die Umsetzung von Standard-Schutzmaßnahmen erreicht	- Risikoanalyse identifiziert die erforderlichen Maßnahmen - Risikoabwägung bestimmt die Umsetzung
Vorteile	- Auditierbar - Einheitlich - Vergleichbares Sicherheitsniveau	- Auditierbar - Unternehmensspezifisch - Effektiv

Tab. 1: Vergleich von Schutzstandards und risikobasiertem DSMS[65]

3.2 NOTWENDIGKEIT

In der DS-GVO werden ein DSMS und dessen Notwendigkeit nicht explizit erwähnt, weshalb keine Pflicht zur Umsetzung eines solchen Systems besteht.[66] Allerdings stellt die DS-GVO sehr hohe Anforderungen an die verantwortlichen Stellen, um der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO nachzukommen.[67] Demnach ist der Verantwortliche und nicht der Datenschutzbeauftragte (DSB) für die Einhaltung der Grundsätze aus Art. 5 Abs. 1 DS-GVO verantwortlich und muss deren Einhaltung nachweisen können.[68] Zudem verdeutlicht Art. 39 DS-GVO, dass nicht der DSB für die Einhaltung der datenschutzrechtlichen Normen verantwortlich ist. Die Verantwortung für den Datenschutz, die nicht delegierbar ist, obliegt vielmehr dem Verantwortlichen, was in den meisten Fällen einem Unternehmen beziehungsweise dessen Vertreter entspricht.[69] Um den datenschutzrechtlichen Pflichten nachzukommen, ist die Bestellung eines DSB mit sämtlichen relevanten Informationen und Ressourcen unzureichend. Ein DSMS ermöglicht dem Verantwortlichen einen Überblick über alle Maßnah-

[64] Vgl. Loomans/Matz/Wiedemann (2014) – S. 21.
[65] Eigene Darstellung in Anlehnung an: Loomans/Matz/Wiedemann (2014) – S. 23.
[66] Vgl. Kranig/Sachs/Gierschmann (2019) – S. 198; Korge (2019) – S. 27; Meyer/Struck/Bitsch (2020).
[67] Vgl. Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (2018) - S. 14; Korge (2019) – S. 27.
[68] Vgl. *Schrulle*, in: Sowa (2020) – S. 21; Kranig/Sachs/Gierschmann (2019) – S. 201.
[69] Vgl. Gardyan-Eisenlohr/Knöpfle, DuD (2017) – S. 69.

men, da dieser selbst in der Regel nicht am Tagesgeschäft und den alltäglichen Problemen beteiligt ist.

Außerdem stellt der Datenschutz einen Teil des Compliance-Programms eines jeden Unternehmens dar.[70] Generell sind unter einem Compliance-Programm die festgelegten Grundsätze und Maßnahmen eines Unternehmens zu verstehen, welche ein regelkonformes Verhalten von Mitarbeitern und dem Unternehmen selbst sicherstellen, wodurch Gesetzesverstöße verhindert werden können.[71] Die Unternehmensführung ist somit auch aus Compliance-Sicht verpflichtet, angemessene und wirksame Maßnahmen zu ergreifen, um Verstöße gegen datenschutzrechtliche Normen zu vermeiden. Dies kann beispielsweise durch unternehmensinterne Vorgaben, wie Arbeitsanweisungen, Leitfäden oder sonstige ergänzende Dokumente, sichergestellt werden, wobei deren Konformität und Einhaltung regelmäßig zu überwachen sind.[72] Die Pflicht zum datenschutzkonformen Handeln besteht deshalb nicht nur aufgrund der datenschutzrechtlichen Normen, sondern auch aus der organisatorischen Pflicht der Unternehmensleitung für eine Datenschutz-Compliance zu sorgen. Aus Unternehmenssicht ist außerdem die enthaftende Wirkung des Art. 82 Abs. 3 DS-GVO von Bedeutung.[73] Demnach scheidet eine Haftung aus, wenn der Verantwortliche nachweisen kann, dass er für den entstandenen Schaden nicht verantwortlich ist. Die Erbringung des Nachweises kann allerdings nur gelingen, wenn die erforderlichen Prozesse der Datenschutz-Compliance systematisch organisiert und dokumentiert sind. Ebenso ist festzustellen, dass das Vertrauen der betroffenen Personen, hauptsächlich der Mitarbeiter und Kunden, in den korrekten Umgang mit ihren personenbezogenen Daten durch den Verantwortlichen nur entstehen und ausgebaut werden kann, wenn der Verantwortliche nachweisen kann, dass die Verantwortung tatsächlich übernommen wurde.[74] Das DSMS dient somit als Maßnahme, um Vertrauen von den betroffenen Personen zu gewinnen.[75]

Der Verantwortliche hat, neben der bereits genannten Rechenschafts- und Nachweispflicht, noch weitere Anforderungen aus der DS-GVO zu erfüllen, wie beispielsweise für die Rechtmäßigkeit der Verarbeitung zu sorgen oder in bestimmten Fällen eine DSFA durchzuführen. Angesichts der Rechenschafts- und Nachweispflicht einerseits und der Anzahl an sonstigen Anforderungen andererseits ist ein Unternehmen verpflichtet, diese Vorgänge und Prozesse in ein geordnetes System in Form eines DSMS zu überführen.[76]

Auch die deutschen Aufsichtsbehörden haben in bereits erfolgten Prüfungen die Umsetzung von strukturierten Maßnahmen aufgegriffen.[77] So wurden „Vorgehensweisen, Prozesse und Methodiken“[78] bewertet, nach „Regelungen für internen Kontrollen zur Einhaltung datenschutzrechtlicher Vorschriften“[79] gefragt und geprüft, ob ein „Datenschutzmanagementsystem installiert“[80] ist. Die strukturierte Organisation des Datenschutzes ist allerdings nicht nur notwendig, sondern kann auch als Chance für das Unternehmen betrachtet werden.[81] Ein

[70] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 1.
[71] Vgl. *Schrulle*, in: Sowa (2020) – S. 33.
[72] Vgl. *Andelfinger/Kneuper*, in: Knoll/Strahringer (2017) – S. 35; Gardyan-Eisenlohr/Knöpfle, DuD (2017) – S. 69.
[73] Vgl. Jung, CCZ (2018) – S. 225.
[74] Vgl. Duda, PinG (2016) – S. 251f.; Scheben (2019).
[75] Vgl. Jung, CCZ (2018) – S. 225; Scheben (2019).
[76] Vgl. Lambertz (2019); Gardyan-Eisenlohr/Knöpfle DuD (2017) – S. 69.
[77] Vgl. *Schrulle*, in: Sowa (2020) – S. 22.
[78] Vgl. LfD Niedersachsen (2019).
[79] Vgl. BayLDA (2018).
[80] Vgl. BayLDA (2017).
[81] Vgl. *Schrulle*, in: Sowa (2020) – S. 22; Gardyan-Eisenlohr/Knöpfle DuD (2017) – S. 69.

DSMS kann beispielsweise die Eintrittswahrscheinlichkeit von Datenpannen und Datenschutzverstößen verringern oder den Schaden für die Betroffenen bei Datenpannen begrenzen, indem diese zeitnah erkannt und Gegenmaßnahmen eingeleitet werden.[82]

Die Ziele eines DSMS können zugleich als Aufgaben verstanden werden. Diese umfassen die bereits genannte Dokumentation der Rechenschafts- und Nachweispflicht, die Einhaltung der sonstigen Verpflichtungen aus der DS-GVO zu gewährleisten, Verstöße gegen datenschutzrechtliche Normen zu verhindern und Vertrauen in die Datenschutzkonformität des Unternehmens aufzubauen.[83] Bereits im Jahr 2017 verdeutlichte der damalige Präsident des Bayrischen Landesamtes für Datenschutzaufsicht (BayLDA) die Notwendigkeit eines DSMS: „Der Datenschutz erfordert ein effektives, Compliance-Management-System, das dadurch geprägt ist, dass es proaktiv, transparent, formell, vollumfänglich, prozessorientiert, risikobasiert und integriert ist.“[84]

3.3 ANFORDERUNGEN

Wie erwähnt, legt die DS-GVO den Aufbau eines strukturierten Datenschutzmanagements beziehungsweise eines DSMS nahe, ohne ein solches wörtlich zu nennen.[85] Deshalb existieren in der DS-GVO keine direkten regulatorischen Anforderungen an ein solches System. Ebenso ist kein allgemeingültiger Standard zur operativen Ausgestaltung der Datenschutzorganisation vorhanden, auf welchem eine spätere Zertifizierung erfolgen könnte und der von allen Beteiligten akzeptiert wird. Zwar wurden die Vorgaben für eine Zertifizierung gemäß Art. 42 DS-GVO und für die Zertifizierungsstellen nach Art. 43 DS-GVO durch den europäischen Datenschutzausschuss definiert[86], jedoch kann demnach nur ein Prozess, ein Produkt oder eine Dienstleistung und nicht das DSMS oder die Datenschutzorganisation zertifiziert werden. Somit lassen sich aus dem Bereich der Zertifizierungen bisher also keine Anforderungen an ein DSMS ableiten.

Allerdings können die Anforderungen an ein effektives DSMS aus den Grundsätzen der DS-GVO (Art. 5) abgeleitet werden, welche auf Art. 8 der Grundrechtecharta der Europäischen Union beruhen.[87] So sollte ein DSMS gewährleisten, dass die in Art. 5 DS-GVO genannten Grundsätze für die Verarbeitung personenbezogener Daten berücksichtigt und eingehalten werden. Hierzu gehört, dass die Datenverarbeitungen rechtmäßig sein müssen, nach Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise erfolgen (Grundsatz „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“ gemäß Art. 5 Abs. 1 lit. a) DS-GVO). Ebenso dürfen die personenbezogenen Daten nur für zuvor festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden (Grundsatz „Zweckbindung“ gemäß Art. 5 Abs. 1 lit. b) DS-GVO). Des Weiteren müssen die zu verarbeitenden, personenbezogenen Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Grundsatz „Datenminimierung“ gemäß Art. 5 Abs. 1 lit. c) DS-GVO). Sichergestellt wird, dass alle personenbezogenen Daten sachlich richtig und erforderlichenfalls auf aktuellem Stand sind und fehlerhafte Daten unverzüglich berichtigt oder gelöscht werden (Grundsatz „Richtigkeit“ gemäß Art. 5 Abs. 1 lit. d) DS-GVO). Außerdem sind die personenbezogenen Daten in einer Form zu speichern,

[82] Vgl. Sächsisches Staatsministerium des Inneren (2021).
[83] Vgl. *Borchers*, in: Schläger/Thode (2018) Teil C, Kapitel 9, Rn. 294.
[84] Vgl. *Kranig*, in: Kranig/Sachs/Gierschmann (2017) – S. 206.
[85] Vgl. *Schrulle*, in: Sowa (2020) – S. 23.
[86] Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018a).
[87] Vgl. Jung, CCZ (2018) – S. 225; ISiCO-Datenschutz.de (2019).

welche die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie die Zwecke, für die sie verarbeitet werden, erfordern (Grundsatz „Speicherbegrenzung“ gemäß Art. 5 Abs. 1 lit. e) DS-GVO). Zusätzlich ist für eine angemessene Sicherheit der personenbezogenen Daten zu sorgen, was den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Schädigung oder Zerstörung durch geeignete technische und organisatorische Maßnahmen einschließt (Grundsatz „Integrität und Vertraulichkeit“ gemäß Art. 5 Abs. 1 lit. f) DS-GVO). Die Rechenschaftspflicht ist der letzte Grundsatz, welcher in Art. 5 Abs. 2 DS-GVO aufgeführt ist und vorschreibt, dass der Verantwortliche für die Einhaltung der zuvor genannten Grundsätze aus Art. 5 Abs. 1 DS-GVO verantwortlich ist und darüber hinaus deren Einhaltung nachweisen können muss, weshalb diese auch als Nachweispflicht bezeichnet wird.[88]

Weitere Vorschriften ergänzen die allgemeinen Grundsätze im Hinblick auf die Zulässigkeit der Datenverarbeitung. So muss beispielsweise der Verantwortliche gemäß Art. 35 DS-GVO eine DSFA durchführen, wenn die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen birgt. Dabei muss der Verantwortliche die geplanten Verarbeitungsvorgänge und deren Zwecke systematisch beschreiben, deren Notwendigkeit und Verhältnismäßigkeit bewerten, die Risiken für die Rechte und Freiheiten der betroffenen Personen abwägen und geeignete Maßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren zur Bewältigung dieser Risiken umsetzen.[89] Insbesondere im Hinblick auf die Sicherheit der Verarbeitung fordert die DS-GVO in Art. 32 Abs. 1 lit. d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgesehenen Schutzmaßnahmen.[90] Der Verantwortliche ist außerdem dazu verpflichtet, dass jede Verarbeitung rechtmäßig erfolgt und somit auf einer der gesetzlichen Tatbestände des Art. 6 DS-GVO beruht. Um auch alle Datenverarbeitungen zu erfassen, ist gemäß Art. 30 DS-GVO ein Verzeichnis aller Verarbeitungstätigkeiten in schriftlicher Form[91] zu führen.[92] Dieses Verzeichnis wird auch Verarbeitungs- oder Verfahrensverzeichnis genannt und stellt den Mittelpunkt der meisten datenschutzrechtlichen Prüfungen dar.[93] Darüber hinaus sollte dieses regelmäßig überprüft und wenn nötig aktualisiert werden.[94] Der Ablauf der Prüfung sollte mindestens jährlich durchgeführt werden.[95] Auch bei einer Datenübermittlung in Drittländer muss der Verantwortliche gemäß Art. 44 DS-GVO entsprechende Vorkehrungen, wie geeignete Garantien (Art. 46 DS-GVO) oder verbindlichen internen Datenschutzvorschriften (Art. 47 DS-GVO), für eine rechtmäßige Verarbeitung treffen. Ebenso fordert die DS-GVO von dem Verantwortlichen, dass dieser geeignete Maßnahmen zur Information und Kommunikation ergreift, um im Falle eines Datenschutzvorfalls entsprechend schnell reagieren zu können.[96] Um die Wirksamkeit des Datenschutzes in der praktischen Umsetzung zu gewährleisten, hat der Verordnungsgeber eine Überprüfung des Datenschutzes vorgesehen, welche der Verantwortliche regelmäßig durchzuführen hat. Die Inhalte werden beispielsweise auch in

[88] Vgl. Lambertz (2019).
[89] Vgl. Art. 35 Abs. 7 DS-GVO.
[90] Vgl. Rieß, DuD (2019) – S. 498; *Schrulle*, in: Sowa (2020) – S. 22; Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2020) – S. 22f.
[91] Schriftlich bedeutet hier allerdings nicht im Kontext von § 126 BGB. Nach Art. 30 Abs. 3 ist die Führung des Verarbeitungsverzeichnisses auch in einer elektronischen Form möglich.
[92] Vgl. Korge (2020) – S. 27.
[93] Vgl. Korge (2020) – S. 56.
[94] Vgl. *Haag*, in: Forgó/Helfrisch/Schneider (2019) – Teil II, Kapitel 2, Rn. 48; IDW PH 9.860.1 – Anlage 1, Nr. 46.
[95] Vgl. IDW PH 9.860.1 – Anlage 1, Nr. 46.
[96] Vgl. Art. 12ff. DS-GVO und Art. 33f. DS-GVO.

Art. 24 Abs. 1 Satz 2 oder Art 32 Abs. 1 lit. d) DS-GVO gefordert.[97] Sofern der Verantwortliche Datenverarbeitungen auslagert beziehungsweise die Verarbeitungen nicht eigenständig durchführt, muss bei der Auswahl des Auftragsverarbeiters geprüft werden, ob dieser für die Aufgabe geeignet ist, die Anforderungen des Art. 28 DS-GVO erfüllt und über das erforderliche Fachwissen sowie die notwendigen Ressourcen verfügt.[98] Zudem muss der Vertrag zur Auftragsverarbeitung schriftlich oder elektronisch dokumentiert werden, auch wenn keine explizite Schriftform des § 126 BGB erwähnt wird.[99] Der Verantwortliche hat außerdem auch gemäß Art. 32 DS-GVO für die Sicherheit der Datenverarbeitungen zu sorgen, indem er geeignete technische und organisatorische Maßnahmen (TOM) ergreift und dadurch ein angemessenes Schutzniveau sicherstellt.[100] Ähnliches wird auch in Art. 25 DS-GVO gefordert, wobei dort der Fokus auf die Technikgestaltung und datenschutz-freundliche Voreinstellungen gelegt wird.

Abb. 2 stellt die grundsätzlichen Anforderungen und Pflichten an das Management des Datenschutzes aus der DS-GVO in zusammengefasster Form dar.

