HOCHSCHULE FURTWANGEN UNIVERSITY | HFU

Betrachtung der technischen und organisatorischen Maßnahmen in der Datenschutz-Grundverordnung – Neue Anforderungen für Unternehmen?

Bachelor Thesis „Security & Safety Engineering (B.Sc.)"

SSB7 SS 2016

Erstellt von:

Müller, Hendrik 242777 Am Großhausberg 4 78120 Furtwangen

Abgabetermin:
Furtwangen, 30.06.2016

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe. Ich bin damit einverstanden, dass die Arbeit durch Dritte eingesehen und unter Wahrung urheberrechtlicher Grundsätze zitiert werden darf.

Furtwangen, 29.06.2016 _____

Ort, Datum

Hendrik Müller

Student

Lizenz/ Freigabe der Arbeit

Ich bin damit einverstanden, dass die vorliegende Arbeit unter der Lizenz Creative Commons Namensnennung 4.0 International (CC BY 4.0) steht. Dies ermöglicht das Teilen und Bearbeiten dieser Arbeit, sofern Urheber und Titel der Arbeit, sowie Rechteangaben und Änderungen kenntlich gemacht werden. Der vollständige Lizenztext befindet sich unter: https://creativecommons.org/licenses/by/4.0/legalcodeLizenzen

Furtwangen, 29.06.2016 _____

Ort, Datum

Hendrik Müller

Student

Kurzfassung

Durch die Novellierung des europäischen Datenschutzrechts werden sich Änderungen in der nationalen Datenschutz-Gesetzgebung in Deutschland ergeben. Die im Mai 2016 erlassene Datenschutz-Grundverordnung wird die bisher gültige europäische Datenschutz-Richtlinie im Jahr 2018 ablösen. Damit wird auch das Bundesdatenschutzgesetz – das auf der europäischen Richtlinie basiert – abgelöst.

Durch die Novellierung sind auch die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten betroffen. Im Folgenden sollen die neuen technischen und organisatorischen Maßnahmen betrachtet und mit bestehenden Anforderungen des Bundesdatenschutzgesetzes verglichen werden. Ziel ist es herauszufinden, was sich für Unternehmen in Bezug auf die technischen und organisatorischen Maßnahmen ändern wird oder inwiefern bestehende Maßnahmen weiterhin ausreichend sein werden.

Dabei wurde festgestellt, dass die neuen Anforderungen generischer sind und sich nur bedingt mit bestehenden Anforderungen vergleichen lassen. Stattdessen werden neue Prinzipien vorgestellt, die ein unterschiedliches Vorgehen voraussetzen.

Abstract

The revision of the European data protection law will have consequences for the national data protection legislation in Germany. The new General Data Protection Regulation, legislated in May 2016, will supersede the so far applicable European Data Protection Directive in 2018. Thereby it will also supersede the “federal data protection law” (dt.: “Bundesdatenschutzgesetz”), which is based off the European Directive.

This revision will also affect the technical and organizational measures that are to be taken to protect personal data. The following paper shall take a look at the new technical and organizational measures and compare them to existing standards as found in the “federal data protection law” (dt.: “Bundesdatenschutzgesetz”). The intention is to isolate possible changes businesses will have to accommodate to in regards to the technical and organizational measures or to what extend existing measures can be adopted.

It was found, that the new requirements are more generic and can only partly be compared to existing requirements. Instead, new principles were introduced, that require a different approach.

INHALTSVERZEICHNIS

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EU	Europäische Union
KMU	kleinere und mittelständische Unternehmen
PbD	Privacy by Design
PET	Privacy Enhancing Technologies
TO-Maßnahmen	Technische und organisatorische Maßnahmen

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Am 4. Mai 2016 wurde von der Europäischen Union (EU) die Verordnung 2016/679 – auch unter dem Namen Datenschutz-Grundverordnung (DSGVO) bekannt – veröffentlicht. Damit endete ein ca. vier Jahre langer Gesetzgebungsprozess. Ziel der EU war es, die sehr unterschiedliche Auslegung der bisherigen Regelung zum Datenschutz in der EU zu vereinheitlichen und an neue Gegebenheiten anzupassen (Verordnung (EU) 2016/679 [DSGVO]). Mit ihrer Veröffentlichung im Amtsblatt am 4. Mai 2016 ist der Prozess nun abgeschlossen und die Verordnung wird (nach einer 2 jährigen Übergangsfrist) zum 25. Mai 2018 gültig sein (DSGVO, 2016). Damit verliert gleichzeitig das Bundesdatenschutzgesetz (BDSG) an Wirkung und wird von der DSGVO abgelöst. Dies bringt eine Reihe von Änderungen mit sich. Unter anderem werden durch die DSGVO die bisherigen Regelungen und Anforderungen an technische und organisatorische Maßnahmen (TO-Maßnahmen) durch die Regelungen in der DSGVO abgelöst.

In der folgenden Ausarbeitung sollen die neuen Anforderungen an TO-Maßnahmen gemäß der neuen Rechtsgrundlage genauer betrachtet und mit den bisherigen TO-Maßnahmen des BDSG verglichen werden. Ziel ist es festzustellen, inwiefern sich die Anforderungen von den bisherigen TO-Maßnahmen unterscheiden und was zukünftig zum Schutz personenbezogener Daten, vor allem auf Seiten von Unternehmen, beachtet werden muss. Dabei werden TO-Maßnahmen gemäß DSGVO wie folgt beschrieben:

> *„Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. […] Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern.“ (Erwägungsgrund 78, DSGVO)*

Im Folgenden sollen die Begriffe „Daten“ und „personenbezogene Daten“ als Synonyme verwendet werden. Da das Spektrum auf der DSGVO und auf deren Bezugsbereich beschränkt ist, werden mit den beiden Begrifflichkeiten die nach DSGVO verstandene Art von personenbezogenen Daten beschrieben. Ähnlich soll mit den Begriffen Datenschutz und

Datensicherheit bzw. den englischen Begriffen „privacy“ und „data protection“ verfahren werden. Sowohl unter Datenschutz als auch unter Datensicherheit soll dabei der Schutz personenbezogener Daten gemäß DSGVO sowohl auf technischer, als auch auf organisatorischer und rechtlicher Ebene verstanden werden. Darunter sollen ebenfalls der Schutz des Menschen an sich und dessen Rechte und Freiheiten, sowie der Schutz von demokratischen Werten fallen (Danezis, Domingo-Ferrer, Hansen, Hoepman, Le Métayer, Tirtea & Schiffner, 2014).

Die Arbeit wird sich zunächst an den bisherigen TO-Maßnahmen des BDSG orientieren, wobei diese mit den neuen Anforderungen an TO-Maßnahmen gemäß DSGVO verglichen werden. Ausgehend der Erkenntnisse werden die neuen Anforderungen untersucht und genauer betrachtet. Entsprechend wird sich der Aufbau der Arbeit gestalten. Ausgehend des Vergleichs werden zusätzliche Anforderungen und Prinzipien, die sich an die TO-Maßnahmen richten isoliert und Methoden angeschaut, wie sich diese neuen Anforderungen in der Praxis umsetzen lassen. Dabei spiegelt die Reihenfolge der Betrachtung der verschiedenen Anforderungen nicht die Reihenfolge, die zur Umsetzung der Maßnahmen in der Praxis geeignet und empfohlen ist, wider.

Beispielunternehmen – Rahmenbedingungen

Zum besseren Verständnis, wie die neuen Anforderungen umgesetzt werden können und welche Konsequenzen diese mit sich führen, werden am Ende eines jeden Kapitels die neuen Erkenntnisse auf ein Beispielunternehmen übertragen. Dieses Beispielunternehmen soll im Folgenden kurz vorgestellt und im Hinblick auf die datenverarbeitungsrelevanten Eigenschaften hin definiert werden. An dieser Stelle sei auch noch einmal erwähnt, dass sich die Betrachtung ausschließlich auf die TO-Maßnahmen bezieht. Sämtliche andere Anforderungen und Regelungen der DSGVO, unter die das Beispielunternehmen fällt, werden nur in Ausnahmefällen betrachtet.

Das Beispiel soll sich an einer größeren Arztpraxis orientieren. Hierzu wird angenommen, dass die Arztpraxis in einer größeren Stadt betrieben wird und einen Zusammenschluss mehrerer Ärzte darstellt. Die Praxis soll insgesamt vier Ärzte, acht Arzthelfer und mehrere Räumlichkeiten, inklusive speziellem medizinischen Gerät, umfassen. Im Rahmen der Tätigkeit werden sowohl personenbezogene Daten, als auch Gesundheitsdaten (gemäß Definition nach Art. 4, DSGVO) verarbeitet. Derartige personenbezogene Daten gehören gemäß Art. 9 DSGVO zu den besonderen Kategorien personenbezogener Daten.

Grundsätzlich ist die Verarbeitung solcher Daten gemäß Art. 9 DSGVO untersagt. Aufgrund der Ausnahme unter Art. 9 Abs. 2 lit. h und Art. 9 Abs. 3 DSGVO ist die Verarbeitung zu Zwecken der Gesundheitsvorsorge jedoch zulässig. Für die Verarbeitung der Daten betreibt der Verantwortliche (in diesem Fall der Chefarzt) verschiedene EDV-Anlagen, inklusive mehrerer Computer, Druckern und zentralen Servern. Alle Anlagen und Systeme sind dabei in der Praxis selbst untergebracht und nicht an Dienstleister ausgelagert. Die Pflege der Systeme wird jedoch von einem extern bestellten Administrator bzw. Techniker durchgeführt. Aufgrund der Verarbeitung von Gesundheitsdaten ist die Benennung eines Datenschutzbeauftragten erforderlich (Art. 37 Abs. 1 lit. c DSGVO). Dieser wurde extern bestellt und ist kein Mitarbeiter der Praxis. Die Daten werden vor Ort gesammelt, gespeichert, verarbeitet und ggf. weitergeleitet. Dies geschieht teilweise über den Postweg, teilweise aber auch über den elektronischen E-Mail Verkehr. Adressaten sind dabei ausschließlich andere Arztpraxen, der Betroffene selbst und Versicherungsunternehmen. Für letztere werden auch Statistiken erhoben und an diese weitergeleitet. Zusätzlich betreibt die Praxis noch einen Online-Dienst. In einem Chatroom können Patienten mit Ärzten in Kontakt treten um Beschwerden oder Symptome anzusprechen und sich Rat einzuholen.

Anmerkung: Das Beispiel Arztpraxis scheint insofern passend, als dass so gut wie jede Person hiervon betroffen ist und sich entsprechend leicht in die Lage des Betroffenen hineinversetzen kann. Zusätzlich bietet die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO eine gute Grundlage, um aufzuzeigen, wie mit der Verarbeitung von Daten verfahren werden sollte, die ein hohes Risiko für den Betroffenen darstellen. Gemäß Erwägungsgrund 53 DSGVO sollte „[d]en Mitgliedstaaten […] gestattet werden, weitere Bedingungen — einschließlich Beschränkungen — in Bezug auf die Verarbeitung von […] Gesundheitsdaten beizubehalten oder einzuführen“. Aufgrund dessen könnten weitere nationale Regelungen im Umgang mit Gesundheitsdaten wirksam werden bzw. wirksam sein. Diese Regelungen könnten bereits vorhanden sein oder im Laufe der Umsetzungsfrist der DSGVO erlassen werden. Entsprechend könnten sich die Ergebnisse, bezogen auf dieses Beispiel, in Zukunft ändern. Da dem Verfasser zum Zeitpunkt der Bearbeitung keine bestehenden nationalen Regelungen bekannt sind, die sich auf die TO-Maßnahmen von Gesundheitsdaten erstrecken, soll auf Grundlage der in der DSGVO zu findenden TO-Maßnahmen verfahren werden. Es sollte allerdings beachtet werden, dass sich diese Verfahren, wie erwähnt, zukünftig durch zusätzliche Regelungen ändern könnten.

2 Grundlagen

Im Vorfeld der genaueren Auseinandersetzung mit den TO-Maßnahmen der neuen DSGVO sollen zunächst die Grundlagen der europäischen Gesetzgebung, sowie die Geschichte des bisher gültigen BDSG vorgestellt werden.

2.1 EU-Gesetzgebung

Die EU-Gesetzgebung lässt sich in zwei unterschiedliche Gesetzgebungsverfahren aufteilen. Zum einen gibt es die Verordnungen und zum anderen die Richtlinien (*siehe Abbildung 1*). Beschlüsse, Stellungnahmen und Empfehlungen können ebenfalls von der EU verabschiedet werden. Interessant mit Blick auf die Datenschutzgesetzgebung sind allerdings vor allem die Erstgenannten. Zudem stellen vor allem Stellungnahmen und Empfehlungen keine Verbindlichkeiten an die Mitgliedstaaten (Art. 288, Vertrag über die Arbeitsweise der Europäischen Union [AEUV], 2012).

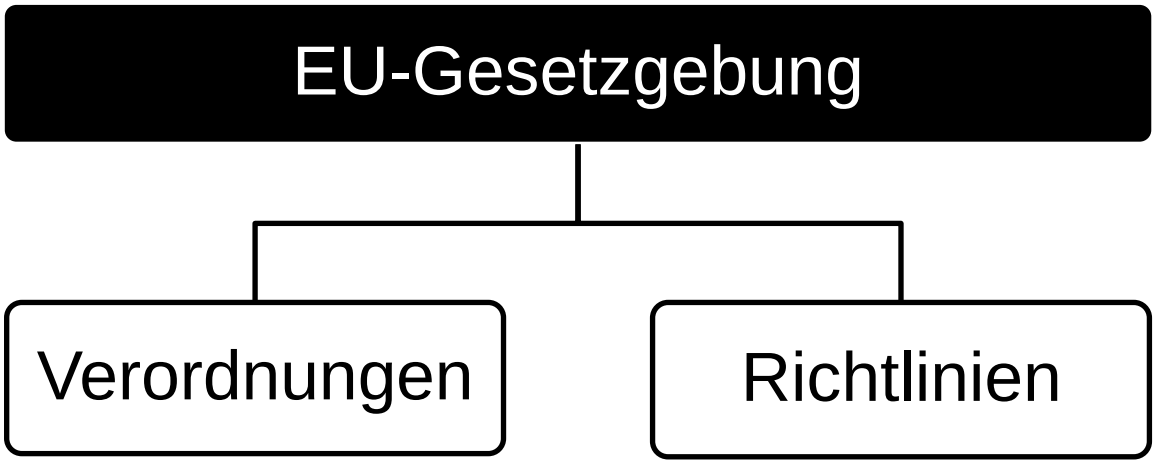

Abbildung 1: EU-Gesetzgebung skizziert (eigene Darstellung, 2016).

Die relevanten Gesetzgebungsverfahren sollen im Folgenden kurz vorgestellt werden, wobei es nicht darum geht das Verfahren an sich zu beschreiben, sondern vor allem sollen die Eigenschaften der verschiedenen Verfahren und Konsequenzen genannt werden.

2.1.1 EU-Richtlinien

Gemäß Art. 288 des Vertrags über die Arbeitsweise der Europäischen Union (2012) sind Richtlinien „[…] für jeden Mitgliedstaat, an den sie gerichtet [werden], hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der

Form und der Mittel.“ Es obliegt somit den Mitgliedstaaten selbst zu entscheiden, wie und in welcher Form die Richtlinie umgesetzt wird. Das hat zur Folge, dass die letztendliche Umsetzung der Richtlinie in den einzelnen Mitgliedstaaten sehr unterschiedlich aussehen kann. Entsprechend ist eine einheitliche Umsetzung nicht gewährleistet. In der Praxis kam es immer wieder zu sehr starken Abweichungen bei der Umsetzung von Richtlinien zwischen den Mitgliedstaaten[1].