Werden die hier genannten Grundsätze, Verfahren und sonstigen Maßnahmen der DS-GVO um die Elemente eines CMS ergänzt, so kann daraus ein vollumfängliches und effektives DSMS entstehen und betrieben werden.[101]

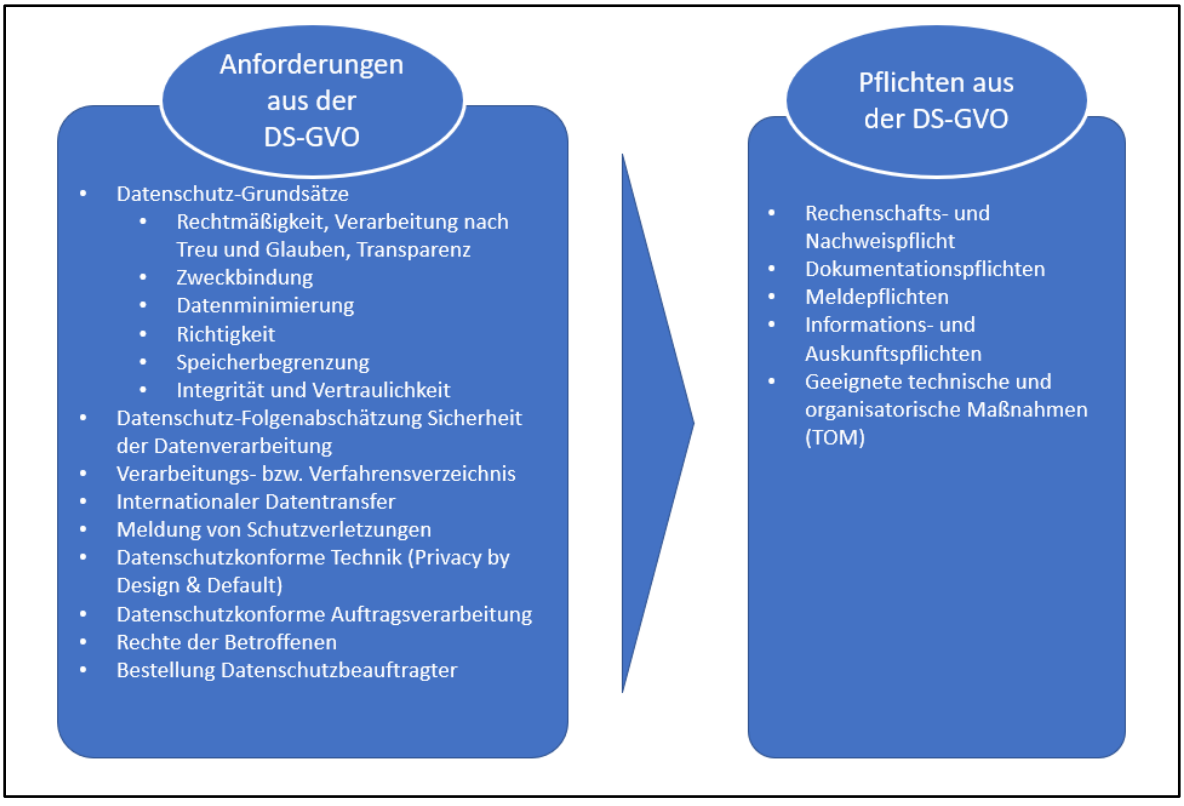

Abb. 2: Anforderungen und Pflichten aus der DS-GVO[102]

[97] Vgl. Schefzig, in: Moos/Schefzig/Arning (2018) – Kapitel 10, Rn. 1; für Compliance-Systeme allg. ähnlich Pampel/Korlak, in: Hauschka/Moosmayer/Lösler (2016) – § 15, Rn. 3.
[98] Vgl. Korge (2020) – S. 55; ErwG 81, S. 1 DS-GVO.
[99] Vgl. Korge (2020) – S. 27.
[100] Vgl. Korge (2020) – S. 58; Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2020) – S. 22f.
[101] Vgl. *Schrulle*, in: Sowa (2020) – S. 24 + 33.

3.4 PRINZIPIEN

Einige Unternehmen haben in Vorbereitung auf die DS-GVO und mit deren Anwendbarkeit ein DSMS eingeführt. Dabei wurde, sofern bislang keine ähnlichen Managementsysteme verwendet wurden, aufgrund mangelnder einheitlicher Standards auf bekannte Managementsysteme aus der Corporate Compliance[103] zurückgegriffen und für den Datenschutz übernommen.[104] Hierzu gehörte oftmals der IDW PS 980 für CMS, welcher weltweit anerkannt wird.[105] Der Datenschutz und die Datensicherheit werden dabei ausdrücklich als Teilbereiche des Standards genannt.[106] Der IDW PS 980 besteht aus sieben Grundelementen: Compliance-Kultur, -Ziele, -Organisation, -Risiken, -Programm, -Kommunikation und -Überwachung sowie -Verbesserung.[107] Einige Jahre später veröffentlichte das IDW als Ergänzung des IDW PS 860[108] den Prüfungshinweis IDW PH 9.860.1[109], wodurch eine umfassende Prüfung eines DSMS ermöglicht wurde.[110] Dabei stellt der Prüfungshinweis die Kriterien an das DSMS transparent dar.[111] Der Prüfungshinweis kann von Wirtschaftsprüfern als Referenz für den Aufbau und die Organisation des Datenschutzes eines Unternehmens verwendet werden.[112]

Das Aufsetzen des DSMS anhand eines bestehenden CMS ermöglicht zudem die Nutzung von Synergieeffekten.[113] Die Prüfungsstandards des IDW haben nicht die Wirkung eines Gesetzes, werden aber regelmäßig als Maßstab für Prüfungen herangezogen.[114] Sie sind teilweise mit DIN-Normen vergleichbar und haben damit eine starke faktische Wirkung.[115] Auch von der International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC) sind Standards aus der ISO/IEC 27000-Normenreihe etabliert worden.[116] Wesentliche Bedeutung hat dabei der ISO/IEC 27701[117], welcher die Erweiterung der ISO/IEC 27001[118] und ISO/IEC 27002[119] für das Datenschutzmanagement darstellt.[120] Ebenso wurde im Hinblick auf die DS-GVO im November 2016 von den deutschen Aufsichtsbehörden das Standard-Datenschutzmodell (SDM) erstellt.[121] Eine grundlegende

---

[102] Eigene Darstellung in Anlehnung an: Kranig/Sachs/Gierschmann (2019) – S. 200.
[103] Vgl. *Schild*, in: Fórgó/Helfrich/Schneider (2019) Kapitel 5, Rn. 7-13 zur Definition von Compliance und zur möglichen Abgrenzung des Datenschutzmanagements zur Corporate Compliance.
[104] Vgl. Wybitul (2016) – S. 141.
[105] Vgl. Rieß, DuD (2019) – S. 501; Wybitul (2016) – S. 141.
[106] Vgl. IDW PS 980 – Tz. A3.
[107] Vgl. Wybitul (2016) – S. 141.
[108] Darunter ist der vom IDW verabschiedete Prüfstandard „IT-Prüfung außerhalb der Abschlussprüfung“ zu verstehen.
[109] Darunter ist der vom IDW verabschiedete Prüfungshinweis „Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz“ mit Stand vom 19.06.2018 zu verstehen.
[110] Vgl. Schrulle, IT-Governance (2019) – S. 25.
[111] Vgl. *Schrulle*, in: Sowa (2020) – S. 24.
[112] Vgl. *Schrulle*, in: Sowa (2020) – S. 25, Schrulle, IT-Governance (2019) – S. 25.
[113] Vgl. CASIS Wirtschaftsprüfung (2020); Kranig/Sachs/Gierschmann (2019) – S. 201.
[114] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 3.
[115] Vgl. BGH-Urteil vom 14.05.1998 – VII ZR 184/97, NJW 1998, 2814.
[116] Vgl. Meyer/Struck/Bitsch (2020).
[117] Sicherheitstechniken - Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz - Anforderungen und Leitlinien.
[118] Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheitsmanagementsysteme – Anforderungen.
[119] Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen.
[120] Vgl. Meyer/Struck/Bitsch (2020).
[121] Vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: „Das Standard-Datenschutzmodell V. 1.0 – Erprobungsfassung“.

Überarbeitung erhielt das Modell im November 2019 durch die Version 2.0 und soll die rechtlichen Anforderungen der DS-GVO mit Hilfe der Gewährleistungsziele (Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit) vollumfänglich erfassen.[122]

Da zur Sicherstellung eines funktionierenden DSMS unabhängig von dem für das Unternehmen einschlägigen DSMS-Standard regelmäßige Überprüfungen durchzuführen sind, beruhen sämtliche Systeme auf dem Prinzip eines kontinuierlichen Verbesserungsprozesses.[123] Der PDCA-Zyklus (Plan-Do-Check-Act) nach DEMING ist dabei eine der bekanntesten Formen eines fortlaufenden Verbesserungsprozesses, welcher in Art. 24 DS-GVO rechtlich berücksichtigt wird.[124] So muss der Verantwortliche stets geeignete Maßnahmen für die aktuelle Bedrohungslage ergreifen, die dem aktuellen Stand der Technik zu entsprechen haben.[125] Dieser sich wiederholende Prozess setzt sich aus vier Phasen zusammen: dem Bereitstellen von Werkzeugen (Plan), deren Einsatz (Do), der kontinuierlichen Überprüfung der Wirksamkeit (Check) sowie der stetigen Weiterentwicklung beim Feststellen von Verbesserungsmöglichkeiten (Act), wodurch ein kontinuierlicher Verbesserungsprozess realisiert wird (siehe Abb. 3).[126] Deshalb ist auch das Datenschutzmanagement gemäß WYBITUL kein einmaliges Projekt, sondern vielmehr ein dauerhafter Prozess, welcher durch die stetige Umsetzung der einzelnen Phasen eine standardisierte, geordnete und nachhaltige Durchführung entsprechender Prozesse gewährleistet.[127]

In der Überprüfungsphase (Check) können einzelne Unternehmensteile stichprobenartig auf die Einhaltung der festgelegten Prozesse und Vorgaben überprüft werden.[128] Die Überprüfung dieser Unternehmensteile und Abteilungen erfolgt dabei meist durch die interne Revision.[129] Hierbei werden für gewöhnlich Dokumente wie Arbeitsanweisungen und Richtlinien, welche das System unterstützen, auf den Grad ihrer Umsetzung überprüft.[130] Insbesondere für international agierende Unternehmen sind interne Richtlinien und Vorgaben besonders wichtig, da hierdurch unternehmensweite einheitliche Standards gesetzt werden können, welche alle regulatorischen Vorgaben erfüllen.[131]

Die Tatsache, dass sämtliche Standards auf einem PDCA-Zyklus beruhen, verdeutlicht dessen Relevanz. Die Planung und Durchführung sind unzureichend. Vielmehr sollte stetig eine Überprüfung stattfinden, ob die vorausgegangen Schritte in korrekter Form gemacht wurden und ob darauf aufbauend Prozesse zur Verbesserung anzustoßen sind.[132] Durch einen kontinuierlichen Prozess können gesteckte Ziele über einen längeren Zeitraum durch eine schrittweise Verbesserung erreicht werden.[133] Ebenso kann hierdurch auf mögliche Änderungen der gesetzlichen Rahmenbedingungen zeitnah reagiert werden.

---

[122] Vgl. Meyer/Struck/Bitsch (2020); Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: „Das Standard-Datenschutzmodell Version 2.0b“ Stand 17. April 2020.
[123] Vgl. Sowa (2017) – S. 18; Loomans/Matz/Wiedemann (2014) – S. 62; Meyer/Struck/Bitsch (2020).
[124] Vgl. *Jaspers/Schwartmann/Hermann*, in: Schwartmann/Jaspers/Thüsing/Kugelmann (2018) Art. 5, Rn. 85; Lambertz (2017).
[125] Vgl. Lambertz (2017).
[126] Vgl. *Andelfinger/Kneuper*, in: Knoll/Strahringer, (2017) – S. 33; Loomans/Matz/Wiedemann (2014) – S. 62.
[127] Vgl. Wybitul (2016) – S. 140f.
[128] Vgl. *Inderst/Steiner*, in: Inderst/Bannenberg/Poppe (2017) – Kapitel 3, Rn. 90.
[129] Vgl. *Inderst/Steiner*, in: Inderst/Bannenberg/Poppe (2017) – Kapitel 3, Rn. 91.
[130] Vgl. *Veil*, in: Gierschmann/Schlender/Stentzel/Veil (2018) – Art. 24, Rn. 72.
[131] Vgl. *Faust,* in: Schimansky/Bunte/Lwowski (2017) – § 109, Rn. 128.
[132] Vgl. Jung, CCZ (2018) – S. 225.
[133] Vgl. Loomans/Matz/Wiedemann (2014) – S. 68.

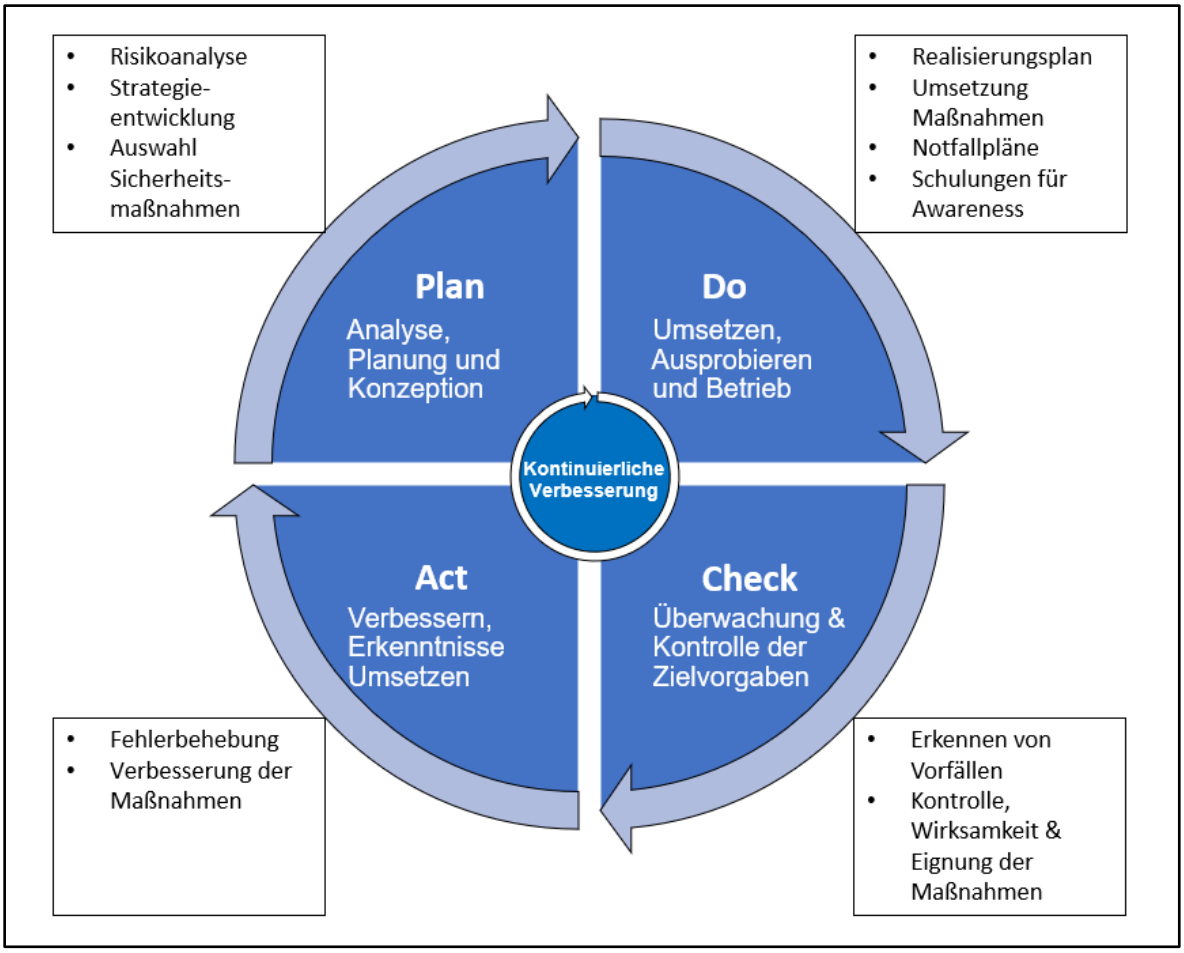

Abb. 3: PDCA-Zyklus[134]

3.5 Elemente

3.5.1 Überblick

Der IDW PS 980 enthält nicht nur Vorgaben zur Prüfung eines CMS, sondern auch bewährte, vorbildliche beziehungsweise optimale Praktiken, Methoden oder Vorgehensweisen (sog. Best Practices)[135], welche als Anforderungskatalog für den Aufbau eines DSMS herangezogen werden können.[136] Hierdurch bietet der IDW PS 980 Unterstützung für die Führungs- und Aufsichtsorgane, um ihren Pflichten aus der Corporate Governance nachzukommen.[137] Wie die meisten Compliance-Maßnahmen trägt ein solches System zur Vermeidung der persönlichen Haftung der Organmitglieder bei.[138]

Wie erwähnt, enthält der Prüfungsstandard 980 des IDW sieben inhaltliche Grundelemente, die miteinander in Wechselwirkung stehen und ein wirksames CMS gewährleisten sollen.[139] Demnach bilden die Compliance-Kultur und das Festlegen von Compliance-Zielen die

[134] Eigene Darstellung in Anlehnung an: Loomans/Matz/Wiedemann (2014) – S. 63.
[135] Vgl. Kranig/Sachs/Gierschmann (2019) – S. 214.
[136] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 3.
[137] Vgl. Kranig/Sachs/Gierschmann (2019) – S. 209.
[138] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 2.
[139] Vgl. IDW PS 980 – Tz. 23.

Grundlage für ein effektives CMS.[140] Ebenso muss ein Prozess zur Identifizierung, Überwachung und Steuerung der Compliance-Risiken, welche die gesetzte Zielerreichung beeinflussen können, integriert werden.[141] Grundlage dieses internen Kontrollsystems (IKS) ist das Compliance-Programm. Zudem sind die Aufgaben und Rollen für die Compliance klar zu verteilen, was für gewöhnlich im Rahmen der Compliance-Organisation festgelegt wird und die Aufbau- und Ablauforganisation darstellt.[142] Um die Beteiligten zu informieren, ist ein entsprechender Kommunikationsprozess, die Compliance-Kommunikation, erforderlich. Abschließend soll durch die Compliance-Überwachung & -Verbesserung die Angemessenheit und Wirksamkeit überprüft und mögliche Anpassungen umgesetzt werden. Damit greift ein CMS, welches nach dem IDW PS 980 aufgebaut wurde, sämtliche Elemente eines PDCA-Zyklus auf.

Die inhaltlichen Bausteine des CMS lassen sich auf ein DSMS übertragen. So wird etwa die Compliance-Organisation zur Datenschutz-Organisation und die Compliance-Kultur zur Datenschutz-Kultur (siehe Abb.4).