Zwar kann es aufgrund einer Richtlinie zu verschiedenen Auslegungen des Rechts in den Mitgliedstaaten kommen, dafür erlaubt es die Richtlinie, dass jeder Mitgliedstaat für sich entscheiden kann, wie das Recht in bestehendes nationales Recht umgesetzt werden soll und ob eventuelle Verschärfungen angebracht sind bzw. gewollt sind. Somit bleibt dem Mitgliedstaat eine gewisse Souveränität erhalten.

Das BDSG basiert auf solch einer von der EU erlassenen Richtlinie (Richtlinie 95/46/EG, 1995). Bisher gab es entsprechend mehr oder weniger starke Auslegungen des Datenschutzes in den Mitgliedstaaten der EU, was zur Folge hatte, dass sich Anforderungen an den Datenschutz von Mitgliedstaat zu Mitgliedstaat teils sehr stark unterscheidet hatten. Um solch einem Effekt entgegen zu wirken gibt es, wie bereits angesprochen, noch eine weitere Form der EU-Gesetzgebung; nämlich die Verordnung.

2.1.2 EU-Verordnungen

Im Gegensatz zur EU-Richtlinie hat die EU-Verordnung einen stärkeren Bindungscharakter. Eine Verordnung ist nach in Kraft treten sofort und für alle Mitgliedstaaten bindend. Es bedarf keiner Anpassung oder Umsetzung durch die Mitgliedstaaten (Art. 288, AEUV, 2012).

So kann im Vergleich zur Richtlinie eine einheitliche Umsetzung einer Norm gewährleistet werden. Allerdings bedeutet das auch, dass den Mitgliedstaaten kein Spielraum geboten wird, um die Norm anzupassen oder abzuändern. Die EU-Verordnung muss entsprechend übernommen werden, auch wenn dadurch bestehende, strengere nationale Gesetze oder Normen verloren gehen.

Durch die DSGVO wird nun aus einer Richtlinie eine Verordnung. Konkret bedeutet das, dass es in Zukunft einen einheitlichen Datenschutz in der EU geben wird, der in jedem Mitgliedstaat den gleichen Anforderungen unterliegt. Es wird also zukünftig keine zahlreichen unterschiedlichen Auslegungen mehr geben.

[1] Vgl. beispielsweise die Umsetzung der Richtlinie 95/46/EG (DSGVO, 2016).

2.2 Geschichte des BDSG

Wie bereits erwähnt, basiert das BDSG auf Grundlage einer EU-Richtlinie. Doch bereits zuvor gab es in Deutschland eine nationale Gesetzgebung, die sich mit dem Datenschutz befasste. Ausgehend von Diskussionen in den Vereinigten Staaten von Amerika wurde auch in Deutschland das Thema Datenschutz diskutiert. Ende der 1960er Jahre wurde letztendlich der eigentliche Begriff des Datenschutzes geprägt und kurze Zeit später, 1970 verabschiedete Hessen das erste Landesdatenschutzgesetz. Sieben Jahre später, 1977 wurde dann auch das erste Bundesdatenschutzgesetz verabschiedet. Erst 1981 hatten alle Bundesländer auch ein Landesdatenschutzgesetz erlassen (BfDI Datenschutz WIKI, ohne Datum).

Zentrales Ereignis der nationalen Gesetzgebung war auch das 1983 erlassene Volkszählungsurteil. Unter dem Begriff der informationellen Selbstbestimmung wurde das Grundrecht zugesprochen, dass jede Person selbst entscheiden können soll, was mit Ihren persönlichen Daten geschieht. Dieses Grundrecht wirkte sich direkt auf die Gesetzgebung auf Landes-, Bundes- und auch auf EU-Ebene aus. So wurde eine Ableitung des Grundrechts auf informationelle Selbstbestimmung auch durch die europäische Menschenrechtskonvention gesehen (BfDI Datenschutz WIKI, ohne Datum). Entsprechend prägte dieses Recht auch die im Jahre 1995 verabschiedete Europäische Datenschutzrichtlinie 1995/46/EG (Richtlinie 95/46/EG, 1995). Aufgrund ihres Rechtscharakters als EU-Richtlinie musste die europäische Regelung in nationales Gesetz übernommen und umgesetzt werden. Dies geschah im Jahre 2001 im Rahmen einer Novellierung des bereits bestehenden Bundesdatenschutzgesetzes. Es folgten in den späteren Jahren noch weitere Novellierungen (BfDI Datenschutz WIKI, ohne Datum).

Die Umsetzung der Europäischen Datenschutzrichtlinie in den einzelnen Mitgliedstaaten führte zu einer sehr unterschiedlichen Auslegung des Datenschutzes. Da viele Mitgliedstaaten unterschiedliche Regelungen erließen wurde der Wunsch nach einem harmonisierten Datenschutz in der EU immer größer. Letztendlich wurde 2016 die DSGVO erlassen, die mit ihrem Rechtscharakter als EU-Verordnung eine Harmonisierung des Datenschutzrechts erreichen soll (DSGVO, 2016).

3 Vergleich der TO-Maßnahmen nach der neuen DSGVO (Art. 32) und dem BDSG (§ 9 und Anlage zu § 9 Satz 1)

Anhand eines Vergleiches der TO-Maßnahmen der DSGVO und des BDSG soll zunächst identifiziert werden, ob sich durch die neue EU-Verordnung Veränderungen ergeben, oder ob die bisherigen Regelungen bereits ausreichen. Das Spektrum des Vergleiches beschränkt sich dabei auf den Art. 32 der DSGVO und den § 9 des BDSG (zzgl. Anlage zu § 9, Satz 1) und gemäß der Thematik dieser Ausarbeitung werden ausschließlich die technischen und organisatorischen Maßnahmen betrachtet.

3.1 Methodik

Vorab sollen zunächst die Rahmenbedingungen des Vergleiches dargelegt werden. Wie einleitend bereits beschrieben, wird sich der Vergleich auf die einschlägigen Artikel bzw. Paragraphen der jeweiligen Rechtsvorschrift beschränken. Im Falle der DSGVO handelt es sich hierbei um den Art. 32 („Sicherheit der Verarbeitung“), im Falle des BDSG um den § 9 („Technische und organisatorische Maßnahmen“) inklusive der dazugehörigen Anlage. Für den Vergleich soll auf Grundlage einer teleologischen Auslegung der beiden Rechtsvorschriften die Inhalte auf deren Bedeutung bzw. sinngemäße Aussage hin betrachtet und an geeigneten Stellen Parallelen gezogen werden. Dabei ist die Intention nicht nach einer 1:1 Übereinstimmung der Inhalte zu suchen, sondern auch diejenigen Punkte miteinander zu vergleichen, die auf den ersten Blick eventuell nicht vergleichbar erscheinen, aufgrund ihrer sinngemäßen inhaltlichen Aussage jedoch diese Betrachtung zulassen.

Die Ergebnisse des Vergleiches werden in drei Teile gegliedert. Zunächst sollen alle TO-Maßnahmen des BDSG identifiziert werden, die in der neuen DSGVO nicht mehr erwähnt werden und somit nicht mehr Bestandteil der neuen TO-Maßnahmen sind. Anschließend sollen vergleichbare TO-Maßnahmen des BDSG und der DSGVO gegenübergestellt werden und etwas näher betrachtet werden. Dabei soll der Fokus auf möglicherweise abweichenden Formulierungen bzw. Änderungen liegen, die Auswirkungen auf die Umsetzung der entsprechenden TO-Maßnahme haben können. Zuletzt sollen die neu hinzugefügten TO-Maßnahmen genannt werden, die es in der bisherigen Rechtsvorschrift nicht gab und demnach als neue, zusätzliche TO-Maßnahmen gesehen werden können.

3.2 Ergebnisse

Zur besseren Übersicht werden die Ergebnisse in tabellarischer Form dargestellt, wobei die Tabelle wie in *Abschnitt 3.1* beschrieben aufgeteilt wird. Jedem Strukturpunkt soll dabei ein Unterabschnitt gewidmet werden, sodass eine strukturierte Darstellung der Ergebnisse gegeben ist.

3.2.1 Gestrichene Maßnahmen

Die in *Tabelle 1* genannten TO-Maßnahmen des BDSG bleiben in der neuen DSGVO unerwähnt und sind entsprechend aus dem Pool der TO-Maßnahmen rausgefallen. Es gibt in der DSGVO (unter Art. 32) keine Punkte, die die entsprechenden TO-Maßnahmen direkt ausdrücken bzw. vorschreiben.

Tabelle 1: Gestrichene Maßnahmen. (Erstellt von dem Verfasser, 2016).

Gesetzestext	*Trivialname*
Anlage (zu § 9 Satz 1) Satz 2 Nummer 1 „…Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren…“	Zutrittskontrolle
Anlage (zu § 9 Satz 1) Satz 2 Nummer 2 „…zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können…“	Zugangskontrolle
Anlage (zu § 9 Satz 1) Satz 2 Nummer 4 „…zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist…“	Weitergabe-kontrolle
Anlage (zu § 9 Satz 1) Satz 2 Nummer 5 „…zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind…“	Eingabekontrolle
Anlage (zu § 9 Satz 1) Satz 2 Nummer 8 „…zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.“	Trennungsgebot

Gut die Hälfte aller bisherigen TO-Maßnahmen des BDSG bleibt in der neuen DSGVO unerwähnt. Es darf jedoch zu diesem Zeitpunkt nicht unterstellt werden, dass die besagten Punkte in der neuen DSGVO vollkommen unberücksichtigt bleiben. Es ist durchaus möglich, dass die TO-Maßnahmen dennoch von Bedeutung sind (*siehe Abschnitt 3.4*).

3.2.2 Vergleichbare Maßnahmen

Wie bereits in *Abschnitt 3.1* einleitend geschildert, soll das Augenmerk des Vergleiches auf einer teleologischen Auslegung der Rechtsvorschriften beruhen. So kann es im Folgenden zu unterschiedlichen Formulierungen kommen, was aber einem sinngemäßen Vergleich nicht im Wege stehen soll. Die Spalte „Kommentar" am rechten Rand von *Tabelle 2* soll dabei Aufschluss darüber geben, wieso die jeweiligen Punkte miteinander verglichen wurden und wo sich trotz Ähnlichkeiten auch Unterschiede ergeben.

Tabelle 2: Vergleichbare Maßnahmen (inklusive Trivialnamen). (Erstellt von dem Verfasser, 2016).

	BDSG § 9 + Anlage	DSGVO Art. 32	Kommentar
	§ 9 Satz 1 „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten."	*Art. 32 Abs. 1* „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;"	Der Verantwortliche und der Auftragsverarbeiter haben wie bisher für die Umsetzung geeigneter TO-Maßnahmen zu sorgen. Durch Art. 32 Abs. 1 der DSGVO wird jedoch besonders Rücksicht auf… ▪ … den Stand der Technik ▪ … Kosten ▪ … Art, Umfang, Umstände und Zweck der Verarbeitung ▪ … Eintrittswahrscheinlichkeit ▪ … und Schwere des Risikos … genommen, was direkte Auswirkungen auf die geforderten TO-Maßnahmen hat. Entsprechend kann von einer Verhältnismäßigkeit gesprochen werden, wie in BDSG § 9 Satz 2 gefordert ist. Eine explizite Forderung einer geeigneten internen Struktur zur Einhaltung datenschutzrechtlicher Vorschriften wird nicht erwähnt, kann aber indirekt aus den oben genannten Punkten abgeleitet werden.
Verhältnismäßigk	*§ 9 Satz 2* „Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."		
	Anlage (zu § 9 Satz 1) Satz 1 „Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,…"		

Zugriffskontrolle	*Anlage (zu § 9 Satz 1) Satz 2 Nummer 3* „…zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,…“	*Art. 32 Abs. 4* „Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.“	Eine Zugriffskontrolle wie sie im BDSG Anlage (zu § 9 Satz 1) Satz 2 Nummer 3 gefordert wird ist in der DSGVO in dieser Form nicht zu finden. Es ist lediglich sicherzustellen, dass Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung der Verantwortlichen verarbeiten. Dieser Punkt bezieht sich ebenfalls auf Personen, die im Auftrag personenbezogene Daten bearbeiten, weshalb hier Parallelen zur Auftragskontrolle nach BDSG Anlage (zu § 9 Satz 1) Satz 2 Nummer 6 gezogen werden können.
Auftragskontrolle	*Anlage (zu § 9 Satz 1) Satz 2 Nummer 6* „…zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können,…“		
Verfügbarkeitskontrolle	*Anlage (zu § 9 Satz 1) Satz 2 Nummer 7* „…zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind,…“	*Art. 32 Abs. 1 lit. c* „…die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;…“	Nach DSGVO soll die Verfügbarkeit personenbezogener Daten auch bei physischen oder technischen Zwischenfällen wieder herstellbar sein.
Verschlüsselung	*Anlage (zu § 9 Satz 1) Satz 3* „Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.“	*Art. 32 Abs. 1 lit. a* „…die Pseudonymisierung und Verschlüsselung personenbezogener Daten;…“	Zusätzlich zu Verschlüsselungsverfahren wird in der DSGVO ebenfalls die Pseudonymisierung zum Schutz von personenbezogenen Daten gefordert (vgl. BDSG § 3a).

In der linken Spalte der Tabelle finden sich die jeweils gängigen Trivialnamen der TO-Maßnahmen des BDSG wieder, um die Zuordnung der jeweiligen Gesetzestexte zu vereinfachen.

Insgesamt werden vier Punkte miteinander verglichen, wobei die Punkte eins und zwei jeweils mehrere Paragraphen des BDSG zusammenfassen und jeweils einem Artikel der DSGVO gegenüberstellen. Vor allem die Punkte zwei (vgl. Trivialnamen „Zugriffskontrolle“ und „Auftragskontrolle“) und drei (vgl. Trivialname „Verfügbarkeitskontrolle“) geben Anlass für eine genauere Betrachtung (*siehe Abschnitt 3.3*).

3.2.3 Hinzukommende Maßnahmen

Zuletzt sollen in *Tabelle 3* alle Maßnahmen aufgelistet werden, die im Pool der bisherigen TO-Maßnahmen des BDSG nicht enthalten waren. Im Vergleich zu *Tabelle 1* gibt es für diese Maßnahmen noch keine gängigen Trivialnamen auf die verwiesen werden kann.

Tabelle 3: Hinzukommende Maßnahmen. (Erstellt von dem Verfasser, 2016).

Gesetzestext
Art. 32 Abs. 1 lit. b „…die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;…“
Art. 32 Abs. 1 lit. d „...ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“
Art. 32 Abs. 2 „Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.“
Art. 32 Abs. 3 „Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.“

- Neu sind die Forderung, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der mit der Verarbeitung zusammenhängenden Systeme sicherzustellen (DSGVO, 2016). Etwaige Anforderungen an die Systeme zur Datenverarbeitung selbst wurden laut BDSG nicht gestellt. Erstmals wird somit auch der Fokus auf die Systeme und nicht ausschließlich auf die personenbezogenen Daten gerichtet.
- Auch der Nachweis eines Verfahrens „zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen“ (vgl. Art. 32 Abs. 1 lit. d DSGVO) wird dem Pool der TO-Maßnahmen hinzugefügt. Ein derartiges Evaluierungsverfahren war bisher nicht Bestandteil der TO-Maßnahmen nach § 9 BDSG.
- Zusätzlich wird eine risikobasierte Beurteilung des Schutzniveaus gefordert, um geeignete TO-Maßnahmen zu treffen und umzusetzen. Diese risikobasierte Herangehensweise stellt einen der wesentlichen Unterschiede zum BDSG dar und soll in den folgenden Abschnitten und Kapiteln weiter betrachtet werden.