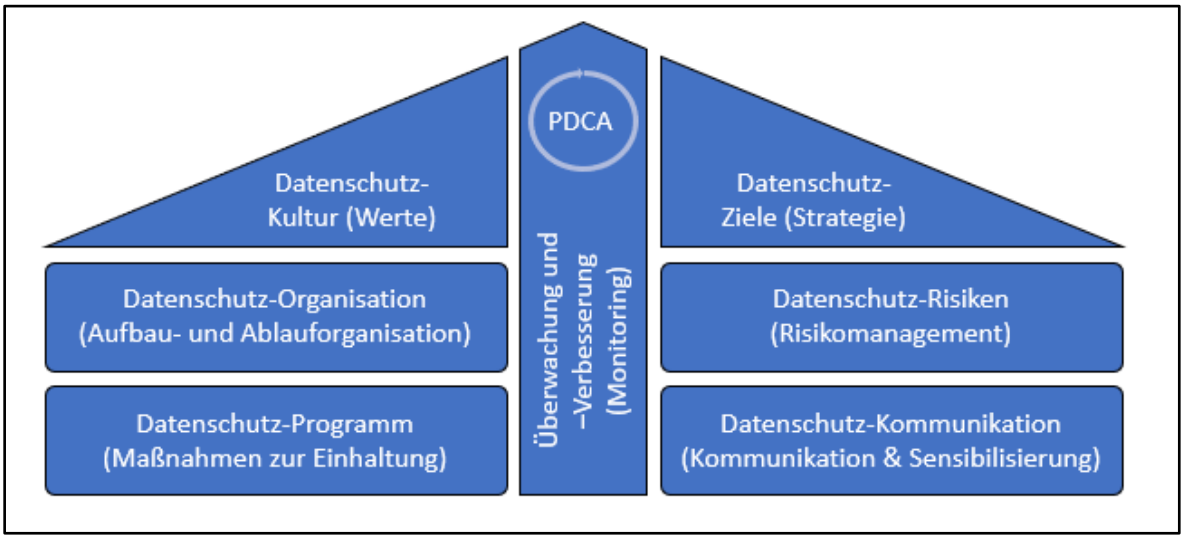

Abb.4: Bausteine eines DSMS[143]

Diese Grundelemente sind nicht als starre Anforderungen zu betrachten, da sie nicht konkret genug ausgeführt sind. Sie sind vielmehr als grundsätzliche Ordnungsprinzipien zu verstehen, welche in einer wechselseitigen Beziehung stehen und sich thematisch überschneiden können.[144] Sie bieten einen Gestaltungsspielraum, um auf die Unternehmenssituation und dessen Risiken einzugehen, anhand derer eine risikoorientierte Datenschutzstrategie entwickelt werden kann.

Der IDW PH 9.860.1 erstreckt sich über insgesamt zwölf Anforderungsgebiete, welche größtenteils auf die sieben Elemente des IDW PS 980 verteilbar sind. Weiterhin sind verschiedene Maßnahmen enthalten, die das vollständige Spektrum der DS-GVO abdecken (siehe Abb.5). Für ein effektives Datenschutzmanagement ist deshalb das Datenschutz-Umfeld

[140] Vgl. *Schrulle*, in: Sowa (2020) – S. 33f.; IDW PS 980 – Tz. 10.
[141] Vgl. *Schrulle*, in: Sowa (2020) – S. 34; IDW PS 980 – Tz. 10.
[142] Vgl. IDW PS 980 – Tz. 10.
[143] Eigene Darstellung in Anlehnung an: *Schrulle*, in: Sowa (2020) – S. 34.
[144] Vgl. Wermelt/Fechte, BB (2013) – S. 811.

sowie die sachgerechte Aufbau- und Ablauforganisation[145] des Datenschutzes von zentraler Bedeutung, da diese die Basis für die Umsetzung aller weiteren Anforderungen bilden.[146]

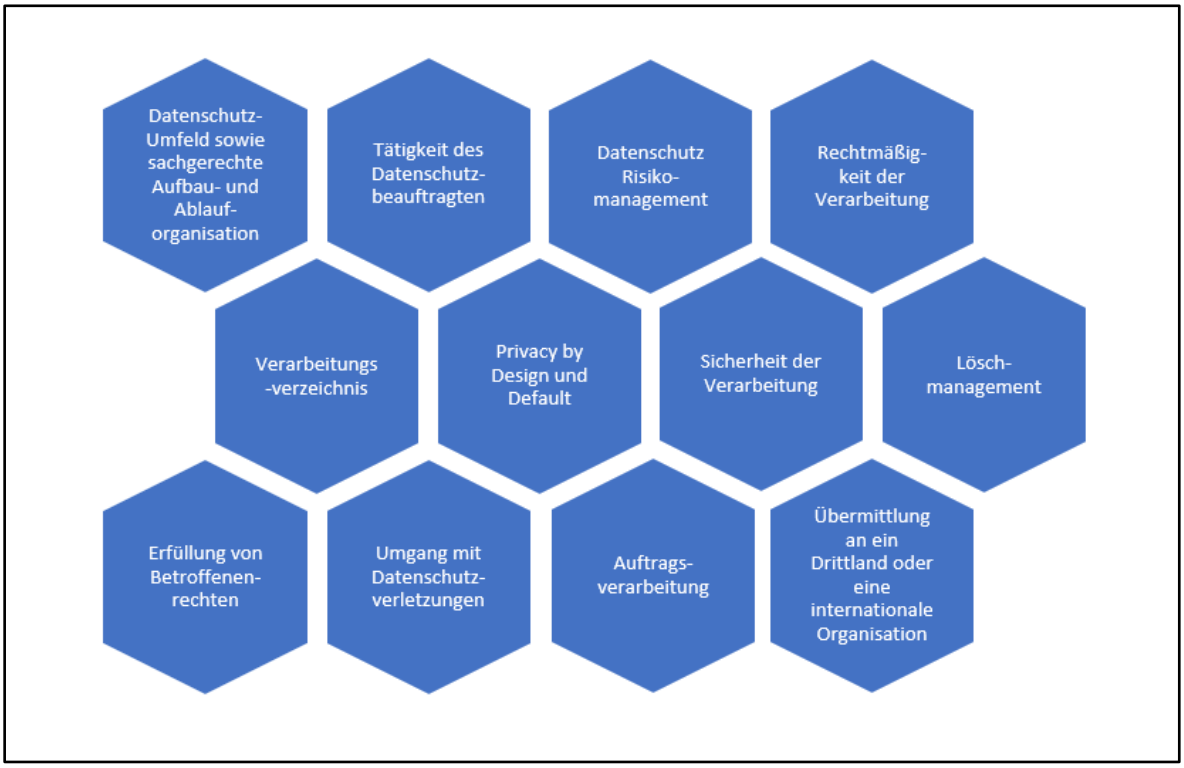

Abb.5: Anforderungsbereiche gemäß Anlage 1 des IDW PH 9.860.1[147]

3.5.2 Kultur

Die Grundlage für ein angemessenes und wirksames CMS und damit auch für ein DSMS ist dem IDW PS 980 zufolge die Compliance- beziehungsweise Datenschutz-Kultur.[148] Die Wirksamkeit eines DSMS wird grundlegend davon beeinflusst, welche Bedeutung die Mitarbeiter des Unternehmens der Beachtung des Datenschutzes beimessen und damit Bereitschaft zeigen sich an die datenschutzrechtlichen Regeln zu halten.[149] Die Mitarbeiter werden wiederum maßgeblich durch die Grundeinstellungen und Verhaltensweisen des Top-Managements zum Datenschutz („Tone from the Top“) geprägt.[150] Für SCHULZ hängt der Erfolg des DSMS maßgeblich von der Einstellung des Vorgesetzten ab: „Der Chef muss es wollen. Er muss es nicht mögen, aber muss es wollen.“[151] Denn nur dadurch kann glaubhaft vermittelt werden, dass die Bemühungen zum datenschutzkonformen Handeln dem Top-Management ein wirkliches Anliegen sind und nicht nur dem Schutz der Organmitglieder vor einer persönlichen Haftung dienen.[152] Das Vorleben dieser Werte durch die Geschäftsführung und Vorgesetzten hat somit einen direkten Einfluss darauf, welche Bedeutung die Mitarbeiter der Einhaltung des Datenschutzes zukommen lassen.[153] Das ist vor allem deshalb

[145] Vgl. IDW PH 9.860.1 – Anlage 1, Nr. 1-11.
[146] Vgl. *Schrulle*, in: Sowa (2020) – S. 26.
[147] Eigene Darstellung in Anlehnung an: *Schrulle*, in: Sowa (2020) – S. 26.
[148] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 3; *Schrulle*, in: Sowa (2020) – S. 26; Korge (2020) – S. 76, IDW PS 980 – Tz. 23 „Compliance-Kultur“.
[149] Vgl. Scheben (2019); IDW PS 980 – Tz. 23 „Compliance-Kultur”.
[150] Vgl. Scheben (2019); *Schrulle*, in: Sowa (2020) – S. 26; IDW PS 980 – Tz. 23 „Compliance-Kultur“.
[151] Vgl. Braunschweig (2020).
[152] Vgl. Scheben (2019).
[153] Vgl. IDW PS 980 – Tz. 23 „Compliance-Kultur“.

besonders wichtig, da der Datenschutz regelmäßig immer noch eine eher kritisch wahrgenommene Tätigkeit in Unternehmen darstellt.[154] Um den Datenschutz im Bewusstsein aller Unternehmenszugehörigen zu verankern, müssen interne Richtlinien erstellt und fortlaufend gepflegt werden. So können die Bedeutung und das Verständnis des Datenschutzes innerhalb der Belegschaft gestärkt und die Bereitschaft zum regelkonformen Verhalten nachhaltig positiv beeinflusst werden.

Die Grundlage der Datenschutz-Kultur eines Unternehmens ist dabei eine Datenschutz-Policy, welche anhand der aktuellen Unternehmenswerte aufgestellt ist und die Datenschutz-Grundsätze sowie -Ziele des Unternehmens zusammenfasst.[155] Die Datenschutz-Policy kann zudem auch als eine Art Selbstverpflichtung des Unternehmens zum datenschutzkonformen Handeln angesehen werden.[156] Sie ist hauptsächlich nach innen gerichtet und entfaltet somit im Unternehmen selbst ihre Wirkung, da die darin festgelegten Grundsätze und Ziele zum Unternehmensleitbild gehören und von allen Mitarbeitern eingehalten und verfolgt werden müssen.[157] Sollte der Begriff „Policy“ auf Widerstände stoßen, da damit z. B. primär Einschränkungen verbunden werden, kann selbstverständlich ein ähnlicher Begriff wie „Leitbild“ oder „Leitlinie“ verwendet werden. Außerdem sollte die Datenschutz-Policy nicht zu umfangreich gestaltet werden und keine technischen Ausführungen beinhalten, da eine Ergänzung der Unternehmensleitlinie um die Datenschutz-Ziele sowie die Vorstellung der Unternehmensleitung zum Datenschutz ausreichend sind. Für eine bessere Akzeptanz der Policy sollten bestehende Selbstverpflichtungserklärungen der Unternehmensleitung als Vorlagen beziehungsweise Orientierung dienen, damit die Policy problemlos zur Kommunikationskultur des Unternehmens passt. Die hierdurch geschaffenen Werte und Ziele sollten im Idealfall in der Unternehmenskultur gelebt werden und Vorgaben des Top-Managements zur Planung, Durchführung, Kontrolle und möglichen Anpassungen enthalten.[158]

Darüber hinaus kann auch die Stelle, an welcher der Datenschutz innerhalb der Unternehmensorganisation angesiedelt ist, ein deutliches Signal bezüglich der Wichtigkeit des Datenschutzes an die Belegschaft senden, wodurch weiterer Einfluss auf die Datenschutz-Kultur ausgeübt wird.[159] Ebenso können die aufgestellten und kommunizierten Verhaltensgrundsätze auf die Datenschutz-Kultur eines Unternehmens einwirken.

3.5.3 Ziele

Neben der Datenschutz-Kultur stellen die unternehmensindividuellen Datenschutz-Ziele ein weiteres wichtiges Element des DSMS dar.[160] Auf Grundlage der relevanten Normen sollte der Verantwortliche festgelegt haben, welche Ergebnisse durch das DSMS zu erzielen sind.[161] Anhand dieser Ziele kann eine Datenschutz-Strategie erstellt werden. Die datenschutzbezogenen Risiken können bewertet werden.[162] Zur Bewertung des Erfolgs der getroffenen Maßnahmen sind messbare und übergeordnete Datenschutzziele notwendig.[163] Somit kann durch eine passende Zielvergabe die Wirksamkeit des DSMS beurteilt werden,

[154] Vgl. Hansch, ZD (2019) – S. 245.
[155] Vgl. Lambertz (2017).
[156] Vgl. Loomans/Matz/Wiedemann (2014) – S. 79.
[157] Vgl. Loomans/Matz/Wiedemann (2014) – S. 80.
[158] Vgl. Braunschweig (2020).
[159] Vgl. IDW PS 980 – Tz. A14.
[160] Vgl. Korge (2020) – S. 82.
[161] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 3; Loomans/Matz/Wiedemann (2014) – S. 67.
[162] Vgl. *Schrulle*, in: Sowa (2020) – S. 26; IDW PS 980 – Tz. 23 „Compliance-Ziele“.
[163] Vgl. Loomans/Matz/Wiedemann (2014) – S. 67.

da das DSMS insbesondere an der Erreichung dieser gesetzten Ziele gemessen wird.[164] Dabei können die Datenschutzziele unspezifisch und abstrakt formuliert sowie Teil des Verhaltenskodex (CoC) sein.[165] Eine Verknüpfung der Datenschutz-Ziele mit den Unternehmenszielen und die Verankerung dieser mit der Datenschutz-Strategie in der Datenschutz-Policy gilt als empfehlenswert.[166] Zwar dient das DSMS vorrangig der operativen Umsetzung des Datenschutzes, jedoch sollte ein Unternehmen auch auf der strategischen Ebene Ziele für den Datenschutz festlegen.[167] Ein DSMS kann nur einen Mehrwert für den Datenschutz des Unternehmens und für das Unternehmen schaffen, wenn definiert ist, in welche Richtung sich der Datenschutz des Unternehmens entwickeln soll. Durch das Festlegen von langfristigen Zielen können zudem weitere Maßnahmen entwickelt werden, welche für die Zielerreichung förderlich sind.

Bei der Definition der Datenschutz-Ziele sind die allgemeingültigen Grundsätze für die Vergabe von Zielen zu beachten.[168] So sollten die Ziele konsistent, verständlich und schriftlich festgelegt werden, objektiv und messbar sein. Zudem sollten sie für einen bestimmten Zeitraum gelten, ambitioniert und somit auch motivierend sein, sich nicht untereinander oder den Grundwerten des Unternehmens widersprechen und bestenfalls zum Erreichen eines übergeordneten Ziels beziehungsweise Hauptziels beitragen.[169] Ebenso sollte darauf geachtet werden, dass die unterschiedlichen Ziele in Relation mit den zur Verfügung stehenden Ressourcen verhältnismäßig sind.[170]

Für das Definieren der Datenschutz-Ziele können verschiedene Vorgehensweisen gewählt werden. So kann beispielsweise das Ziel verfolgt werden, eine bestmögliche Datenschutz-Compliance zu erreichen, weshalb das DSMS vorrangig dafür genutzt wird, die gesetzlichen Vorschriften einzuhalten und umzusetzen.[171] Ebenso können Ziele gesetzt werden, die über die gesetzlichen Anforderungen hinaus gehen, wenn der Datenschutz als Wettbewerbsfaktor betrachtet wird. Die Entscheidung, welchen der beiden Ansätze ein Unternehmen verfolgen will, sollte davon abhängig gemacht werden, in welcher Branche das Unternehmen tätig ist. Manche Branchen haben ohnehin umfangreiche gesetzliche Anforderungen im Datenschutz umzusetzen, während in anderen Branchen weniger intensiv mit dem Datenschutz geworben werden kann wie beispielsweise Lieferanten von Rohmaterial. Branchen wie beispielsweise der Dienstleistungssektor führen eine vertrauensvolle Beziehung mit den Kunden und heben sich durch einen besonders ausgeprägten Datenschutz von der Konkurrenz ab, wodurch der Datenschutz als Wettbewerbsvorteil genutzt werden kann.[172] Die exakte Bestimmung der Datenschutz-Ziele ist deshalb von besonderer Bedeutung.

Die deutschen Aufsichtsbehörden haben in ihrem Standard-Datenschutzmodell sieben Gewährleistungsziele formuliert, welche für Unternehmen als Orientierung bei der Bestimmung

[164] Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2020) – S. 56.
[165] Vgl. Korge (2020) – S. 82, IDW PS 980 – Tz. 23 „Compliance-Organisation“; Tz. A18.
[166] Vgl. Loomans/Matz/Wiedemann (2014) – S. 79; *Schrulle*, in: Sowa (2020) – S. 26; IDW PS 980 – Tz. A15.
[167] Vgl. Loomans/Matz/Wiedemann (2014) – S. 68.
[168] Vgl. Tracy (2018) – S. 61.
[169] Vgl. Tracy (2018) – S. 61 - 63.
[170] Vgl. IDW PS 980 – Tz. A15.
[171] Vgl. Loomans/Matz/Wiedemann (2014) – S. 68; Korge (2020) – S. 82.
[172] Vgl. Scheben (2019).

ihrer Ziele dienen können: Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Intervenierbarkeit, Transparenz und Nichtverkettung.[173]

Die Datenschutz-Ziele müssen nicht veröffentlicht werden, allerdings empfiehlt sich eine transparente Darstellung und Kommunikation der Ziele, da das Vertrauen der Kunden, Lieferanten und Beschäftigten in das Unternehmen gestärkt werden kann.[174]

3.5.4 Organisation

Neben den (übergeordneten) Datenschutz-Zielen sollten im Rahmen der Datenschutz-Organisation die entsprechenden Rollen, Verantwortlichkeiten und Aufgaben wie beispielsweise des DSB, der DSK beziehungsweise DSM und der zentralen Ansprechpartner in Sachen Datenschutz festgelegt sein.[175] Das schließt die Arbeit der Rollen untereinander ebenso wie das Zusammenspiel mit weiteren unternehmensinternen Rollen, wie dem Beauftragten für die Informationssicherheit, ein.[176] Die geografische Verteilung der Standorte kann dabei eine entscheidende Rolle spielen und sollte daher mit berücksichtigt werden.[177] Darüber hinaus sollten die Zuständigkeiten und Befugnisse in den jeweiligen Stellenbeschreibungen schriftlich festgehalten werden und im Hinblick auf mögliche Konflikte regelmäßig überprüft werden.[178] Nur mit einer ausreichenden Dokumentation können im Hinblick auf die Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO die Verantwortlichkeiten für einzelne Aufgaben nachgewiesen werden. Ebenso empfiehlt sich in diesem Rahmen eine festgelegte Verteilung der Zuständigkeit für die Umsetzung und Erreichung der Ziele auf die jeweiligen Rollen. Diese Zuständigkeit sollte mit den Datenschutz-Zielen in der Datenschutz-Policy dokumentiert werden.[179] Zu einer funktionierenden Datenschutz-Organisation gehört ebenfalls die Aufbau- und Ablauforganisation des Datenschutzmanagements als integraler Bestandteil der Unternehmensorganisation.[180] Außerdem muss die Unternehmensleitung dafür sorgen, dass den verantwortlichen Personen beziehungsweise Abteilungen ausreichend Ressourcen für die Erfüllung ihrer Aufgaben zur Verfügung stehen, um ein wirksames DSMS zu gewährleisten.[181]