3.3 Diskussion

Wie in *Unterabschnitt 3.2.2* bereits angesprochen, sollen die Ergebnisse des Vergleichs in Bezug auf *Tabelle 2* (*siehe S. 9*) etwas genauer betrachtet werden. Speziell geht es um die grammatische Auslegung der Wörter „Zugang“, „Zugriff“ und „Zutritt“. Während im BDSG eine Unterscheidung der drei Begriffe stattfindet, so findet sich in der DSGVO lediglich der Begriff „Zugang“ wieder (*siehe Abbildung 2*).

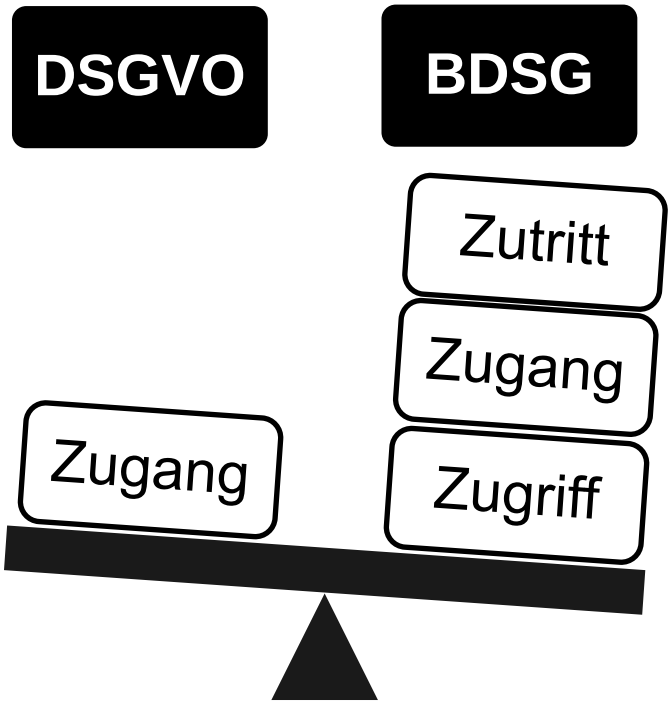

Abbildung 2: Terminologie der Begriffe „Zutritt“, „Zugang“ und „Zugriff“ wie sie im BDSG und in der DSGVO wiedergefunden werden (eigene Darstellung, 2016).

Nach bisherigem Verständnis des BDSG fand zwischen den drei Begriffen eine eindeutige Sinntrennung statt. Während mit dem Begriff der Zutrittskontrolle eine physische Trennung assoziierte wurde, damit Unbefugte physisch von der Datenverarbeitungsanlage getrennt wurden, wurde unter der Zugangskontrolle die Authentifizierung mit der Datenverarbeitungsanlage verstanden. Respektive war unter einer Zugriffskontrolle die Sicherstellung, dass nur Berechtigte Personen Zugriff auf die jeweiligen Daten erhalten (im Sinne von Berechtigungen), gemeint (BfDI Datenschutz WIKI, ohne Datum).

In der neuen DSGVO jedoch findet sich ausschließlich der Begriff „Zugang“ wieder. Auch eine Legaldefinition des Begriffes findet sich in der DSGVO nicht (vgl. Art. 4 DSGVO). Ein Blick in die Erwägungsgründe der DSGVO lässt zumindest erahnen, welche Bedeutung dem Begriff „Zugang“ zukommt. So heißt es in Punkt 39 der Erwägungsgründe, dass „Unbefugte keinen

Zugang zu den Daten haben [dürfen] und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können [sollen]“ (DSGVO, 2016). Gemäß dieser Definition kann geschlossen werden, dass mit „Zugang“ im Sinne der DSGVO sowohl der physische Zugang zu den Systemen bzw. Geräten, als auch ein technischer Zugangsschutz im Sinne einer Authentifizierung, sowie eine Berechtigungskontrolle gemeint sind. Anhand dieser Einschätzung wird der Vergleich, wie in *Tabelle 2* (*siehe S. 9*) zu sehen, sinngemäß nachvollziehbar.

Ein Blick auf die englische Originalversion der Verordnung gibt ebenfalls nicht eindeutig Aufschluss auf die genaue Absicht bzw. Definition des Begriffs. Hier wird lediglich der generische – ähnlich ungenaue bzw. unspezifische – Begriff „access“ verwendet (Regulation (EU) 2016/679 [GDPR], 2016).

Es kann davon ausgegangen werden, dass eine sinngemäße Trennung der bisherigen Terminologie des BDSG in der DSGVO nicht mehr vorgenommen wird. Vor allem für Personen, die sich an die Terminologie des BDSG gewöhnt haben wird es entsprechend notwendig sein, sich die neue Terminologie anzueignen und es sollte darauf geachtet werden, die Begriffe nicht durcheinander zu bringen.

3.4 Fazit

Auf den ersten Blick scheint die DSGVO dadurch gekennzeichnet zu sein, dass es weniger spezifische TO-Maßnahmen gibt im Vergleich zu den recht spezifischen Kontrollen des BDSG. Allerdings kann dadurch nicht abgeleitet werden, dass die zu implementierenden TO-Maßnahmen weniger umfangreich sind. Stattdessen sind die neuen TO-Maßnahmen der DSGVO allgemeiner gehalten und setzen eine unterschiedliche Herangehensweise zur Bestimmung der TO-Maßnahmen voraus.

Wie im Security-Bereich oft üblich, gibt es auch in der Informationstechnologie nur eine bestimmte Anzahl an TO-Maßnahmen, die zum Schutz personenbezogener Daten angewendet werden können. Diese werden nunmehr nicht länger genau vorgegeben, stattdessen wird es darum gehen, die geeigneten Maßnahmen gemäß dem Schutzziel und dem damit verbundenen Risiko zu ermitteln und umzusetzen (vgl. Art 32 Abs. 1 DSGVO). Somit fallen die in *Unterabschnitt 3.2.1* genannten Maßnahmen des BDSG nicht zwangsweise weg, sondern werden ggf. je nach individueller Sachlage trotzdem gefordert sein, um einen geeigneten Schutz zu gewährleisten.

Aufgrund der unterschiedlichen Herangehensweise macht es auf Grundlage der Ergebnisse nach *Abschnitt 3.2* wenig Sinn zu versuchen, bestehende TO-Maßnahmen nach § 9 BDSG in die neue DSGVO zu „übersetzen“. Einen derartigen Transfer der TO-Maßnahmen lassen die Ergebnisse nicht zu. Stattdessen sollten bestehende TO-Maßnahmen auf Grundlage der folgenden Kapitel und gemäß Art. 32 DSGVO evaluiert und ggf. an geforderter Stelle angepasst werden.

Da eine risikobasierte Herangehensweise den neuen Schwerpunkt der geforderten TO-Maßnahmen darstellt, soll der Fokus der weiteren Kapitel auf genau diesen zusätzlichen Anforderungen liegen.

3.5 *Beispiel*: Was sich in der Praxis ändert

Durch den Erlass der DSGVO ist auch die Arztpraxis betroffen. Um zu evaluieren, inwiefern die bereits vorhandenen TO-Maßnahmen nach BDSG evtl. ergänzt werden müssen, schauen sich der Verantwortliche und der IT-Administrator unter Rücksprache mit dem Datenschutzbeauftragten die neuen Anforderungen an die TO-Maßnahmen an.

Es fällt zunächst auf, dass einige der bereits implementierten TO-Maßnahmen, wie beispielsweise eine Verschlüsselung, wie sie im BDSG bereits gefordert waren auch weiterhin gefordert sind. Eine Abschaffung ist damit nicht empfehlenswert.