In Bezug auf die Datenschutz-Organisation ist darauf hinzuweisen, dass der DSB zwar Teil des Datenschutzmanagements ist, jedoch aufgrund der gesetzlich geforderten Unabhängigkeit[182] nicht für die Umsetzung der Maßnahmen verantwortlich sein darf.[183] Deshalb sollte der Tätigkeitsumfang des DSB, der Datenschutz-Abteilung und der sonstigen Mitarbeiter des Datenschutzes im Rahmen der Datenschutz-Organisation festgelegt werden. Die Aufgaben und Zuständigkeiten des DSB waren in den Entwürfen des europäischen Parlamentes und der europäischen Kommission deutlich umfangreicher gestaltet als in der finalen Fassung.[184] So hatte der DSB im ursprünglichen Entwurf neben den in Art. 39 Abs. 1 DS-GVO genann-

[173] Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2020) – S. 10; Für eine detailliertere Definition der Ziele siehe S. 53f.
[174] Vgl. Korge (2020) – S. 83.
[175] Vgl. *Schrulle*, in: Sowa (2020) – S. 26; IDW PS 980 – Tz. 23 „Compliance-Organisation"; Tz. A18; Loomans/Matz/Wiedemann (2014) – S. 70; Gardyan-Eisenlohr/Knöpfle, DuD (2017) – S. 69.
[176] Vgl. *Schrulle*, in: Sowa (2020) – S. 26.
[177] Vgl. Korge (2020) – S. 78.
[178] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel III, Nr. 2; Schrulle, IT-Governance (2019) – S 26; *Schrulle*, in: Sowa (2020) – S. 27.
[179] Vgl. Loomans/Matz/Wiedemann (2014) – S. 67.
[180] Vgl. IDW PS 980 – Tz. 23 „Compliance-Organisation", Tz. A18.
[181] Vgl. *Schrulle*, in: Sowa (2020) – S. 27; IDW PS 980 – Tz. 23 „Compliance-Organisation", Tz. A18.
[182] Vgl. Art. 38 Abs. 3 und Abs. 6 DS-GVO.
[183] Vgl. *Schrulle*, in Sowa (2020) – S. 23.
[184] Vgl. *Paal,* in: Paal/Pauly (2021) – Art. 39, Rn. 3; *Bergt*, in Kühling/Buchner (2020) – Art. 39, Rn. 2ff.; *Klug*, in: Gola (2018) – Art. 39, Rn. 1.

ten Aufgaben auch die Erstellung des Verarbeitungsverzeichnisses gemäß Art. 30 DS-GVO zu überwachen[185] und war für die Überwachung der Dokumentation sowie der Meldung und Benachrichtigung von Verletzungen des Schutzes von personenbezogenen Daten[186] gemäß Art. 33, 34 DS-GVO zuständig.[187] Der in Art. 39 DS-GVO genannte Aufgabenkatalog des DSB ist daher nicht als abschließend zu betrachten, sondern vielmehr als dessen Mindestaufgaben zu verstehen, wie sich aus dem Wortlaut „zumindest folgende Aufgaben" des Art. 39 Abs. 1 S. 1 DS-GVO ableiten lässt.[188] So kann beispielsweise die datenschutzrechtliche Schulung der Mitarbeiter an den DSB delegiert werden.[189] Besteht die Datenschutz-Organisation neben dem DSB noch aus weiteren Mitarbeitern, so sollte festgelegt werden, ob diese Mitarbeiter lediglich dem DSB und dessen gesetzlichen (Mindest-)Aufgaben zuzuordnen sind oder welche weiteren Aufgaben diese haben.[190] Die grundlegende Entscheidung ist dabei, ob die Aufgaben service- oder kontrollorientierten Charakter aufweisen. Hierbei sollte berücksichtigt werden, dass die Datenschutzabteilungen in den meisten Unternehmen sowohl eine dienstleistende als auch kontrollierende Funktion haben. Dieser Zustand ist mit einer Rechts- und Compliance-Abteilung vergleichbar, wodurch lediglich der Schwerpunkt der Arbeit bestimmt wird.[191]

Eine Reglung der Weisungsbefugnis des DSB beziehungsweise der Mitarbeiter der Datenschutzabteilung innerhalb der Datenschutz-Organisation ist für das Unternehmen wichtig, da diese Personen somit verbindliche Weisungen gegenüber anderen Abteilungen oder Mitarbeitern erteilen können.[192] Weisungsbefugt sollte diejenige Stelle sein, die für die tatsächliche Einhaltung des Datenschutzes zuständig ist. Dies kann beispielsweise auch die Compliance- oder Rechtsabteilung sein. Auf dieser Grundlage sollten die entsprechende Rechte eingeräumt sein. Häufig wird von der Unternehmensleitung erwartet, dass die Datenschutzabteilung auch für die Durchsetzung des Datenschutzes zuständig ist. Oftmals fehlt jedoch ein unmissverständliches Mandat der Unternehmensleitung, welches die Datenschutzabteilung adressiert.[193] Wird ein solches Mandat erteilt, sollte dies eindeutig formuliert und schriftlich festgehalten sein. Ist das nicht der Fall, verbleibt die Verantwortung für die Einhaltung des Datenschutzes bei der Unternehmensleitung.[194] Allerdings kann ein solches Mandat im Konflikt zu den gesetzlichen Aufgaben des DSB stehen, insbesondere wenn es zum Erteilen von verbindlichen Anweisungen ermächtigt. Aus dem Grundsatz der Weisungsfreiheit kann abgeleitet werden, dass die Unternehmensleitung und nicht der DSB Entscheidungen zu treffen hat.[195] Sowohl unter dem BDSG a.F. als auch unter der DS-GVO steht grundsätzlich der DSB dem Verantwortlichen beratend zur Seite, wodurch die Neutralität des DSB gewahrt wird und er seinen Kontrollaufgaben effektiv nachgehen kann.[196] Allerdings wäre somit, neben der neutralen, kontrollierenden und beratenden Einheit des DSB, noch eine zweite Einheit notwendig, wie beispielswiese die Rechts- oder Compliance-Abteilung, welche den Datenschutz im Unternehmen aktiv durchsetzt und entsprechende Weisungen erteilt. Insbesondere bei kleinen Unternehmen, welche regelmäßig nur den DSB als zentrale Einheit haben,

[185] Vgl. Art. 37 Abs. 1 lit. d) DS-GVO-E(KOM).
[186] Vgl. Art. 37 Abs. 1 lit. e) DS-GVO-E(KOM).
[187] Vgl. *Paal,* in: Paal/Pauly (2021) – Art. 39, Rn. 3.
[188] Vgl. *Klug*, in: Gola (2018) – Art. 39, Rn. 1; *Paal,* in: Paal/Pauly (2021) – Art. 39, Rn. 4.
[189] Vgl. *Schrulle*, in: Sowa (2020) – S. 27.
[190] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel III, Nr. 2, Anmerkung Nr. 3.
[191] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel III, Nr. 3.
[192] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel III, Nr. 2, Anmerkung Nr. 4.
[193] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel III, Nr. 2, Anmerkung Nr. 5.
[194] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel III, Nr. 2, Anmerkung Nr. 4.
[195] Vgl. *Klug*, in: Gola (2018) – Art. 39, Rn. 4 und 6; *Schrulle*, in: Sowa (2020) – S. 27.
[196] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel III, Nr. 2, Anmerkung Nr. 5.

entsteht deshalb ein unlösbarer Konflikt.[197] Auch bei größeren Unternehmen scheint eine Bündelung der Aufgaben der datenschutzrechtlichen Kontrolle, Beratung und Durchsetzung in einer Einheit beziehungsweise Abteilung am effektivsten zu sein, welche von allen Mitarbeitern anerkannt wird und als zentrale Stelle zum Thema Datenschutz fungiert. In der Literatur wird zunehmend anerkannt, dass die Unternehmensleitung über die Möglichkeit verfügen sollte, Verantwortungsbereiche für die Einhaltung des Datenschutzes an den DSB oder die Datenschutzabteilung zu delegieren.[198] Theoretisch können sämtliche den Datenschutz betreffenden Weisungen über die Unternehmensleitung erteilt und damit die Vorstellungen durchgesetzt werden. Allerdings sollte dieses Mittel nur eingesetzt werden, wenn keine anderen Möglichkeiten mehr verfügbar sind.[199] Ein solches Vorgehen bindet Ressourcen bei der Unternehmensleitung, wirft Fragen der Überzeugungs- und Durchsetzungsfähigkeit des Datenschutzes auf und schafft zudem Unbehagen bei den Beteiligten.

3.5.5 Risiken

In einem effektiven DSMS werden unter Berücksichtigung der Datenschutz-Ziele und der Unternehmensumwelt die Datenschutz-Risiken festgestellt.[200] Gemäß WYBITUL entstehen bei der Umsetzung operative Auswirkungen des betrieblichen Datenschutzmanagements.[201] Dabei sollte analysiert werden, welche Datenschutzverstöße beziehungsweise -vorfälle einen negativen Einfluss auf das Erreichen der Datenschutz-Ziele haben können. Ebenso kann der bestehende Reifegrad der Datenschutzorganisation anhand einer Risikoanalyse abgeleitet werden. Das Feststellen und Beurteilen von Datenschutz-Risiken bildet zudem die Grundlage für ein angemessenes Datenschutz-Programm.[202] Im IDW PH 9.860.1 ist die Forderung nach Elementen eines Datenschutz-Risikomanagements inklusive der DSFA zu finden.[203] Hierfür sollte ein geordnetes Verfahren mit definierten Zuständig- und Verantwortlichkeiten vorliegen, welches regelmäßig überprüft wird.[204]

Im Rahmen des Datenschutz-Risikomanagements sind die größten (sowohl internen als auch externen) Risiken, welche zu einem Verstoß gegen die relevanten Datenschutzvorschriften führen können, anhand einer Risikoanalyse zu identifizieren.[205] Hierdurch kann die Risikosituation des Unternehmens besser eingeschätzt werden.[206] Ebenso ermöglicht dieses Vorgehen, dass aus den identifizierten Risiken zielgerichtete Gegenmaßnahmen entwickelt und abgeleitet werden.[207] Diese Risiken inklusive der Maßnahmen sind den relevanten Stakeholdern mitzuteilen, damit diese die Umsetzung der Maßnahmen überwachen können.[208] Eine solche Risikoanalyse erfolgt typischerweise anhand einer Risikomatrix, die beispielhaft in Tab. 2 dargestellt ist.

[197] Vgl. *Schrulle*, in: Sowa (2020) – S. 23.
[198] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel III, Nr. 2, Anmerkung Nr. 5.
[199] Vgl. Schneider (2018) – S. 46.
[200] Vgl. IDW PS 980 – Tz. 23 „Compliance-Risiken“.
[201] Vgl. Wybitul (2016) – S. 140.
[202] Vgl. IDW PS 980 – Tz. A16.
[203] Vgl. IDW PH 9.860.1 – Anlage 1, Nr. 31–35.
[204] Vgl. *Schrulle*, in: Sowa (2020) – S. 28.
[205] Vgl. Loomans/Matz/Wiedemann (2014) – S. 92.
[206] Vgl. Loomans/Matz/Wiedemann (2014) – S. 97.
[207] Vgl. Loomans/Matz/Wiedemann (2014) – S. 93 + 95; *Schrulle*, in: Sowa (2020) – S. 28.
[208] Vgl. *Schrulle*, in: Sowa (2020) – S. 28.

Risikomatrix						
Schadenshöhe	existenz-bedrohend					
	kritisch					
	spürbar					
	gering					
	unbedeutend					
		unwahr-scheinlich	möglich	gelegentlich	wahr-scheinlich	regelmäßig
		Eintrittswahrscheinlichkeit				

Tab. 2: Risikomatrix[209]

Die Analyse und Bewertung der Risiken erfolgt anhand der Eintrittswahrscheinlichkeit und den möglichen Folgen, wie der Höhe des direkten Schadens oder eventuellen weiteren Folgen, wie einem Bußgeld oder einem aus dem Datenschutzvorfall resultierenden Reputationsverlust (siehe Abb.6).[210]

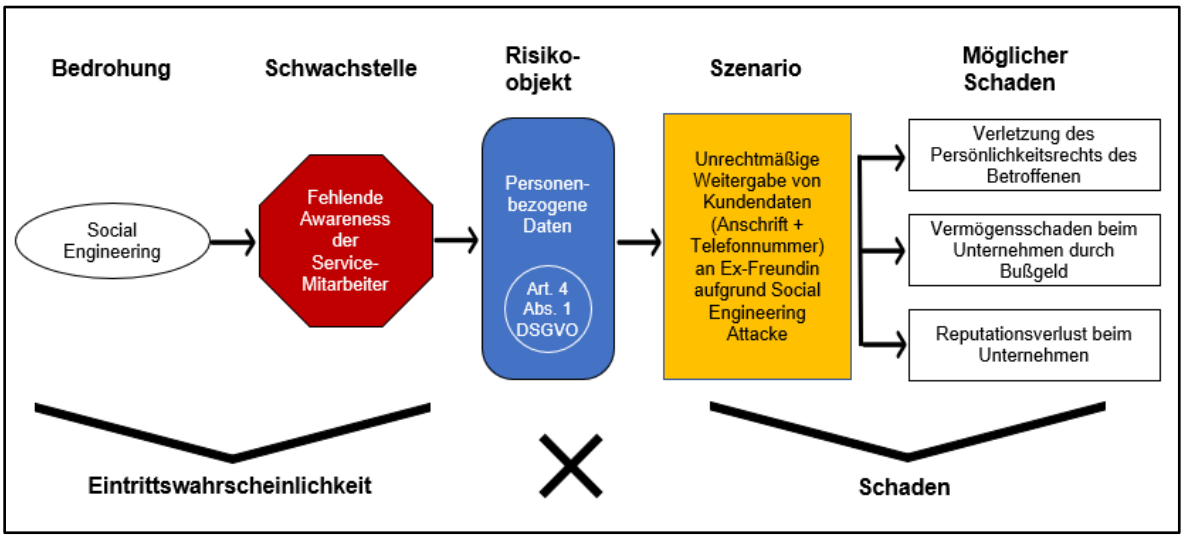

Abb. 6: Zusammenhänge der Risikoanalyse[211]

[209] Eigene Darstellung.
[210] Vgl. IDW PS 980 – Tz. 23 „Compliance-Risiken".
[211] Eigene Darstellung in Anlehnung an: Loomans/Matz/Wiedemann (2014) – S. 98.

Eine Risikoeinschätzung muss, unabhängig von dem Bestehen eines DSMS, durchgeführt werden, beispielsweise im Rahmen der Notwendigkeitsprüfung einer DSFA gemäß Art. 35 DS-GVO. So muss das Risiko jeder Verarbeitungstätigkeit vorab bewertet und dokumentiert werden, um zu überprüfen, ob eine DSFA notwendig ist beziehungsweise um deren fehlende Notwendigkeit entsprechend nachweisen und dokumentieren zu können.[212] Deshalb sollte der Prozess der DSFA standardisiert werden und dabei durch ein zweistufiges Prüfungsverfahren sicherstellen, dass für Verarbeitungstätigkeiten mit hohem Risiko eine DSFA durchgeführt wird.[213] Im ersten Schritt sollte deshalb die Erforderlichkeit gemäß Art. 35 Abs. 3 DS-GVO geprüft werden. Liegt ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der Betroffenen vor, so muss im zweiten Schritt die DSFA durchgeführt werden. Beide Schritte sind dabei zu protokollieren. Ebenfalls sind von den Aufsichtsbehörden Verfahren und Listen veröffentlich worden, wann eine DSFA durchgeführt werden muss.[214] Wie auch in Art. 35 wird ebenfalls in Art. 24 Abs. 1 und Art. 32 DS-GVO die Berücksichtigung der Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen gefordert.[215] Daher sollte zum Management dieser Risiken ein geregelter Prozess eingerichtet werden, der die potentiellen Risiken identifiziert und bewertet sowie Maßnahmen zur Risikobehandlung festlegt und diese anschließend überwacht. Ebenfalls sollten die Risiken an die relevanten Stellen der Organisation kommuniziert und regelmäßig auf deren Aktualität überprüft werden.

Findet das Aktiengesetz Anwendung, so gehört die Erfassung der Unternehmensrisiken und die Einrichtung eines IKS gemäß §§ 91 Abs. 2, 107 Abs. 3 S. 2 zur Aufgabe des Vorstandes.[216] Die Identifikation und Bewertung der Datenschutz-Risiken sollte allerdings unabhängig von der Rechtsform eines Unternehmens durchgeführt werden, weshalb die Datenschutz-Risiken nur einen Teil des unternehmensweiten Risikomanagements darstellen. Diese Risikoidentifizierung und -bewertung sollten einerseits nicht getrennt von den Risikoaktivitäten anderer Abteilungen beziehungsweise Fachbereichen erfolgen, andererseits aber auch im DSMS integriert sein.[217] Dabei sollte das Unternehmen einen einheitlichen Ansatz beim Risikomanagement festlegen und verfolgen. Insbesondere bei einem risikobasierten DSMS[218] stellt die Risikoanalyse und -behandlung einen zentralen Vorgang dar.[219]

Nachdem die Risiken entsprechend analysiert und bewertet wurden, sollte ein ausführliches Register vorliegen, in welchem die jeweiligen Risiken und dazugehörigen Maßnahmen festgehalten sind und welches als Grundlage für die Überwachung der Risiken dient.[220] Dieses Register sollte regelmäßig überprüft und aktualisiert werden, da dies wesentlicher Bestandteil der fortlaufenden Weiterentwicklung des DSMS ist.[221]

3.5.6 Programm

Das Datenschutz-Programm beinhaltet die Grundsätze, Verfahren und Maßnahmen des Unternehmensdatenschutzes, welche beispielsweise auf der Grundlage der bewerteten Daten-

[212] Vgl. Schrulle, IT-Governance (2019) – S. 26; Rieß, DuD (2019) – S. 498; *Schrulle*, in: Sowa (2020) – S. 28.
[213] Vgl. IDW PH 9.860.1 – Anlage 1, Nr. 32.
[214] Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018b); Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018c).
[215] Vgl. IDW PH 9.860.1 – Anlage 1, Nr. 31.
[216] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 1.
[217] Vgl. Loomans/Matz/Wiedemann (2014) – S. 96; Rieß, DuD (2019) – S. 499.
[218] Zur Unterscheidung von Schutzstandards und risikobasiertem DSMS siehe Tabelle 1 in Kapitel 3.
[219] Vgl. Loomans/Matz/Wiedemann (2014) – S. 95; Rieß, DuD (2019) – S. 499.
[220] Vgl. Loomans/Matz/Wiedemann (2014) – S. 96.
[221] Vgl. IDW PS 980 – Tz. A16.

schutz-Risiken definiert und umgesetzt wurden.[222] Diese sollen die Einhaltung der Anforderungen der DS-GVO und des BDSG bei der Verarbeitung personenbezogener Daten sicherstellen.[223] Hierdurch soll gewährleistet werden, dass die Datenschutz-Risiken verringert und somit künftige Datenschutz-Verstöße vermieden werden. Unter den Grundsätzen sind in diesem Zusammenhang die Regelungen und Richtlinien zu verstehen, durch welche die Mitarbeiter zur Einhaltung des Datenschutzes aufgefordert werden.[224] Die Maßnahmen sind oftmals präventiv ausgerichtet und zielen auf die Verhinderung zukünftiger Datenschutzverstöße ab. Falls eine Verhinderung dieser Verstöße nicht möglich ist, sollen die Maßnahmen dazu beitragen, dass die Verstöße frühzeitig erkannt und entsprechende Reaktionen zur Minderung des Schadens eingeleitet werden. Dies kann beispielsweise mit der Hilfe eines Hinweisgebersystems erfolgen. Einige Inhalte des Datenschutz-Programms können Überschneidungen mit Aspekten der Datenschutz-Organisation aufweisen, da der Aufbau und die Integration einer Datenschutz-Organisation Bestandteile des Datenschutz-Programms darstellen.[225] Deshalb können auch im Rahmen des Datenschutz-Programms die Verantwortlichkeiten überprüft und inhaltliche Richtlinien sowie ggf. auch Betriebsvereinbarungen über den Umgang mit personenbezogenen Daten von Mittarbeitern oder Dritten erlassen werden. Zudem umfasst das Datenschutz-Programm, welche Maßnahmen bei festgelegten Verstößen gegen den Datenschutz zu ergreifen sind.[226]

Die Grundsätze, Verfahren und Maßnahmen des Datenschutzes müssen in angemessener Weise dokumentiert sein, damit diese konsistent angewendet werden und personenunabhängig funktionieren.[227] Die internen Vorgaben zur Umsetzung aller datenschutzrechtlichen Anforderungen sollten deshalb in einer Art Ordnung schriftlich festgehalten werden.[228] Dabei sind die entsprechenden Dokumente in Bezug auf Struktur und Inhalt an die jeweiligen Adressaten auszurichten und müssen den jeweiligen Personengruppen zugänglich sein.[229] Um dabei den Überblick zu behalten, kann eine Dokumentenhierarchie in Form einer Dokumentenpyramide hilfreich sein (siehe Abb. **7**7).[230]

[222] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 3; IDW PS 980 – Tz. 23 „Compliance-Programm“ und Tz. A16; IDW PH 9.860.1 – Tz. 13.
[223] Vgl. IDW PH 9.860.1 – Tz. 13.
[224] Vgl. IDW PS 980 – Tz. A17.
[225] Vgl. *Koglin*, in: Koreng/Lachenmann (2018) – Kapitel A, Unterkapitel II, Nr. 3.
[226] Vgl. IDW PS 980 – Tz. 23 „Compliance-Programm“.
[227] Vgl. IDW PH 9.860.1 – Tz. 19 und 21.
[228] Vgl. *Schrulle*, in: Sowa (2020) – S. 26.
[229] Vgl. *Schrulle*, in: Sowa (2020) – S. 27.
[230] Vgl. Schrulle, IT-Governance (2019) – S. 26; IDW PH 9.860.1 – Anlage 1, Nr. 4.

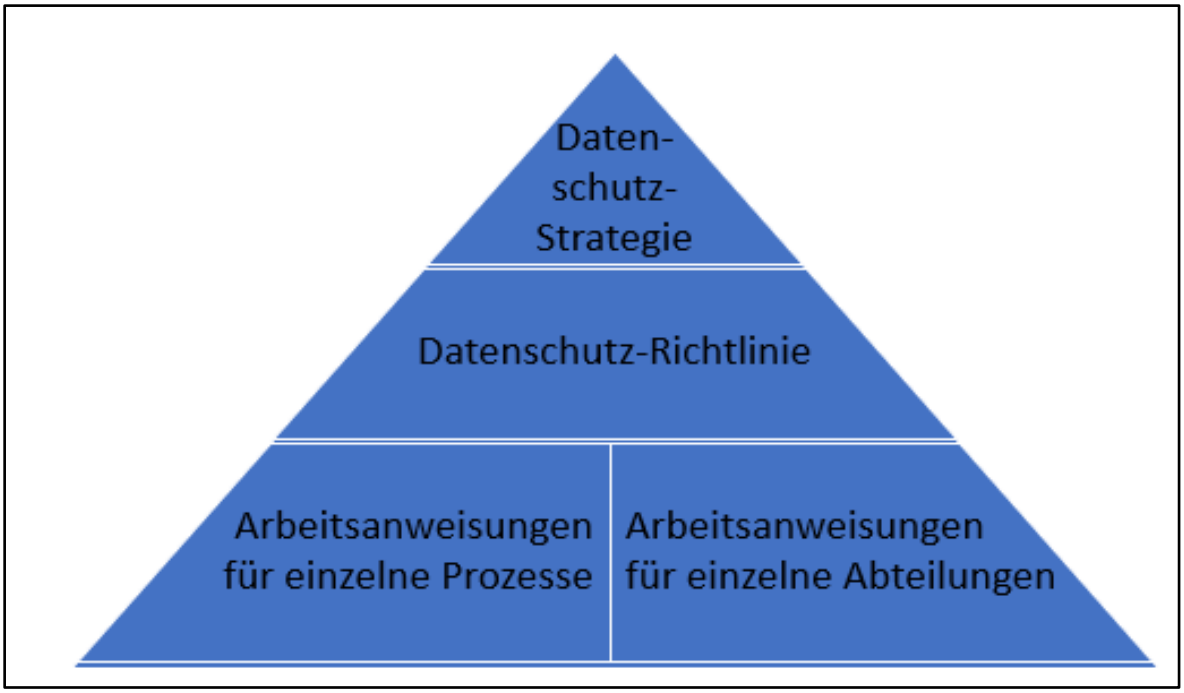

Abb. 7: Dokumentenhierarchie in Form einer Dokumentenpyramide[231]

Laut dem IDW PH 9.860.1 sollte für ein funktionierendes Datenschutz-Programm ein Rahmenwerk vorliegen, welches den Umgang mit dem Datenschutz ausführlich regelt und dabei mindestens die nachfolgenden Bereiche beinhaltet: Datenschutzorganisation, Grundsätze der Verarbeitung personenbezogener Daten gemäß Art. 5 DS-GVO, Stellung und Aufgaben des DSB, Datenschutz-Risikomanagement und DSFA, Zulässigkeit der Verarbeitung personenbezogener Daten, Datenschutz durch Technikgestaltung (Privacy by Design), Verarbeitungs- beziehungsweise Verfahrensverzeichnis, TOM, Datenlöschung, Rechte der Betroffenen, Datenschutzverletzungen und Meldung dieser Verletzungen, Auftragsverarbeitung und Zulässigkeit der Datenübermittlung, Sensibilisierung und Kommunikation, Nachweis und Rechenschaftspflichten.[232] Diese Dokumente müssen nachvollziehbar dokumentiert sein und allen Mitarbeitern zur Verfügung gestellt werden. Ebenso setzt der Prüfungshinweis voraus, dass Richtlinien beziehungsweise Anweisungen vom Management freigeben sind und entsprechend kommuniziert wurden. Die Abhängigkeiten zu anderen Richtlinien sollten zudem bei der Erstellung geprüft und dokumentiert werden. Die Aktualisierung des Rahmenwerks ist regelmäßig durchzuführen.

3.5.7 Kommunikation

Die Datenschutz-Kommunikation ist ein weiterer Baustein eines DSMS nach dem IDW PS 980. Ziel der Kommunikation ist im ersten Schritt, dass sowohl die Belegschaft als auch Dritte darüber informiert werden, wer für den Datenschutz im Unternehmen zuständig sowie verantwortlich ist und welche Inhalte vom Datenschutz-Programmumfasst werden. [233] Dadurch soll sichergestellt werden, dass jeder Mitarbeiter über die Rolle der Verantwortlichen informiert ist, sodass diese ihren Aufgaben effektiv nachgehen können. Ebenso wichtig ist die Kenntnis der beteiligten Personen, die innerhalb des Unternehmens für den Daten-

[231] Eigene Darstellung.
[232] Vgl. IDW PH 9.860.1 – Anlage 1, Nr. 4.
[233] Vgl. IDW PS 980 – Tz. 23 „Compliance-Kommunikation“.

schutz verantwortlich sind, über ihre eigenen Datenschutz-Verantwortungen und -Aufgaben.[234]

Weitere Maßnahmen, die im Rahmen der Datenschutz-Kommunikation durchgeführt werden sollten, sind beispielsweise regelmäßige Schulungen zur Sensibilisierung der Mitarbeiter.[235] So können neue Mitarbeiter im Rahmen ihrer Einarbeitung persönlich geschult werden, wohingegen die Bestandsmitarbeiter eine internetbasierte Basisschulung zur Auffrischung der Grundlagen des Datenschutzes erhalten.[236] Allerdings können in Bereichen mit einem erhöhten Datenschutz-Risiko oder für bestimmte Personengruppen Präsenz-Schulungen sinnvoll sein. Wichtig dabei ist, dass eine Dokumentation von Teilnahmen und Inhalten erfolgt, wodurch die Prozesse nachweisbar sind. Mit Hilfe eines abgestuften Kommunikations- und Schulungskonzeptes kann die bereits angesprochene Sensibilisierung der Mitarbeiter erfolgen und kommuniziert werden, wer welche Aufgaben und Pflichten innerhalb der Datenschutz-Organisation hat. Auch die Berichterstattung des DSB beziehungsweise der Datenschutz-Abteilung gegenüber der Unternehmensleitung ist Teil der Datenschutz-Kommunikation.[237] Hierzu gehört beispielsweise eine aktuelle Einschätzung der Datenschutz-Compliance des Unternehmens, die Information über identifizierte Schwachstellen sowie Aussagen zu generellen Statuskennzahlen wie der Anzahl von Betroffenenanfragen oder Datenschutzverletzungen innerhalb des Berichtszeitraums.[238] Wünschenswert sind dabei auch Auskünfte über die Entwicklung des Reifegrads des Unternehmensdatenschutzes.

Voraussetzungen einer wirksamen Datenschutz-Kommunikation sind auch, dass ausreichende Kenntnisse über die Berichtspflichten vorhanden und die Mitarbeiter sich der Bedeutung einer zeitnahen sowie vollständigen Kommunikation bewusst sind.[239] Hierzu gehört auch, dass Berichtswege etabliert sind und die Mitarbeiter wissen, wer bei einem möglichen Datenschutz-Verstoß beziehungsweise bei Hinweisen auf einen solchen zu informieren ist.[240] Deshalb sollte im Rahmen der Datenschutz-Kommunikation auch ein Data-Breach-Prozess aufgesetzt werden, der beschreibt, wie Datenpannen definiert sind und wie mit diesen umzugehen ist.[241]

3.5.8 Überwachung und Verbesserung

Zuletzt sieht der IDW PS 980 vor, dass sowohl die Angemessenheit als auch Wirksamkeit des DSMS fortlaufend analysiert und überprüft werden.[242] Eine entsprechende Dokumentation des DSMS ist dafür unumgänglich. Durch eine solche Prüfschleife wird ein fortlaufender Verbesserungsprozess wie beim PDCA-Zyklus angestoßen.[243] Werden im Rahmen der Überwachung Schwachstellen des DSMS oder datenschutzrechtliche Verstöße festgestellt, müssen diese an das Management beziehungsweise die hierfür verantwortliche Stelle gemeldet werden.[244] Die Verantwortlichen haben anschließend für die Beseitigung dieser Mängel und der damit verbundenen Verbesserung des Systems sowie für die Durchsetzung der Maßnahmen zu sorgen.

---

[234] Vgl. Schrulle, IT-Governance (2019) – S. 26.
[235] Vgl. Schrulle, IT-Governance (2019) – S. 26.
[236] Vgl. *Schrulle*, in: Sowa (2020) – S. 27.
[237] Vgl. IDW PS 980 – Tz. A19.
[238] Vgl. *Schrulle*, in: Sowa (2020) – S. 28.
[239] Vgl. IDW PS 980 – Tz. A19.
[240] Vgl. IDW PS 980 – Tz. A19.
[241] Vgl. *Sowa*, in: Sowa (2020) – S. 18.
[242] Vgl. IDW PS 980 – Tz. 23 „Compliance-Überwachung und Verbesserung“.
[243] Vgl. *Schrulle*, in: Sowa (2020) – S. 34.
[244] Vgl. IDW PS 980 – Tz. 23 „Compliance-Überwachung und Verbesserung“.

Die Datenschutz-Überwachung sollte für gewöhnlich von einer prozessunabhängigen Instanz wie beispielsweise der Internen Revision durchgeführt werden.[245] Durch diese Überwachung soll festgestellt werden, ob das DSMS unter Beachtung der DSMS-Grundsätze angemessen ausgestaltet und zudem auch wirksam ist. Hierfür ist eine eindeutige Festlegung der Zuständigkeiten für die Datenschutz-Überwachung ebenso erforderlich wie ein Überwachungsplan, ausreichende (erfahrene) Ressourcen für die Überwachung und eine Strukturierung der Berichtswege an die zuständige Stelle. Die Ergebnisse der Überwachungsmaßnahmen können auf Schwachstellen des DSMS hindeuten, weshalb diese zu untersuchen und ggf. entsprechende Maßnahmen zur Wirksamkeitssteigerung zu ergreifen sind. Beispielsweise kann dies durch eine intensivere Kommunikation des Datenschutz-Programms oder spezielle Schulungen erreicht werden.

Im Prüfungshinweis 9.860.1 werden als Prüfungshandlung beispielsweise die Einsichtnahme in Auswertungen über die Erreichung beziehungsweise Abweichung der Ziele von einzelnen Bereichen des DSMS und die regelmäßige Überprüfung dieser empfohlen.[246] Das regelmäßige Überprüfen ist von Bedeutung, da hierdurch der kontinuierliche Verbesserungsprozess vorangetrieben wird und das DSMS optimiert werden kann.

Insbesondere das Datenschutzmonitoring als Element des DSMS nach dem IDW PS 980 ist zur Messung, Beurteilung und Verbesserung der Wirksamkeit eines DSMS elementar, da eine Steuerung nur erfolgen kann, wenn entsprechende Messungen vorgenommen wurden.[247] Gemäß JUNG bestehen die primären Ziele im Datenschutz darin, die gesetzlichen Vorgaben einzuhalten.[248] Allerdings können die Ziele wie in Kapitel 3.5.3 auch über die Einhaltung der gesetzlichen Vorgaben hinaus gehen. JUNG vertritt dabei die Meinung, dass keine Verbesserung des DSMS stattfindet, solange dessen Verbesserungsbedarf nicht festgestellt wird.[249] So können beispielsweise in Folge einer Wirksamkeitsprüfung, Anpassungen von Schulungen oder von internen Richtlinien und Prozessen angestoßen werden.

Hauptsächlich sollen daher die Effektivität und Effizienz der Maßnahmen gemessen werden können. Allerdings kann eine Wirksamkeitsmessung nicht ausschließlich anhand der Anzahl entdeckter datenschutzrechtlicher Rechtsverstöße aufgebaut werden, da diese eine zu geringe Aussagekraft hätten.[250] Um eine zutreffende Aussage über die Wirksamkeit des DSMS in Bezug auf die Anzahl an Rechtsverstößen ableiten zu können, wäre ein Vergleich zwischen der Anzahl der auftretenden Rechtsverstöße hilfreich, welche mit und welche ohne einem DSMS entstehen. Zusätzlich müsste die Sicherheit bestehen, dass sämtliche Datenschutzvorfälle entdeckt und gemeldet wurden. Da allerdings beide Voraussetzungen nicht möglich sind, ist auch ein direkter Vergleich unmöglich.

Damit stellt sich die Frage, wie der Nutzen und die Wirksamkeit eines etablierten DSMS gemessen werden können.[251] Hierfür wird nachfolgend auf verschiedene Methoden zur Messung der Wirksamkeit eines DSMS eingegangen.

Die Messung beziehungsweise die Ermittlung kritischer Erfolgsfaktoren, wie dem Fortschritt oder dem Erfüllungsgrad bestimmter Ziele, kann einen ersten Schritt darstellen, um die Ziele

[245] Vgl. IDW PS 98ß – Tz. A20.
[246] Vgl. IDW PH 9.860.1 – Anlage 1, Nr. 1.
[247] Vgl. *Schlaghecke*, in: Hauschka/Moosmayer/Lösler (2016) – § 43, Rn. 82 f.
[248] Vgl. Jung, CCZ (2018) – S. 226.
[249] Vgl. Jung, CCZ (2018) – S. 226
[250] Vgl. Pape, CCZ (2009) – S. 233.
[251] Vgl. Hansch, ZD (2019) – S. 246.

zur Messung der Wirksamkeit eines DSMS zu erfüllen.[252] Deshalb werden für diese Messungen oftmals KPIs oder andere Leistungskennzahlen herangezogen, da diese eine Steuerung und Kontrolle komplexer Vorgänge ermöglichen.[253] Aus diesem Grund werden Kennzahlen und KPIs[254] für einen Bereich des Unternehmens benötigt, welcher die Einhaltung von Richtlinien und Gesetzen beaufsichtigt.