Weiterhin fällt jedoch auf, dass beispielsweise die bereits implementierte Weitergabekontrolle nicht mehr direkt gefordert wird. Diese Maßnahme wurde im Rahmen des BDSG umgesetzt, um die Daten zu schützen, wenn diese an Dritte (z.B. Versicherungsunternehmen oder andere Arztpraxen) weitergeleitet werden. Der IT-Administrator geht nun davon aus, dass diese Maßnahmen nicht mehr notwendig sind. Seiner Meinung nach wäre die Implementation dieser Maßnahme nun als zusätzlich zu betrachten und nicht mehr als gefordert. Der Datenschutzbeauftragte hingegen stimmt dem nicht zu. Er legt dem Verantwortlichen nahe, sich die neuen Forderungen noch einmal genau anzuschauen. Das Risiko, ausgehend der von der Weiterleitung betroffenen Daten, ist als sehr hoch anzusehen. Aufgrund dessen müssen gemäß der neuen Anforderungen der DSGVO TO-Maßnahmen getroffen werden, um dieses sehr hohe Risiko bei der Weitergabe zu senken. Um dies realisieren zu können sieht der Datenschutzbeauftragte die Implementierung einer Art Weitergabekontrolle, wie sie im BDSG gefordert war, weiterhin als notwendige und rechtlich vorgeschriebene Maßnahme an.

Auch in anderen Bereichen werden sich Änderungen ergeben. Zum einen muss zusätzlich geprüft werden, ob die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der mit der Verarbeitung zusammenhängenden Systeme zusätzlich zur Vertraulichkeit, Integrität und Verfügbarkeit der Daten gewährleistet wird. Ggf. müssten an dieser Stelle weitere TO-Maßnahmen in der Praxis getroffen werden. Da diese Forderung im BDSG noch nicht zur Sprache kam, müssen der Verantwortliche und der IT-Administrator die vorhandenen TO-Maßnahmen dahingehend untersuchen. Ebenso muss ein Verfahren geschaffen werden, um die getroffenen TO-Maßnahmen auf ihre Wirksamkeit hin zu überprüfen. Hierfür empfiehlt der Datenschutzbeauftragte die Dokumentation der ergriffenen TO-Maßnahmen, sowie die Dokumentation evtl. verhinderter Angriffe auf das System. Der Verantwortliche sollte in Zusammenarbeit mit dem IT-Administrator und in regelmäßigen Abständen (beispielsweise halbjährig) die TO-Maßnahmen auf ihre Aktualität hin überprüfen, und sicherstellen, dass die TO-Maßnahmen nach wie vor korrekt implementiert sind und Wirkung zeigen. Diese Überprüfung sollte ebenfalls dokumentiert werden. Da der Verantwortliche selbst sich nicht in der Lage sieht diese Überprüfung durchzuführen, muss darüber nachgedacht werden diese Überprüfung externen Dienstleistern zu übertragen.

Eine weitere Neuerung ist, dass das Schutzniveau explizit von den mit der Verarbeitung verbundenen Risiken abhängig ist. Um also angemessene TO-Maßnahmen treffen zu können wird es notwendig sein, dass der Verantwortliche zunächst einmal das Risiko erfasst, welches von den Datenverarbeitungssystemen in der Praxis ausgeht. Um dies zu erreichen empfiehlt der Datenschutzbeauftragte eine Datenschutz-Folgenabschätzung durchzuführen, wie sie in Art. 35 der DSGVO gefordert ist.

4 Data protection by design

Durch die Novellierung des europäischen Datenschutzrechts findet zum ersten Mal das Prinzip von *data protection by design* oder *Privacy by Design (PbD)* Einzug in das europäische Datenschutzrecht. Auf die deutsche Übersetzung dieses Prinzips soll an dieser Stelle verwiesen[2], im Verlauf der weiteren Ausarbeitung allerdings verzichtet werden, da diese irreführend sein kann.

Art. 25 DSGVO – in dem das Prinzip von PbD verankert ist – ist neben Art. 32 DSGVO einer der Kernpunkte in Bezug auf die technischen und organisatorischen Maßnahmen. So wird in Art. 25 Abs. 1 DSGVO gefordert, dass der Verantwortliche…

> *„…sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen […] zu treffen hat], die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Person zu schützen".*

Auch hierbei soll wie bereits in Art. 32 Abs. 1 DSGVO Rücksicht auf…

- … den Stand der Technik
- … die Implementierungskosten
- … Art, Umfang, Umstände und Zwecke der Verarbeitung
- … die Eintrittswahrscheinlichkeit
- … und die Schwere der mit der Verarbeitung verbundenen Risiken genommen werden.

Laut Danezis, et al. (2014) wurde der Begriff „Privacy by Design" hauptsächlich von Ann Cavoukian (Information and Privacy Commissioner of Ontario) geprägt. Ziel ist es, den Datenschutz nicht nur als zusätzliche Maßnahme im Verlauf der Datenverarbeitung zu implementieren, sondern Systeme und Prozessabläufe von Anfang an am Datenschutz auszurichten (*siehe Abschnitt 4.1*). So soll es zur Norm werden, dass Systeme und Prozessabläufe standardmäßig auf den Schutz von Daten ausgelegt sind.

[2] Vgl. Art. 25 DSGVO: „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen"

PbD beschränkt sich dabei nicht nur auf technische Maßnahmen (wie zum Beispiel Verschlüsselungsverfahren und Protokolle zur anonymen Kommunikation), sondern umfasst auch organisatorische Maßnahmen und soll sich auch in den Geschäftsmodellen wiederfinden (Danezis, et al. 2014).

Konkrete Vorgaben seitens der DSGVO oder anderen Rechtsvorschriften gibt es allerdings nicht. Was genau zum Prinzip des PbD gehört und wie dieses Prinzip bereits zum derzeitigen Zeitpunkt umgesetzt werden kann soll im Folgenden etwas ausführlicher betrachtet werden.

4.1 Die 7 Prinzipien von PbD

Das Prinzip von PbD soll anhand folgender Prinzipien verdeutlicht werden (Cavoukian, 2011):

(1) Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe (*Eng.: „Proactive not Reactive; Preventative not Remedial“*):

→ PbD ist auf eine proaktive Herangehensweise ausgelegt. Ziel ist es Risiken gar nicht erst entstehen zu lassen bzw. deren Eintreten durch aktives Zutun zu verhindern. PbD ist kein Werkzeug zur Minimierung der Auswirkungen nach Eintritt eines Zwischenfalls (Cavoukian, 2011).

(2) Datenschutz als Standardeinstellung (*Eng.: “Privacy as the Default Setting”*):

→ Durch die Standardeinstellung sollten bereits alle nötigen Maßnahmen zum Schutz personenbezogener Daten gewährleistet werden. Es sollte der betroffenen Person nicht obliegen, durch Änderungen die Sicherheit der Daten zu erhöhen; auch ohne jegliche aktive Beteiligung sollten die Systeme den optimalen Schutz gewährleisten (Cavoukian, 2011).

(3) Der Datenschutz ist in das Design eingebettet (*Eng.: “Privacy Embedded into Design”*):

→ Datenschutz soll Bestandteil der Grundfunktionen von IT-Systemen und Geschäftsabläufen sein und nicht als Zusatzfunktion hinzugefügt werden (Cavoukian, 2011).

(4) Volle Funktionalität und volle Datensicherheit (*Eng.: “Full Functionality — Positive-Sum, not Zero-Sum”*):

→ Durch PbD sollen keine Kompromisse eingegangen werden müssen und es soll trotz Datenschutz zu keinen Einsparungen an anderen Stellen kommen (Cavoukian, 2011).

(5) Datenschutz während des gesamten Lebenszyklus (*Eng.: "End-to-End Security — Full Lifecycle Protection"*):

→ PbD zielt darauf ab, dass während der gesamten Lebenszeit der Systeme Rücksicht auf den Datenschutz genommen wird. Durch die Einbettung entsprechender Funktionalität in die Systeme soll gewährleistet werden, dass bereits vor Inbetriebnahme Maßnahmen vorgesehen wurden, um während der Verarbeitung personenbezogener Daten deren Sicherheit zu gewährleisten, bis das System wieder abgeschafft wird (Cavoukian, 2011).