KPI werden in der jüngeren deutschsprachigen Literatur auch Kennziffern, Kontrollzahlen, Kennzahlen, Messzahlen oder Steuerungsgrößen genannt, wobei die unterschiedlichen Begriffe meist synonym verwendet werden.[255] Allgemein besteht in der deutschen Sprache aber ein Unterschied zwischen einer Kennzahl und einem Indikator.[256] Indikatoren erlauben nur eine eingeschränkte Aussage über die Messgröße und deren Veränderung.[257] Sie liefern keinen konkreten Tatbestand, sondern nur Anzeichen für einen bestimmten Umstand und erleichtern somit die Einschätzung der Entwicklung des Leistungsniveaus.[258] Mit Hilfe von Indikatoren können deshalb nicht direkt messbare Größen abgebildet werden. Im Gegensatz zu Kennzahlen stellen Indikatoren keine quantitativen Informationen dar.[259] Sie sind meist nicht selbsterklärend und müssen deshalb entsprechend interpretiert werden.[260] Außerdem sind Indikatoren leichter zu messen, weshalb sie auch eine geringere Aussagekraft als Kennzahlen aufweisen.[261] Für gewöhnlich werden Indikatoren benutzt, um Rückschlüsse aus den vorgelagerten Ursachen-Wirkungs-Zusammenhängen zu ziehen und diese auf die Sachverhalte zu übertragen. So kann die Anzahl der Datenschutz-Schulungen beziehungsweise deren Teilnehmerzahl eine Sensibilisierung der Mitarbeiter indizieren, jedoch keine Größe der Sensibilisierung gemessen werden.[262] Deshalb versteht man unter einem KPI in diesem Zusammenhang einen einfachen und verständlichen Indikator, welcher die Leistungsfähigkeit des DSMS in Form einer Kennziffer misst und wiedergibt. Anhand dieser speziellen Kennzahlen ist eine Bewertung möglich, ob und in welchem Umfang die zuvor festgelegten Aufgaben und Ziele erreicht wurden.[263]

Während bei einem klassischen Audit der Frage nachgegangen wird, ob die vorgenommen Maßnahmen richtig umgesetzt werden[264] und ob alle nötigen Prozesse vorhanden sind, entfaltet die Steuerung mit Hilfe von KPIs schon früher ihr Potential.[265] Wenn bereits die gemessenen KPIs eine Abweichung zum Zielzustand andeuten, wird dies aller Wahrscheinlichkeit nach auch bei einem umfangreicheren Audit festgestellt werden. KPIs sind deshalb prognostische Indikatoren, welche widerspiegeln, ob eine Datenschutz-Compliance erreicht wird oder zumindest erreichbar scheint.

---

[252] Vgl. *Demir/Theis*, in: Fiedler (2018) – S. 379.
[253] Vgl. *Mußmann*, in: Kleinfeld/Martens (2018) – S. 304.
[254] Unterscheidung von Kennzahlen und KPI: Eine Kennzahl ist ein Wert, welcher direkt messbar ist. Ein KPI hingegen lässt sich nicht direkt messen, sondern zeigt den Erfüllungsgrad einer bestimmten Zielsetzung an. Deshalb ist die Formulierung von messbaren Zielen für die Ermittlung von KPI notwendig.
255 Vgl. Kleindienst (2017) – S. 41; Mußmann, in: Kleinfeld/Martens (2018) – S. 304.
[256] Vgl. Kaack (2012) – S. 67; Gladen (2014) – S. 9f.
[257] Vgl. Kaack (2012) – S. 67f.
[258] Vgl. Distelzweig (2014) – S. 12.
[259] Vgl. Gladen (2014) – S. 9.
[260] Vgl. Schreyer, M. (2007) – S. 4.
[261] Vgl. Distelzweig (2014) – S. 12.
[262] Vgl. Brandt (2017) – S. 80f.
[263] Vgl. Hohmann/Pede, CB (2017) – S. 416.
[264] Vgl. Sowa (2017) – S. 85.
[265] Vgl. Jung, CCZ (2018) – S. 226.

Soll die Wirksamkeit des DSMS mit Hilfe von KPIs gemessen werden, müssen zunächst eindeutige und verständliche Ziele definiert und festgelegt werden.[266] Dies kann beispielsweise anhand der konkreten Datenschutz-Ziele erfolgen. Jedoch sollten die Ziele und Zielwerte nicht abstrakt bestimmt werden,[267] sondern sollten unternehmensbezogen und risikoadäquat sein, weshalb vorab eine umfassende Risikoanalyse erforderlich ist.[268] Für diese Zielwerte können anschließend KPIs bestimmt werden, welche zukünftig erhoben, abgeglichen und interpretiert werden, wodurch der Grad der Zielerreichung messbar wird.[269] Bleiben einzelne KPIs bei einer späteren Überprüfung hinter dem zuvor definierten Ziel, so sind die Hintergründe hierfür zu hinterfragen und Gegenmaßnahmen zur künftigen Verbesserung zu ergreifen. Hierdurch entfalten die KPIs ihre Steuerungsfunktion. Eine nachhaltige Verbesserung des bestehenden Systems wird somit ermöglicht. Wenn in den Vorjahren noch keine Daten erhoben wurden beziehungsweise noch keine valide Datenlage vorliegt, sollten zunächst eindimensionale Messgrößen erhoben und mit diesen gearbeitet werden. Deshalb sollten die für die Performance des DSMS relevanten Indikatoren identifiziert werden. Außerdem müssen die KPIs objektiv sowie unmissverständlich sein und zudem möglichst keine Fehlinterpretation erlauben. Denn nicht der KPI, sondern die methodische Herleitung des KPI wird kritisch hinterfragt,[270] damit innerhalb des Unternehmens ein einheitliches Verständnis darüber herrscht, was beispielsweise ein Datenschutzverstoß ist und wann dieser vorliegt.[271] Die Qualität der Kennzahlen ist somit entscheidend und wichtiger als deren Anzahl.[272] Um KPIs als Instrument zur Steuerung zu verwenden sollte mit einer überschaubaren Anzahl an Kennzahlen gearbeitet werden.[273]

Zur Bewertung eines DSMS schlägt HANSCH vor, dass die KPIs in verschiedene Klassen eingeteilt werden könnten.[274] Er nimmt dabei die folgende Gruppierung der Kennzahlen vor:

- Kennzahlen, die zur Bewertung der Wirksamkeit einzelner Prozesse beziehungsweise des DSMS dienen, wie beispielsweise die Entwicklung der Anzahl der Meldungen über Datenpannen oder sonstigen Hinweisgebersystemen, welche im Zusammenhang mit Datenschutzverstößen sowie der Durchlaufgeschwindigkeit dieser Prozesse stehen.
- Kennzahlen, welche die Reaktionsfähigkeit und -zeit der Prozesse wiedergeben, z. B. wie lange für die Durchführung einer Datenschutzfolgeabschätzung gemäß Art. 35 DS-GVO durchschnittlich gebraucht wurde.
- Kennzahlen, mit welchen der Output des DSMS erfasst wird, beispielsweise wie viele Mitarbeiter die Datenschutzschulung beziehungsweise das E-Learning zum Datenschutz erfolgreich absolviert haben oder wie oft datenschutzrechtliche Beratungen von den Fachabteilungen gefordert und durchgeführt wurden. Bezüglich der Schulungen von Mitarbeitern können detailliertere KPIs entwickelt werden, wenn beispielsweise zwischen neu eingestellten Mitarbeitern und Bestandsmitarbeiter unterschieden wird oder für Mitarbeiter aus Abteilungen mit erhöhtem Risiko, wie beim Umgang mit besonderen personenbezogenen Daten i. S. d. Art. 9 DS-GVO, spezielle Schulungen angeboten werden.

[266] Vgl. Hansch, ZD (2019) – S. 247.
[267] Vgl. Jung, CCZ (2018) – S. 226.
[268] Vgl. Koyuncu (2015) – S. 584.
[269] Vgl. Hansch, ZD (2019) – S. 247.
[270] Vgl. Sowa (2017) – S. 91.
[271] Vgl. Jung, CCZ (2018) – S. 227.
[272] Vgl. Georg (2019) – S. 5.
[273] Vgl. Jung, CCZ (2018) – S. 226.
[274] Vgl. Hansch, ZD 2019 – S. 246.

Werden diese KPIs über mehrere Jahre erhoben, lassen sich daraus beispielsweise Aussagen über den Wissensstand der Belegschaft oder bestimmter Abteilungen ableiten. Aus diesen können dann weitere, spezifisch zugeschnittene Schulungs-, Kommunikations- oder sonstige Maßnahmen entwickelt werden, welche den datenschutzrechtlichen Wissenstand kontinuierlich verbessern.

Außerdem können aus verschiedenen KPIs Rückschlüsse auf die Belastbarkeit einzelner Prozesse innerhalb des DSMS gezogen werden.[275] So kann der Umgang mit Betroffenenanfragen, wie dem Auskunftsrecht nach Art. 15 DS-GVO, analysiert werden. Ebenso kann eine Kennzahl ausdrücken, wie lange für die Beantwortung einer Anfrage benötigt wird und wie viele Auskunftsersuchen durchschnittlich in einem bestimmten Zeitraum anfallen. Somit kann ermittelt werden, ob die Datenschutz-Organisation auch bei einem erhöhten Aufkommen von Anfragen, beispielsweise weil das Unternehmen aktuell verstärkt in den Medien auftaucht und damit die öffentliche Wahrnehmung erhöht ist, sämtliche Anfragen innerhalb der gesetzlichen Fristen vollumfänglich beantworten kann. Ebenso kann hierdurch die Kapazitätsgrenze des Systems ermittelt werden. Als weitere mögliche Kennzahl könnte beispielsweise ermittelt werden, wie viele Vollzeitstellen (FTE) im Datenschutz pro 1.000 Mitarbeiter tätig sind[276] oder wie viele Mitarbeiter im Verhältnis zur Gesamtbelegschaft an Maßnahmen zur Steigerung des Datenschutz-Bewusstseins teilgenommen haben.[277]

Der Adressat dieser KPIs sollte festgelegt werden, wobei durchaus mehrere Adressaten existieren können. So haben der betriebliche DSB beziehungsweise KDSB und die Datenschutz-Abteilung ein Interesse, die von ihnen ein- und durchgeführten Maßnahmen auf Effektivität zu überprüfen, um ggf. nachsteuern zu können. Gemäß Art. 39 Abs. 1 lit. b) DS-GVO hat der DSB unter anderem die Aufgabe zu überwachen, dass der Verantwortliche die Anforderungen der DS-GVO einhält und diesen auch bei Mängeln darauf hinzuweisen.[278] Das schließt ein, dass der DSB die Strategien des Verantwortlichen überwachen muss, woraus eine Hinweispflicht gegenüber der Geschäftsleitung entsteht. Deshalb ist eine Überprüfung der getroffenen Maßnahmen bezüglich der Effektivität unabdingbar. Eine solche Überprüfung wird ohne die Messung einzelner Kennzahlen oder KPIs für den DSB kaum möglich sein, weshalb er ein Interesse an deren Erhebung und Auswertung hat.[279] Neben dem DSB und der Datenschutz-Abteilung kann allerdings auch die Unternehmensleitung ein starkes Interesse an den KPI haben, da diese auch gesetzlich dazu verpflichtet sind, Kenntnis darüber zu haben, ob und inwieweit das Unternehmen den datenschutzrechtlichen Verpflichtungen nachkommt und wie die Effektivität des DSMS ist.[280] Die KPIs können also neben der Effektivitätsmessung auch dazu verwendet werden, um Investitionen in den Datenschutz auf Rentabilität zu überprüfen.[281] Außerdem bietet sich an, dass Risiken aus den Kennzahlen und KPIs abgeleitet und in betriebswirtschaftlichen Größen dargestellt werden.[282] Somit kann die Aufmerksamkeit bei der oftmals stark auf Zahlen orientierten Unternehmensleitung erhöht und weitere erforderliche Mittel gewährt werden.

Entscheidet sich ein Unternehmen die Wirksamkeit des DSMS mit Hilfe von KPIs zu überwachen, ist die Messgröße der KPI zu definieren. Beispielsweise werden die allgemeine Daten-

[275] Vgl. Hansch, ZD (2019) – S. 247.
[276] Vgl. Brandt (2017) – S. 80.
[277] Vgl. *Dieners/Lembeck*, in: Dieners (2010) – Kapitel 7, Unterkapitel D, Rn. 83.
[278] Vgl. *Scheja*, in: Taeger/Gabel (2019) – § 39, Rn. 7 ff.
[279] Vgl. Hansch, ZD (2019) – S. 247.
[280] Vgl. *Poppe*, in: Inderst/Bannenberg/Poppe (2017) – Kapitel 1.6, Rn. 32 und 35.
[281] Vgl. Jung, CCZ (2018) – S. 226; / Wybitul (2016) – Anhang 1: Praktiker-Glossar.
[282] Vgl. Hansch, ZD (2019) – S. 246.

schutz-Compliance oder die Einhaltung einzelner spezieller Normen betrachtet.[283] Ebenso können die KPIs für das gesamte Unternehmen oder für einzelne Abteilungen erhoben werden.

Bei der Wirksamkeitsmessung durch KPIs besteht jedoch stets eine gewisse Manipulationsgefahr, da Zahlen manipuliert werden können, um je nach Zielrichtung der KPIs ein entsprechendes Ergebnis zu erhalten.[284] Ebenso kann die unterschiedliche Interpretation von Ereignissen zu Problemen führen. So kann eine niedrige Anzahl gemeldeter Datenpannen als Zeichen für eine gute datenschutzrechtliche Aufklärung interpretiert werden. Daraus kann jedoch auch geschlossen werden, dass eine Sensibilisierung fehlt, weshalb die Mitarbeiter nicht wissen, wann eine Datenpanne vorliegt und wann beziehungsweise dass diese zu melden ist.[285] Deshalb sollten bei der Abweichung eines KPI von dessen Zielwert nicht unmittelbar Gegenmaßnahmen ergriffen werden, sondern die Maßnahmen überlegt, analysiert und anschließend umsetzt werden.[286] Denn ein KPI ist ein Indikator, welcher nur eine gewisse Richtung aufzeigt und deshalb noch einer Interpretation bedarf.[287] Das kann einer der Gründe sein, weshalb in einer Studie ermittelt wurde, dass 53 % der befragten Führungskräfte kein Vertrauen in Kennzahlen haben und diese ungeeignet finden, um eine künftige Entwicklung verlässlich einzuschätzen.[288]

Auch wenn die Erhebung und Auswertung von KPIs innerhalb eines DSMS nicht zwingend erforderlich sind, ist die Durchführung trotzdem empfehlenswert. Durch das Erheben und Auswerten von KPI können Zielabweichungen frühzeitig festgestellt werden. Außerdem sind KPIs notwendig, um einen kontinuierlichen Verbesserungsprozess im DSMS zu integrieren.[289] Zudem bieten KPIs die Möglichkeit, Kosten durch die Optimierung von Prozessen zu senken und die Effektivität des DSMS und somit auch der gesamten Unternehmens-Compliance-Organisation zu erhöhen.

Um in der Praxis die Effektivität, Effizienz und damit auch die Qualität eines DSMS zu dokumentieren, wird häufig das Datenschutzreifegradmodell[290] verwendet.[291]

Wie jeder andere Prozess lassen sich auch die Prozesse eines DSMS in Form von Reifegraden bewerten.[292] Dabei bewegen sich die Einstufungen auf einer Werteskala zwischen 0 (keine Umsetzung) und 5 (kontinuierliche Verbesserung) und lassen sich wie in Tab. 3 beschreiben:

[283] Vgl. Hohmann/Pede, CB (2017) – S. 416.
[284] Vgl. Jung, CCZ (2018) – S. 227.
[285] Vgl. *Dieners/Lembeck*, in: Dieners (2010), Kapitel 7, Unterkapitel D, Rn. 83.
[286] Vgl. *Künzel*, in: Künzel Erfolgsfaktor Performance Management, 2016 – S. 18.
[287] Vgl. Jung, CCZ (2018) – S. 227.
[288] Vgl. Kleindienst (2017) – S. 5.
[289] Vgl. Hansch, ZD (2019) – S. 247.
[290] Englisch: (Data) Privacy Maturity Models.
[291] Vgl. Wybitul (2016) – S. 142.
[292] Vgl. Wybitul (2016) – S. 142.

Reifegrad	Bezeichnung	Erklärung
0	Keine Umsetzung	Es sind bisher keine Maßnahmen ergriffen, erkennbar oder geplant.
1	Formlose Umsetzung	Es liegen einzelne Maßnahmen vor, allerdings liegt kein wirklicher Prozess vor oder ist kaum organisiert.
2	Geplant und weiterverfolgt	Es existiert ein stabiler Prozess, welcher in Projekten mit einem Projektmanagement gelebt wird.
3	Gut definiert	Es liegt ein definierter Prozess vor, welcher die konsistente Umsetzung des Prozesses sicherstellt.
4	Qualitativ – kontrolliert	Es erfolgen Prozessanalysen und -messungen, um den Prozess weiterzuentwickeln.
5	Kontinuierliche Verbesserung	Zur Prozessbewertung und -optimierung wird das Management regelmäßig eingebunden.

Tab. 3: Datenschutzreifegradmodel[293]

Bei einem Reifegradmodell sollten die wichtigsten Prozesse des DSMS regelmäßig bewertet werden.[294] Dieser Ansatz ist allerdings erst dann von Bedeutung, wenn die bewerteten Prozesse auch in Bezug zu den Datenschutz-Risiken gesetzt werden.[295] Damit kann transparent festgelegt werden, welche Datenschutz-Risiken in den jeweiligen qualitativen Abstufungen prozessual angegangen werden.[296] Um jedoch einen umfassenden Blick auf die Qualität der Datenschutz-Prozesse zu erhalten, müssen das DSMS und seine Prozesse über mehrere Jahre analysiert und bewertet werden.[297] Das Ziel dabei ist die Qualität aller Teilbereiche und Prozesse des DSMS zu erhöhen. Regelmäßige Analysen helfen dabei die noch unzureichend gesteuerten Prozesse zu identifizieren und zu verbessern. Das Reifegradmodell kann dabei helfen, die künftigen Schwerpunkte zur Weiterentwicklung des DSMS zu setzen.