(6) Sichtbarkeit und Transparenz (*Eng.: "Visibility and Transparency — Keep it Open"*):

→ Durch unabhängige Prüfungen soll gewährleistet werden, dass die geforderten Maßnahmen gemäß den Versprechungen durchgesetzt werden und Wirkung zeigen, unabhängig der Geschäftspraktiken und integrierten Systeme (Cavoukian, 2011).

(7) Anwenderorientierte Gestaltung (*Eng.: "Respect for User Privacy — Keep it User-Centric"*):

→ PbD soll sowohl von Herstellern von Systemen, als auch von Anwendern so ausgerichtet werden, dass die entsprechenden Maßnahmen zum Schutz der Daten standardmäßig eingestellt sind und der betroffenen Person durch entsprechende anwenderfreundliche Gestaltung die Bedienung erleichtert wird (Cavoukian, 2011).

Dabei erstreckt sich das Prinzip von PbD laut Cavoukian (2011) auf insgesamt drei Kernbereiche:

(1) IT-Systeme
(2) Geschäftspraktiken
(3) Physisches Design und Netzwerkinfrastrukturen

Diese sieben Prinzipien können jedoch nicht als Anleitung zur effektiven Umsetzung von Maßnahmen gesehen werden, sondern beschreiben lediglich die Eigenschaften von PbD (Danezis, et al. 2014).

4.2 Privacy Enhancing Technologies

Im Zusammenhang mit dem Prinzip des PbD kommen auch oft sogenannte Privacy Enhancing Technologies (PETs) zur Sprache. Wohingegen PbD als übergreifendes Konzept gesehen werden kann, dass sich in allen Bereichen der Datenverarbeitung wiederfindet – einschließlich in Prozessabläufen und Geschäftspraktiken – stehen PETs hauptsächlich für die technische Umsetzung und Entwicklung von Systemen (Rost & Bock, 2011 & Cavoukian & Prosch, 2010). Die Implementierung von PETs bedeutet im Grunde eingebauter Datenschutz, der die gesamte Lebenszeit des Systems berücksichtigt (Danezis, et al. 2014). PETs sind somit auch wesentlicher Bestandteil des Prinzips des PbD. Allerdings sind PETs weitaus bekannter und umfangreicher dokumentiert, als es bei PbD der Fall ist (Hoepman, 2013).
ISO/IEC 29100 definiert PETs wie folgt:

> *"[P]rivacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system" (ISO/IEC 29100, 2011).*

Es handelt sich also um Systeme, die ohne Funktionalitätsverlust benötigte, personenbezogene Daten auf ein Minimum beschränken bzw. an geeigneten Stellen ganz darauf verzichten. Darunter fallen unter anderem Verschlüsselungssysteme, sowie Systeme zur anonymen Kommunikation oder zur Pseudonymisierung. Durch Einsatz von PETs können Risiken für betroffene Personen in Bezug auf Ihre personenbezogene Daten verringert bzw. vermieden werden, was den Verantwortlichen helfen kann, gesetzliche Vorgaben, wie sie auch in der DSGVO gefordert werden, einzuhalten (Danezis, et al. 2014).
Trotz ihrer Bekanntheit sind PETs (bis auf wenige Ausnahmen wie z.B. Verschlüsselungstechniken) noch nicht zum Standard geworden. Manchmal werden PETs allerdings auch als Allheilmittel gesehen, die alle datenschutzrelevanten Bedenken begraben, indem PETs einfach zu einem bestehenden System hinzufügt werden. Dies funktioniert in dieser Weise allerdings kaum. Um eine optimale Umsetzung von PETs zu gewährleisten, sollten diese im Rahmen eines übergreifenden Prozesses in die Unternehmensstrategien übernommen und integriert werden. Dies kann beispielsweise durch eine konsequente Umsetzung des Prinzips PbD erreicht werden (Danezis, et al. 2014).

4.3 Strategien zur Umsetzung von PbD

Um das Prinzip von PbD umsetzen zu können, muss zunächst verstanden werden, dass es sich hierbei nicht nur um reine Grundsätze, noch um eine reine Implementierung von PETs handelt. Stattdessen handelt es sich laut Danezis, et al. (2014) um einen Prozess, bestehend aus verschiedenen technischen und organisatorischen Maßnahmen.

Hoepman (2013) veröffentlichte acht Strategien zur Umsetzung von PbD. Auf Grundlage verschiedener Rechtsvorschriften und Datenschutzgrundsätzen isolierte Hoepman zunächst zehn Grundsätze des Datenschutzes. Diese zehn Grundsätze können auf die nun gültigen und geforderten Grundsätze der DSGVO bezogen werden. Wie in *Tabelle 4* zu sehen ist, finden sich alle von Hoepman genannten Grundsätze auch in der DSGVO wieder.

Tabelle 4: Grundsätze des Datenschutzes. (Erstellt von dem Verfasser, 2016).

Grundsätze des Datenschutzes nach Hoepman (2013)	**Grundsätze gemäß DSGVO**	
	Grundsatz	*Gesetzesreferenz*
Purpose limitation (comprising both specification of the purpose and limiting the use to that stated purpose).	Zweckbindung	Art. 5 Abs. 1 lit. b
Data minimisation.	Datenminimierung	Art. 5 Abs. 1 lit. c
Data quality.	Richtigkeit	Art. 5 Abs. 1 lit. d
Transparency.	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Art. 5 Abs. 1 lit. a
Data subject rights (in terms of consent, and the right to view, erase, and rectify personal data).	Rechte der betroffenen Person (z.B.: Recht auf Berichtigung)	Kap. 3, Abs. 3 (Art. 16)
The right to be forgotten.	Recht auf Vergessenwerden	Art. 17
Adequate protection.	Integrität und Vertraulichkeit	Art. 5 Abs. 1 lit. f
Data portability.	Recht auf Datenübertragbarkeit	Art. 20
Data breach notifications.	○ Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde ○ Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person	Art. 33 Art. 34
Accountability and (provable) compliance.	Rechenschaftspflicht	Art. 5 Abs. 2

Ausgehend von diesen Datenschutzgrundsätzen leitete Hoepman insgesamt acht Strategien ab, anhand derer diese Grundsätze wirksam umgesetzt werden können. Dabei wurden die

acht Strategien nochmals aufgeteilt in datenorientierte Strategien und prozessorientierte Strategien (Hoepman, 2013). Während die datenorientierten Strategien sich auf den direkten Umgang mit den Daten auf technischer Ebene beziehen, beziehen sich die prozessorientierten Strategien vor allem auf organisatorische Maßnahmen. Die Strategien sollen im Folgenden kurz beschrieben werden, wobei die englischen Originalbegriffe nach Hoepman (2013) beibehalten werden sollen. Zu den jeweiligen Strategien sollen in Anlehnung an Hoepman Ausprägungen genannt werden, die als Beispiel dafür dienen sollen, wie man die jeweilige Strategie umsetzen kann.

4.3.1 Datenorientierte Strategien

1) MINIMISE

> *"The amount of personal data that is processed should be restricted to the minimal amount possible." (Hoepman, 2013; S. 7)*

Daten sollten nur im benötigten Umfang gesammelt und verarbeitet werden. Durch die Limitierung personenbezogener Daten kann auch das Risiko für den Betroffenen gesenkt werden. Der Verantwortliche sollte sich überlegen, ob es eventuell auch Systeme gibt, die das gleiche Ziel erreichen, auch ohne die Verarbeitung von personenbezogenen Daten bzw. Systeme, die mit weniger Daten auskommen (Hoepman, 2013).

Ausprägungen: z.B.: Temporäres Cashen von Daten.

2) HIDE

> *"Any personal data, and their interrelationships, should be hidden from plain view." (Hoepman, 2013; S. 8)*

Daten selbst und auch deren mögliche Verbindung zueinander sollten so geschützt werden, dass sie für Dritte nicht einsehbar sind. Zum einen sollte die Vertraulichkeit der Daten geschützt werden und zum anderen sollte es auch nicht möglich sein, Verbindungen verschiedener Daten nachvollziehen zu können (vgl. *Abschnitt 5.2.2*: „Nichtverkettbarkeit") (Hoepman, 2013).