Neben der Effektivitätsmessung mithilfe von KPIs oder durch das Reifegradmodell könne auch einzelne Prozesse beziehungsweise Bausteine des DSMS auf ihre Effektivität und Effizienz überprüft werden. Beispielsweise kann die Datenschutz-Kultur auf ihre Wirksamkeit überprüft werden, indem Mitarbeiter befragt werden, ob diesen die Relevanz des Datenschutzes bewusst ist, wie diese den „Tone from the Top“ wahrnehmen und ob sie ein Datenschutz-Bewusstsein haben. Auch das Management kann befragt werden beziehungsweise in die Protokolle des Managements Einsicht genommen werden, um den „Tone from the Top“ nachzuvollziehen. Ebenso können die Datenschutz-Ziele auf ihre Effizienz durch Einsichtnahme in Berichte und Auswertungen über die Zielerreichung oder -abweichung überprüft werden. Auch regelmäßige Überprüfungen und ggf. Anpassungen der Ziele können nachverfolgt werden. Das datenschutzrechtliche Rahmenwerk, welches zum Baustein des Datenschutz-Programms gehört, kann nur effektiv sein, wenn die wichtigsten Bereiche des Datenschutzes durch Richtlinien geregelt werden, das Rahmenwerk regelmäßig aktualisiert wird und alle Richtlinien vom Management freigegeben sind. Dies kann durch die Prüfung der Richtlinien ermittelt werden. Die Datenschutz-Organisation kann ebenfalls auf Effektivität geprüft werden, indem Einsicht in die Dokumentation zu regelmäßigen Abstimmungen zwischen dem DSB und der Datenschutz-Abteilung sowie auch zwischen der Datenschutz-

[293] Eigene Darstellung in Anlehnung an: Wybitul (2016) – S. 142; BSI (2021) – Reifegradmodelle.
[294] Vgl. Wybitul (2016) – S. 142.
[295] Vgl. Wybitul (2016) – S. 142f.
[296] Vgl. Wybitul (2016) – S. 143.
[297] Vgl. BSI (2021) – Reifegradmodelle.

Abteilung und den DSK beziehungsweise Fachbereichen genommen wird. Zudem kann geprüft werden, ob die Aufgaben und Verantwortlichkeiten der jeweiligen Personen beziehungsweise Personengruppen aus der Stellen- und Aufgabenbeschreibung auch der betrieblichen Praxis entsprechen. Die Datenschutz-Risiken können beispielsweise durch die Prüfung der Risikobewertung und der daraus folgenden Risikobehandlung, der Überwachung der Maßnahmen und der entsprechenden Kommunikation der festgestellten Risiken an die Verantwortlichen und relevanten Stellen des Unternehmens auf ihre Effektivität und Effizienz geprüft werden. In die Risikobewertung kann bei einzelnen Verarbeitungstätigkeit Einsicht genommen und überprüft werden, ob die TOM gemäß dem Verarbeitungsverzeichnis ergriffen wurden. Innerhalb der Datenschutz-Kommunikation kann z. B. die Effektivität der Schulungen durch Einsichtnahme in Nachweise über die Schulungen und das Sichten der getroffenen Erfolgskontrollen geprüft werden, welche den gewünschten Wissenstand sicherstellen. Ebenso kann geprüft werden, ob eine regelmäßige Aktualisierung der Schulungsinhalte im Schulungskonzept vorgesehen ist und ob die Inhalte in dem vorgeschriebenen Rhythmus aktualisiert werden. Eine weitere Möglichkeit besteht darin, im Rahmen einer Funktionsprüfung zu beurteilen, ob die Grundsätze und Maßnahmen innerhalb eines bestimmten Zeitraums wirksam waren.

4 SCHLUßBETRACHTUNG

Zukünftig wird der Datenschutz weiter an Bedeutung gewinnen. Dies liegt zum Teil an neuen Gesetzen und damit einhergehend auch mit einem tendenziell höheren Risiko an Bußgeldern und Schadensersatzansprüchen. Zudem stellt Datenschutz ein wichtiges Element der datengetriebenen Geschäftsmodelle dar.[298] Dies wird beispielsweise durch den IoT-Trend verstärkt, wodurch zahlreiche Geräte „smart“ sowie vernetzt sind und Nutzer die Möglichkeit haben, sich eigene Profile zu erstellen, welche oftmals nicht ausschließlich lokal auf den Geräten gespeichert werden. So war das Thema „DSGVO Compliance“ der Top-Technologie-Trend des Jahres 2019 gemäß einer Studie des Beratungs- und IT-Dienstleistungsunternehmens Capgemini.[299] Auch die Corona-Pandemie erwies sich als Treiber für den Ausbau der Digitalisierung. So ergab eine Umfrage im September und Oktober 2020, dass 87 % der befragten Unternehmen und Behörden die Pandemie zum Anlass nahmen, die Digitalisierung weiter auszubauen.[300]

Zukünftige Anforderungen an die Funktion und den Umfang eines DSMS können unter anderem davon abhängen, wie weit der Anspruch auf Kopie der personenbezogenen Daten gemäß Art. 15 Abs. 3 S. 1 DS-GVO ausreichen wird. Hierbei herrschen gegensätzliche Ansichten. So wird der Standpunkt vertreten, dass der Anspruch auf Kopie nur bedeute, dass der Betroffene eine schriftliche Auskunft mit den Angaben nach Art. 15 Abs. 1 verlangen könne. Allerdings existiert eine weitere Auffassung, dass eine Kopie aller Dokumente und Dateien herauszugeben ist, welche einen Bezug zur betroffenen Person vorweisen. Dies würde auch Screenshots und Chats (wie beispielsweise Microsoft Teams, Skype for Business, slack etc.) sowie den gesamten E-Mail-Verkehr von und über die betroffene Person beinhalten. Auch innerhalb der Rechtsprechung werden die verschiedenen Ansichten vertreten. So hat das Landesarbeitsgericht Baden-Württemberg in seinem Urteil vom 20.12.2018 entschieden, dass sich der Anspruch nicht nur auf die in der Personalakte gespeicherten personenbezo-

[298] Vgl. *Schrulle*, in: Sowa (2020) – S. 35.
[299] Vgl. Capgemini (2019).
[300] Vgl. Capgemini (2021).

genen sondern auf sämtliche „Leistungs- und Verhaltensdaten“ bezieht.[301] Das LG Köln wiederum entschied in seinem Urteil vom 18.03.2019, dass der Anspruch aus Art. 15 DS-GVO nicht der vereinfachten Buchführung der betroffenen Person dient, sondern sicherstellen soll, dass die betroffene Person den Umfang und Inhalt der gespeicherten personenbezogenen Daten beurteilen kann.[302] Der Auskunftsanspruch beziehe sich nicht auf sämtliche interne Vorgänge des Unternehmens, wie beispielsweise Vermerke oder Schriftverkehr. Durch die Begründung des LG Köln wäre die Herausgabepflicht des E-Mail-Verkehrs ehemaliger Beschäftigter zu verneinen. Eine höchstrichterliche Entscheidung liegt hierzu bisher nicht vor. Ein solcher Fall wurde dem Bundesarbeitsgericht bereits vorgelegt, allerdings wurde dieser aus prozessualen Gründen abgewiesen.[303] Die zukünftige Stellungnahme der Arbeits- und Landesarbeitsgerichte sowie der Aufsichtsbehörden bleibt daher abzuwarten. Abhängig von der Positionierung der Rechtsprechung und der Aufsichtsbehörden können Auswirkungen auf die Speicherbegrenzung beziehungsweise Löschung von personenbezogenen Datenentstehen. Wenn eine Kopie von jeglichen personenbezogenen Daten im Rahmen eines Auskunftsersuchens zur Verfügung gestellt werden muss, dann müssen diese Daten mit sehr hoher Wahrscheinlichkeit auch innerhalb eines Löschkonzepts berücksichtigt und regelmäßig nach der Erfüllung des Verarbeitungszwecks gelöscht werden, sofern keine Aufbewahrungspflichten bestehen. Die reine Definition von Löschfristen ist unzureichend.[304] Die Löschung der personenbezogenen Daten muss durchgeführt und protokolliert werden.[305] Um solchen Auskunftsansprüchen und Löschpflichten entsprechen zu können und diese mit möglichst geringem Aufwand bearbeiten zu können, empfiehlt sich deshalb ebenso die Investition in den Ausbau, die Pflege und Weiterentwicklung eines DSMS.[306]

Außerdem wird sich zeigen, welcher der etablierten Standards (IDW PH 9.860.1 mit dem IDW PS 980, die ISO/IEC 27701 oder das Standard-Datenschutzmodell) sich zukünftig für DSMS durchsetzen kann. So gewinnt das Standard-Datenschutzmodell in Deutschland durch die Verankerung im IT-Grundschutz-Kompendium (CON.2) an Akzeptanz.[307] Insbesondere im Konsumentenbereich sind zwar diverse Anbieter von Zertifikaten verfügbar, welche allerdings i. d. R. keinem offiziellen Standard unterworfen sind, weshalb deren Aussagekraft gering ist.

Da die meisten Prozesse des Datenschutzes losgelöst von anderen Prozessen gepflegt und dokumentiert werden und die Datenverarbeitungen dynamischer sowie komplexer werden, sind neue Ansätze zur intelligenten beziehungsweise „smarten“ Verknüpfung von Dokumentationen notwendig.[308] So könnte zukünftig ein sich automatisch aktualisierendes Verfahrensverzeichnis entwickelt werden, welches Informationen aus weiteren Systemen und Programmen des Unternehmens erhält und diesen Input direkt dokumentiert. Außerdem könnte ein solches System den Inhalt entsprechend in der Datenschutzerklärung aktualisieren und falls nötig die betroffenen Personen informieren. Eine Verknüpfung der Datenverarbeitungen in Echtzeit würde den Dokumentations- und Pflegeaufwand des Verfahrensverzeichnisses senken und zeitgleich die Transparenz erhöhen. Außerdem wird die Kontrolle erhöht, wodurch das Unternehmen aber auch beispielsweise Vertragspartner oder die zuständige Aufsichtsbehörde vereinfacht prüfen könnten. Jedoch ist noch nicht abzusehen, wann solche

[301] Vgl. LAG Urteil vom 20.12.2018 – 17 Sa 11/18.
[302] Vgl. LG Köln Urteil vom 18.03.2019 – 26 O 25/18.
[303] Vgl. BAG Pressemitteilung Nr. 8/21.
[304] Vgl. CNIL (2021).
[305] Vgl. Chibber (2021).
[306] Vgl. Dr-Datenschutz.de (2021).
[307] Vgl. *Schrulle*, in: Sowa (2020) – S. 23f.
[308] Vgl. Seidel/Seidel, ZD (2020) – S. 110.

„smarten“ Systeme auf den Markt kommen werden. Zwar werben Anbieter bereits mit solchen Systemen, allerdings funktionieren diese noch nicht automatisch. Ein weiteres Problem dabei ist die Verwendung von Programmen und Systemen unterschiedlicher Anbieter in Unternehmen, wodurch Schnittstellen zu Daten zur Verfügung gestellt werden müssten.

5 LITERATURVERZEICHNIS

Albrecht, Jan Philipp; Jotzo, Florian: „Das neue Datenschutzrecht der EU“, 1. Auflage 2017, Baden-Baden: Verlag Nomos (zit.: *Bearbeiter*, in: Albrecht/Jotzo (2017))

Brandt, Verena: „Compliance-Management digitalisieren“, in: Controlling & Management Review Volume 61, issue 4, 2017, S. 78 – 81 (zit.: Brandt (2017)

Braunschweig, Melanie: „DSGVO: Datenschutzmanagementsystem erfolgreich umsetzen“, in: TÜV Nord Webseite, Juli 2020, URL: https://www.tuev-nord.de/de/unternehmen/bildung/wissen-kompakt/datenschutz/datenschutzmanagementsystem/, Abruf 26.04.2021 (zit.: Braunschweig (2020))

Bundesamt für Sicherheit in der Informationstechnik (BSI): „Lerneinheit 9.4: Reifegradmodelle“, in BSI Webseite, o.J., URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_9_Aufrechterhaltung/Lektion_9_04/Lektion_9_04_node.html, Abruf: 30.07.2021 (zit.: BSI (2021) – Reifegradmodelle)

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD): „Das berufliche Leitbild der Datenschutzbeauftragten“, in BvD Webseite, 4. Ausgabe 2018, URL: https://www. bvd-net.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf, Abruf: 09.07.2021 (zit.: Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (2018))

Capgemini Service SAS: „Studie IT-Trends 2019 – Intelligente Technologien“, in Capgemini Webseite, Februar 2019, URL: https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/02/IT-Trends-Studie-2019.pdf, Abruf: 10.05.2021 (zit.: Capgemini (2019))

Capgemini Service SAS: „Studie IT-Trends 2021 – IT ermöglicht Business trotz Kontaktbeschränkungen“, in Capgemini Webseite, Februar 2021, URL: https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2021/02/IT-Trends-Studie-2021.pdf, Abruf: 10.05.2021 (zit.: Capgemini (2021))

CASIS Wirtschaftsprüfung: „Implementierung eines Datenschutz-Management-Systems“, in CASIS Heimann Buchholz Espinoza Partnerschaft Wirtschaftsprüfungsgesellschaft Webseite, September 2020, URL: https://casis-wp.de/implementierung-eines-datenschutz-management-systems/, Abruf: 31.03.2021 (zit.: CASIS Wirtschaftsprüfung (2020))

Chibber, Julina: „Top 5 DSGVO-Bußgelder im Juli 2021“, in Dr-Datenschutz.de Webseite (intersoft consulting services AG), August 2021, URL: https://www.dr-datenschutz.de/top-5-dsgvo-bussgelder-im-juli-2021/, Abruf: 11.08.2021 (zit.: Chibber (2021))

Commission Nationale de l’Informatique et des Libertés (CNIL): „Sanction de 1,75 million d’euros à l’encontre d'AG2R LA MONDIALE“, in CNIL Webseite, Juli 2021, URL:

https://www.cnil.fr/fr/sanction-1-75-million-deuros-ag2r-la-mondiale, Abruf: 12.08.2021 (zit.: CNIL (2021))

Determann, Lothar: „California Privacy Law – Practical Guide and Commentary“, 4. Auflage 2020, International Association of Privacy Professionals (IAPP) (zit.: Determann (2020))

Determann, Lothar: „Kaliforniens erste Datenschutzbehörde – dank Volksentscheid“, in: Zeitschrift für Datenschutz (ZD), 2021, S. 69 – 74 (zit.: Determann, ZD (2021))

Dieners, Peter: „Handbuch Compliance im Gesundheitswesen“, 3. Auflage 2010, München: Verlag C.H. Beck (zit.: *Bearbeiter*, in: Dieners (2010))

Distelzweig, Anja: „Performance Measurement in der Beschaffung“, 2014, Wiesbaden: Springer Gabler. (zit.: Distelzweig (2014))

Duda, Daniela: „Das Verfahrensverzeichnis und die DSGVO – Ohne geht es nicht!“, in: Privacy in Germany (PinG), 2016, S. 248 – 252 (zit.: Duda, PinG (2016))

Dr-Datenschutz.de: „Cookie-Richtlinie der EU direkt in Deutschland anwendbar!“, in Dr-Datenschutz.de Webseite (intersoft consulting services AG), Mai 2012, URL: https://www.dr-datenschutz.de/cookie-richtlinie-der-eu-direkt-in-deutschland-anwendbar/, Abruf: 15.04.2021 (zit.: Dr-Datenschutz (2012))

Dr-Datenschutz.de: „EU-Datenschutzreform: Zwei Schritte vor – ein Schritt zurück“, in: Dr-Datenschutz.de Webseite (intersoft consulting services AG), Oktober 2013, URL: https://www.dr-datenschutz.de/eu-datenschutzreform-zwei-schritte-vor-ein-schritt-zurueck/, Abruf: 15.04.2021 (zit.: Dr-Datenschutz (2013))

Dr-Datenschutz.de: „Begriff und Geschichte des Datenschutzes“, in: Dr-Datenschutz.de Webseite (intersoft consulting services AG), Mai 2014, URL: https://www.dr-datenschutz.de/begriff-und-geschichte-des-datenschutzes/, Abruf: 15.04.2021 (zit.: Dr-Datenschutz (2014))

Dr-Datenschutz.de: „CCPA 2.0 – Das neue kalifornische Datenschutzgesetz“, in Dr-Datenschutz.de Webseite (intersoft consulting services AG), Dezember 2020, URL: https://www.dr-datenschutz.de/ccpa-2-0-das-neue-kalifornische-datenschutzgesetz/, Abruf: 16.04.2021 (zit.: Dr-Datenschutz (2020))

Dr-Datenschutz.de: „BAG entscheidet (nicht) über Recht auf Kopie des E-Mail-Verkehrs“, in Dr-Datenschutz.de Webseite (intersoft consulting services AG), April 2021, URL: https://www.dr-datenschutz.de/bag-entscheidet-nicht-ueber-recht-auf-kopie-des-e-mail-verkehrs/, Abruf: 25.05.2021 (zit.: Dr-Datenschutz (2021))

Ehmann, Eugen; Selmayr, Martin: DS-GVO Datenschutz-Grundverordnung Kommentar, 2. Auflage 2018, München, Verlag C.H. Beck (zit.: *Bearbeiter*, in: Ehmann/Selmayr (2018))

Faust, Sebastian; Spittka, Jan; Wybitul, Tim: “Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz“, in: Zeitschrift für Datenschutz (ZD), 2016, S. 120 – 125 (zit.: Faust/Spittka/Wybitul, ZD (2016))

Fiedler, Martin: „Lean Construction - Das Managementhandbuch”, 1. Auflage 2018, Berlin: Springer Gabler. (zit.: *Bearbeiter*, in: Fiedler (2018))

Figas, Lisa: „CCPA – Das kalifornische Datenschutzgesetz“, in boxcryptor.com Webseite (Secomba GmbH), März 2021, URL: https://www.boxcryptor.com/de/blog/post/ccpa/, Abruf: 16.04.2021 (zit.: Figas (2021))

Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen: „Betrieblicher Datenschutz“, 3. Auflage 2019, München, Verlag C.H. Beck (zit.: *Bearbeiter*, in: Forgó/Helfrich/Schneider (2019))

Gabel, David: „Was ist ein Datenschutz Managementsystem (DSMS)“, in DSGVO-Support.de Webseite, Januar 2019, URL: https://www.dsgvo-support.de/was-ist-ein-dsms/, Abruf: 21.04.2021 (zit.: Gabel (2019))

Gardyan-Eisenlohr, Eva; Knöpfle, Kornel: „Accountability für Datenschutz in einem globalen Unternehmen“, in Datenschutz und Datensicherheit (DuD), 2017, S. 69 – 73 (zit.: Gardyan-Eisenlohr/Knöpfle, DuD (2017))

Georg, Stefan: „Key Performance Indicators Für Junge Unternehmen“, 1. Auflage 2019, Wiesbaden, Verlag Springer Fachmedien Wiesbaden GmbH, S. 5 (zit.: Georg (2019))

Gierschmann, Sybille; Schlender, Katharina; Stentzel, Rainer; Veil, Winfried (Hrsg.): Kommentar Datenschutz-Grundverordnung, 1. Auflage 2018, Köln, Bundesanzeiger Verlag (zit.: *Bearbeiter*, in: Gierschmann/Schlender/Stentzel/Veil (2018))

Gladen, Werner: „Performance Measurement – Controlling mit Kennzahlen“, 6. Auflage 2014, Wiesbaden: Springer Gabler. (zit.: Gladen (2014))

Gola, Peter: „Datenschutz-Grundverordnung“, 2. Auflage 2018, München: Verlag C.H. Beck (zit.: *Bearbeiter*, in: Gola (2015))

Hansch, Guido: „Ein Jahr DS-GVO in der unternehmerischen Praxis: Wie effektiv ist mein Datenschutzmanagement?“, in: Zeitschrift für Datenschutz (ZD), 2019, S. 245 – 247 (zit.: Hansch, ZD (2019))

Hauschka, Christoph E.; Moosmayer, Klaus; Lösler, Thomas: „Corporate Compliance”, 3. Auflage 2016, München, Verlag C.H. Beck (zit.: *Bearbeiter*, in: Hauschka/Moosmayer/Lösler (2016))

Hohmann, Olaf; Pede, Regina: „Key Performance Indicators (KPI): Grundsätze, Gefahren, Möglichkeiten“, Compliance Berater (CB) 2017, S. 416 – 418 (zit.: Hohmann/Pede, CB (2017))

Inderst, Cornelia; Bannenberg, Brita; Poppe, Sina: “Compliance”, 3. Auflage 2017, Heidelberg, Verlag C.F. Müller (zit.: *Bearbeiter*, in: Inderst/Bannenberg/Poppe (2017))

ISiCO-Datenschutz.de: „Kriterien für ein effektives Datenschutzmanagementsystem“, in ISiCO Datenschutz GmbH Webseite, Oktober 2019, URL: https://www.isico-datenschutz.de/blog/kriterien-effektives-dsms/, Abruf: 20.04.2021 (zit.: ISiCO-Datenschutz.de (2019))

Jung, Alexander: „Key Performance Indicators zur Messung der Effizienz eines Datenschutz-Management-Systems“, in Corporate Compliance (CCZ), 2018, S. 224 – 228 (zit.: Jung, CCZ (2018))

Jüttner, Markus: „Die 42 der Compliance – Das Kriterium der Wirksamkeit eines Compliance Management Systems“, in Corporate Compliance (CCZ), 2018, S. 168 – 170 (Jüttner, CCZ (2018))

Kaack, Jörn: „Performance-Measurement für die Unternehmenssicherheit – Entwurf eines Kennzahlen- und Indikatorensystems und die prozessorientierte Implementierung“, 2012, Wiesbaden: Springer Gabler. (zit.: Kaack (2012))

Kelso, J. Clark: „California's Constitutional Right to Privacy“, in: Pepperdine Law Review Volume 19 Issue 2, 1992, S. 328, URL: https://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1631&context=plr, Abruf: 21.04.2021 (zit.: Kelso (1992)

Kleindienst, Bernd: „Performance Measurement und Management“, 1. Auflage 2017, Wiesbaden, Verlag Springer Fachmedien Wiesbaden GmbH, (zit.: Kleindienst (2017))

Kleinfeld, Anette; Martens, Annika (Hrsg.): „CSR und Compliance“, 1. Auflage 2018, Berlin: Springer Gabler. (zit.: *Bearbeiter*, in: Kleinfeld/Martens (2018))

Kleinz, Torsten: „USA: Gesetzentwurf soll Datenexport begrenzen – Sorge in Irland“, in Heise Webseite, April 2021, URL: https://www.heise.de/news/USA-Gesetzentwurf-soll-Datenexport-begrenzen-Sorge-in-Irland-6018071.html, Abruf: 20.04.2021 (zit.: Kleinz (2021))

Knoll, Matthias; Strahringer, Susanne (Hrsg.): „IT-GRC-Management – Governance, Risk und Compliance”, 1. Auflage 2017, Wiesbaden, Verlag Springer Vieweg (zit.: *Bearbeiter*, in: Knoll/Strahringer (2017))

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i.V.m. DIN EN ISO/IEC 17065“, in Datenschutzkonferenz Webseite, August 2018, URL: https://www.datenschutzkonferenz-online.de/media/ah/20180828_ah_DIN17065-Ergaenzungen-full-V10-final_V3_DSK.pdf, Abruf: 05.05.2021 (zit.: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018a))

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: „Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist“, in LfD Niedersachsen Webseite, Oktober 2018, URL: https://lfd.niedersachsen.de/download/134415/DSFA_Muss-Liste_fuer_den_nicht-oeffentlichen_Bereich.pdf, Abruf: 21.05.2021 (zit.: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018b))

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: „Kurzpapier Nr. 5 – Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“, in Datenschutzkonferenz Webseite, Dezember 2018, URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf, Abruf: 21.05.2021 (zit.: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018c))

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: „Kurzpapier Nr. 12 – Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“, in Datenschutzkonferenz Webseite, Dezember 2018, URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf, Abruf: 15.06.2021 (zit.: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018d))

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: „Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen“, in Datenschutzkonferenz Webseite, Oktober 2019, URL: https://www.datenschutzkonferenz-online.de/media/ah/_20191016_bu%C3%9Fgeldkonzept.pdf, Abruf: 04.05.2021 (zit.: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2019))

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: „Das Standard-Datenschutzmodell – Version 2.0b“, in Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern Webseite, April 2020, URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-

Methode_V20b.pdf, Abruf: 31.05.2021 (zit.: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2020))

Koreng, Ansgar; Lachenmann, Matthias: „Formularhandbuch Datenschutzrecht“, 2. Auflage 2018, München: Verlag C.H. Beck (zit.: *Bearbeiter*, in: Koreng/Lachenmann (2018))

Korge, Tobias: „Aufbau von Datenschutz-Management-Systemen nach der DS-GVO“, 2020, Köln: Reguvis Fachmedien GmbH (zit.: Korge (2020))

Koyuncu, Adem: „Healthcare Compliance 2015“, in: Pharma Recht (PharmaR), 2015, S. 583 – 589 (zit.: Koyuncu (2015))

Kranig, Thomas; Sachs, Andreas; Gierschmann, Markus: “Datenschutz-Compliance nach der DS-GVO”, 1. Auflage 2017, Köln: Reguvis Bundesanzeiger Verlag (zit.: *Bearbeiter*, in: Kranig/Sachs/Gierschmann (2017))

Kranig, Thomas; Sachs, Andreas; Gierschmann, Markus: “Datenschutz-Compliance nach der DS-GVO”, 2. Auflage 2019, Köln: Reguvis Bundesanzeiger Verlag (zit. Kranig/Sachs/Gierschmann (2019))

Kühling, Jürgen; Buchner, Benedikt: “Datenschutz-Grundverordnung Bundesdatenschutzgesetz“, 3. Auflage 2020, München: Verlag C.H. Beck (zit.: *Bearbeiter*, in: Kühling/Buchner (2020))

Künzel, Hansjörg (Hrsg.): “Erfolgsfaktor Performance Management”, 1. Auflage 2016, Berlin Heidelberg: Springer Gabler. (zit.: *Bearbeiter*, in: Künzel (2016))

Lambertz, Peer: „DSGVO: Aufgaben im PDCA-Zyklus organisieren“, in Datenschutz-Praxis.de Webseite (WEKA MEDIA GmbH & Co. KG), Januar 2017, URL: https://www.datenschutz-praxis.de/datenschutzbeauftragte/dsgvo-aufgaben-im-pdca-zyklus-organisieren/, Abruf: 11.04.2021 (zit.: Lambertz (2017)).

Lambertz, Peer: „DSGVO: Anforderungen an ein Datenschutz-Management-System“, in Datenschutz-Praxis.de Webseite (WEKA MEDIA GmbH & Co. KG), November 2019, URL: https://www.datenschutz-praxis.de/datenschutzbeauftragte/dsgvo-anforderungen-datenschutz-management-system/, Abruf: 22.04.2021 (zit.: Lambertz (2019))

Landesbeauftragte für den Datenschutz Niedersachsen: „Kriterienkatalog zur Querschnittsprüfung in der Wirtschaft“, in LfD Niedersachsen Webseite, August 2019, URL: https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/kriterien-querschnittspruefung-179455.html, (zit.: LfD Niedersachsen (2019))

Loomans, Dirk; Matz, Manuela; Wiedemann, Michael: „Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems“ 2014, Wiesbaden: Springer Vieweg (zit.: Loomans/Matz/Wiedemann (2014))

Meyer, Eric; Struck, Matthias; Bitsch, Aljona: “Datenschutzmanagement & Audits - Stärkung der Eigenkontrolle und des Datenschutzmanagements“, in: EY Law – Lexology Webseite, Februar 2020, URL: https://www.lexology.com/library/detail.aspx?g=f666bc2a-a18a-4a93-b840-51120c6dcbc4, Abruf: 17.05.2021 (zit.: Meyer/Struck/Bitsch (2020))

Moos, Flemming; Schefzig, Jens; Arning, Marian: „Die neue Datenschutz-Grundverordnung“, 1. Auflage 2018, Berlin: Verlag De Gruyter (zit.: *Bearbeiter*, in: Moos/Schefzig/Arning (2018))

Öztürk, Ebru: „Türkische Datenschutzaufsichtsbehörde verlängert die Registrierungspflicht in VERBIS für Verantwortliche bis zum 31.12.2019“, in Datenschutz-Notizen.de Webseite (DSN

Holding GmbH), September 2019, URL: https://www.datenschutz-notizen.de/tuerkische-datenschutzaufsichtsbehoerde-verlaengert-die-registrierungspflicht-in-verbis-fuer-verantwortliche-bis-zum-31-12-2019-5023342/, Abruf: 16.04.2021 (zit.: Öztürk (2019))

Paal, Boris P.; Pauly, Daniel A.: Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Auflage 2021, München, Verlag C.H. Beck (zit.: *Bearbeiter*, in: Paal/Pauly (2021))

Pape, Jonas: „Zur Wirksamkeit von Corporate Compliance“, in Corporate Compliance (CCZ), 2009, S. 233 – 236 (zit.: Pape, CCZ (2009))

Rieß, Joachim: „Innovationen der DSGVO in der Praxis“, in Datenschutz und Datensicherheit (DuD), 2019, S. 498 – 501 (zit.: Rieß, DuD (2019))

Rödl & Partner: “Datenschutz in Brasilien – dringender Handlungsbedarf für alle Gesellschaften in Brasilien”, in Rödl & Partner GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft Webseite, April 2019, URL: https://www.roedl.de/themen/datenschutz-brasilien-lgpd-dsgvo-handlungsbedarf, Abruf: 16.04.2021 (zit.: Rödl & Partner (2019))

Sächsisches Staatsministerium des Inneren: „Einführung eines Datenschutzmanagement-Systems“, in Sachsen.de Webseite, o.J., URL: https://www.datenschutzrecht.sachsen.de/einfuehrung-eines-datenschutzmanagement-systems-4235.html, Abruf 05.05.2021 (zit.: Sächsisches Staatsministerium des Inneren (2021))

Scheben, Barbara: „Datenschutz als Managementaufgabe“, in KPMG AG Wirtschaftsprüfungsgesellschaft Webseite, Februar 2019, URL: https://klardenker.kpmg.de/datenschutz-als-managementaufgabe/, Abruf: 28.05.2021 (zit.: Scheben (2019))

Scheben, Barbara: “Das kalifornische Datenschutzrecht wird verschärft”, in KPMG AG Wirtschaftsprüfungsgesellschaft Webseite, März 2021, URL: https://home.kpmg/de/de/ home/insights/2021/03/das-kalifornische-datenschutzrecht.html, Abruf: 16.04.2021 (zit.: Scheben (2021))

Schewior, Christopher: „Irland und die Big Player – Neues Gesetz in den USA?“, in Dr-Datenschutz.de Webseite (intersoft consulting services AG), April 2021, URL: https://www.dr-datenschutz.de/irland-und-die-big-player-neues-gesetz-in-den-usa/, Abruf: 04.05.2021 (zit.: Schewior (2021))

Schimansky, Herbert; Bunte, Hermann-Josef; Lwowski, Hans Jürgen: „Bankrechts-Handbuch“, 5. Auflage 2017, München: Verlag C.H. Beck (zit.: *Bearbeiter*, in: Schimansky/Bunte/Lwowski (2017))

Schläger, Uwe; Thode, Jan-Christoph: „Handbuch Datenschutz und IT-Sicherheit“, 1. Auflage 2018, Berlin: Erich Schmidt Verlag GmbH & Co. KG (zit.: *Bearbeiter*, in: Schläger/Thode (2018))

Schneider, Thomas: „Wirkungsvolle Compliance“, 2018, Berlin: Springer Gabler. (zit. Schneider (2018))

Schreyer, Maximilian: „Entwicklung und Implementierung von Performance Measurement Systemen“, 2007, Wiesbaden: Deutscher Universitäts-Verlag. (zit.: Schreyer (2007))

Schrulle, Jan: „Aufbau und Prüfung der Datenschutzorganisation - der IDW PH 9.860.1 als geeignetes Rahmenwerk“, in: IT-Governance Fachzeitschrift des ISACA Germany Chapter e.V. (IT-Governance), Heft 29, 2019, S. 25 – 28 (zit.: Schrulle, IT-Governance (2019))

Schwartmann, Rolf; Jaspers, Andreas; Thüsing, Gregor; Kugelmann, Dieter: Heidelberger Kommentar „Datenschutz-Grundverordnung“, 1. Auflage 2018, Heidelberg, Verlag C.F. Müller (zit.: *Bearbeiter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann (2018))

Seidel, Hendrik; Seidel, Ulrich: „50 Jahre Datenschutz - wie geht es weiter?“, in: Zeitschrift für Datenschutz (ZD), 2020, S. 609 – 610 (zit.: Seidel/Seidel, ZD (2020))

Seidel, Ulrich: „Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten“, in: Neue Juristische Wochenschrift (NJW), 1970, S. 1581 – 1583 (zit.: Seidel, NJW (1970))

Sowa, Aleksandra: „Management der Informationssicherheit“, 1. Auflage 2017, Wiesbaden: Verlag Springer Fachmedien Wiesbaden GmbH (zit.: Sowa (2017))

Sowa, Aleksandra: „IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit“, 1. Auflage 2020, Wiesbaden: Verlag Springer Fachmedien Wiesbaden GmbH (zit.: *Bearbeiter*, in: Sowa (2020))

SüdWest Datenschutz: „Gegenüberstellung türkisches Datenschutzrecht zur Datenschutzgrundverordnung (DSGVO)“, in SüdWest Datenschutz Rechtsanwaltsgesellschaft mbH Webseite, Juni 2018, URL: https://www.suedwest-datenschutz.com/gegenueberstellung-tuerkisches-datenschutzrecht-zur-datenschutzgrundverordnung-dsgvo/, Abruf: 16.04.2021 (zit.: SüdWest Datenschutz (2018))

Taeger, Jürgen; Gabel, Detlev: „DSGVO - BDSG“ Kommentar, 3. Auflage 2019, Frankfurt am Main, Verlag Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft (zit.: *Bearbeiter*, in: Taeger/Gabel (2019))

Tracy, Brian: „Ziele“, 2. Auflage 2018, Frankfurt/New York: Campus Verlag GmbH (zit.: Tracy (2018))

Veil, Winfried: „21 Thesen zum Irrweg der DS-GVO“, in: CR-online, Mai 2018, URL: https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/, Abruf: 26.03.2021 (zit.: Veil, CR-online (2018))

Veil, Winfried: „Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO?“, in: Zeitschrift für Datenschutz (ZD), 2018, S. 9 – 16 (zit.: Veil, ZD (2018))

Von Schenck, Sophie; Tilman Mueller-Stöfen: „Die Datenschutz – Grundverordnung: Auswirkungen in der Praxis“, in Gesellschaftsrecht- und Wirtschaftsrecht (GWR), 2017, S. 171 – 179 (zit.: Von Schenck/Mueller-Stöfen, GWR (2017))

Wermelt, Andreas; Fechte, Tim: „Datenschutz-Compliance - praktische Unterstützung bei der Umsetzung durch den IDW PS 980“, Betriebsberater (BB) 2013, S. 811 (zit.: Wermelt/Fechte, BB (2013))

Wichtermann, Marco: „Einführung eines Datenschutz-Management-Systems im Unternehmen – Pflicht oder Kür?“, in Zeitschrift für Datenschutz (ZD), 2016, S. 421 – 422 (zit.: Wichtermann ZD (2016))

Wybitul, Tim: „EU-Datenschutz-Grundverordnung im Unternehmen“, 1. Auflage 2016, Frankfurt am Main, Verlag Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft (zit.: *Bearbeiter*, in: Wybitul (2016))

6 AUTORENINFORMATION

Manuel Kling LL. M. ist Absolvent des Masterstudienganges „Legal Management“ an der Hochschule Konstanz (HTWG).

Dr. Thomas Zerres ist Professor für Zivil- und Wirtschaftsrecht an der Hochschule Konstanz. Vor seinem Ruf an die Hochschule Konstanz lehrte Prof. Dr. Thomas Zerres 15 Jahre an der Hochschule Erfurt, nachdem er mehrere Jahre als Rechtsanwalt und als Bundesgeschäftsführer eines großen Wirtschaftsverbandes der Dienstleistungsbranche tätig war. Seine Lehr- und Forschungsschwerpunkte sind das Marketingrecht sowie das Europäische Privatrecht.

Dr. Christopher Zerres ist Professor für Marketing an der Hochschule Offenburg. Seine Schwerpunkte in Lehre und Forschung sind das Online-Marketing und das Marketing-Controlling. Christopher Zerres ist Autor zahlreicher Publikationen zu den Bereichen Management und Marketing.