Ausprägungen: z.B.: Verschlüsselung, sowie Anonymisieren und Pseudonymisieren.

3) SEPARATE

> *"Personal data should be processed in a distributed fashion, in separate compartments whenever possible." (Hoepman, 2013; S. 8)*

Bei dieser Strategie können Parallelen zum Trennungsgebot nach Anlage (zu § 9 Satz 1) Satz 2 Nummer 8 des BDSG gezogen werden. Daten sollten getrennt voneinander verarbeitet und gespeichert werden. Hoepman geht noch einen Schritt weiter und bezieht diese Strategie auch auf die Vermeidung von Profilbildungen, indem zusammenhängende Daten getrennt voneinander gespeichert werden sollten. Im Gegensatz zu dieser Strategie stehen zentrale Webdienste, die Daten zentral zur Verfügung stellen. Dezentrale Systeme sollten hier vorgezogen werden (Hoepman, 2013).

Ausprägungen: z.B.: Physische Trennung (Festplatten), Peer-to-Peer Verbindungen.

4) AGGREGATE

> *"Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful." (Hoepman, 2013; S. 9)*

Durch das Zusammenführen von Daten können Rückschlüsse auf einzelne Personen verhindert bzw. erschwert werden. Anstatt alle gesammelten Daten einzelnen Personen zuzuordnen, können durch solche Zusammenführungen bzw. Aggregationen von Daten Gruppierungen gebildet werden, bei denen ab einer gewissen Größe einzelne Zuordnungen nur noch sehr schwer nachvollzogen werden können (Hoepman, 2013).

Ausprägungen: z.B.: Daten zu Datensätzen zusammenfügen (Beispiel: Personengruppen bei Umfragen)

4.3.2 Prozessorientierte Strategien

5) INFORM

> *"Data subjects should be adequately informed whenever personal data is processed." (Hoepman, 2013; S. 9)*

Betroffene Personen sollten darüber informiert werden, welche Daten gesammelt werden, weshalb diese gesammelt werden und wie diese gesammelt werden. Es sollten Angaben darüber gemacht werden, wie die Daten geschützt werden und ob Daten auch an Dritte übermittelt werden (Hoepman, 2013).

Ausprägungen: z.B.: Meldung von Verletzungen des Schutzes personenbezogener Daten durch automatische Versendung von E-Mails (automatisch generierte Verteilerlisten).

6) CONTROL

> *"Data subjects should be provided agency over the processing of their personal data." (Hoepman, 2013; S. 9)*

Zusätzlich zu den Rechten, die dem Betroffenen nach DSGVO zustehen, erstreckt sich diese Strategie auch auf die Art und Weise wie Betroffene auf ihre personenbezogenen Daten zugreifen und selbstständig kontrollieren können (Hoepman, 2013).

Ausprägungen: z.B.: Optionen zum Entfernen von Bild-Tags auf Social Media Seiten.

7) ENFORCE

> *"A privacy policy compatible with legal requirements should be in place and should be enforced." (Hoepman, 2013; S. 10)*

Richtlinien zur Umsetzung von Vorgaben und Anforderungen gemäß DSGVO sollten eingeführt und umgesetzt werden. Dies muss beispielsweise anhand von Art. 40 DSGVO bereits erfolgen. Entsprechend sollten geeignete TO-Maßnahmen umgesetzt werden, um den Anforderungen gerecht zu werden. Auch bei dieser Strategie können wieder Parallelen zu den gestrichenen TO-Maßnahmen des BDSG (*siehe Unterabschnitt 3.2.1*) gezogen werden (Hoepman, 2013).

Ausprägungen: z.B.: Verhaltensregeln nach Art. 40 DSGVO.

8) DEMONSTRATE

> *"Be able to demonstrate compliance with the privacy policy and any applicable legal requirements." (Hoepman, 2013; S. 10)*

Verantwortliche sollten nachweisen können, dass die Umsetzung der Richtlinien und den entsprechenden Maßnahmen auch tatsächlich erfolgt (Hoepman, 2013). Diese Strategie ist, ebenso wie Strategie sieben („ENFORCE"), inzwischen fester Bestandteil der DSGVO und somit erforderlich (Vgl. Art. 40, Abs. 4 DSGVO).

Ausprägungen: z.B.: Audits, Protokolle und Kontrollen durch Aufsichtsbehörden.

4.3.3 Zusammenfassung

Die Strategien nach Hoepman (2013) erlauben es, das Prinzip PbD greifbarer zu machen. Für die verschiedenen Ausprägungen der Strategien können schließlich PETs ausgewählt werden, um diese auf technischer Ebene umzusetzen. Zusammen mit den prozessorientierten Strategien kann so ein Gesamtkonzept geschaffen werden, das mit dem Prinzip PbD harmonisiert.

Wichtiger noch ist die Tatsache, dass Konformität mit den Strategien auch gleichzeitig Konformität mit den Datenschutzgrundsätzen bedeutet. Nicht jede Strategie erfüllt dabei alle Datenschutzgrundsätze. *Tabelle 5* soll die Zusammenhänge der Strategien mit den jeweiligen Datenschutzgrundsätzen veranschaulichen. In Anlehnung an Hoepman (2013) wurden dabei die nach DSGVO relevanten Datenschutzgrundsätze (*siehe Tabelle 4*; S. 20) der Tabelle beigefügt.

Tabelle 5: Zuordnung der Strategien auf die Datenschutzgrundsätze. (In Anlehnung an Hoepman, 2013; S. 11).

Legende: *+ trifft zu* *o trifft bedingt zu*		Zweckbindung	Datenminimierung	Richtigkeit	Transparenz	Rechte der betroffenen Person	Recht auf Vergessenwerden	Integrität, Vertraulichkeit	Recht auf Datenübertragbarkeit	„Informationspflicht“	Rechenschaftspflicht
Acht Strategien nach Hoepman (2013)	MINIMISE	o	+								
	HIDE		+					o			
	SEPARATE	o						o			
	AGGREGATE	o	+								
	INFORM				+	+				+	
	CONTROL			o		+			+		
	ENFORCE	+		+			+	+			o
	DEMONSTRATE										+

Erst durch die Kombination verschiedener Strategien kann ein einheitliches Konzept geschaffen werden.

Mit Bezug auf *Kapitel 3* ist zu bemerken, dass durch die Strategien nach Hoepman TO-Maßnahmen gefordert sein können, die zuvor als gestrichen deklariert wurden. So können beispielsweise zur Umsetzung der Strategie sieben („ENFORCE“) Maßnahmen zur Zugangs-, Zutritts- und Zugangskontrolle umgesetzt werden. Wie bereits in *Abschnitt 3.4* angemerkt, können diese TO-Maßnahmen somit durchaus von Bedeutung sein, auch wenn diese nicht mehr explizit in der DSGVO vorgeschrieben werden. Um jedoch die Forderungen, wie sie beispielsweise in Art. 25 DSGVO (PbD) genannt werden erfüllen zu können, werden diese gestrichenen TO-Maßnahmen durchaus wieder relevant.

4.4 *Beispiel*: Wie sich das Prinzip PbD umsetzen bzw. integrieren lässt

Im Rahmen der Evaluierung bestehender TO-Maßnahmen auf DSGVO Konformität, richtet sich der Blick des Verantwortlichen nun auf den Art. 25. Es geht darum, das Prinzip von PbD umzusetzen. In der Rechtsvorschrift selbst finden sich hierzu allerdings kaum Informationen. Um den Eigenschaften von PbD, sowie den Datenschutzgrundsätzen gerecht zu werden, empfiehlt der Datenschutzbeauftragte dem Verantwortlichen sich an den Strategien von Hoepman (2013) zu orientieren. Diese sind:

Datenorientierte Strategien:

- Minimise
- Hide
- Separate
- Aggregate

Prozessorientierte Strategien:

- Inform
- Control
- Enforce
- Demonstrate

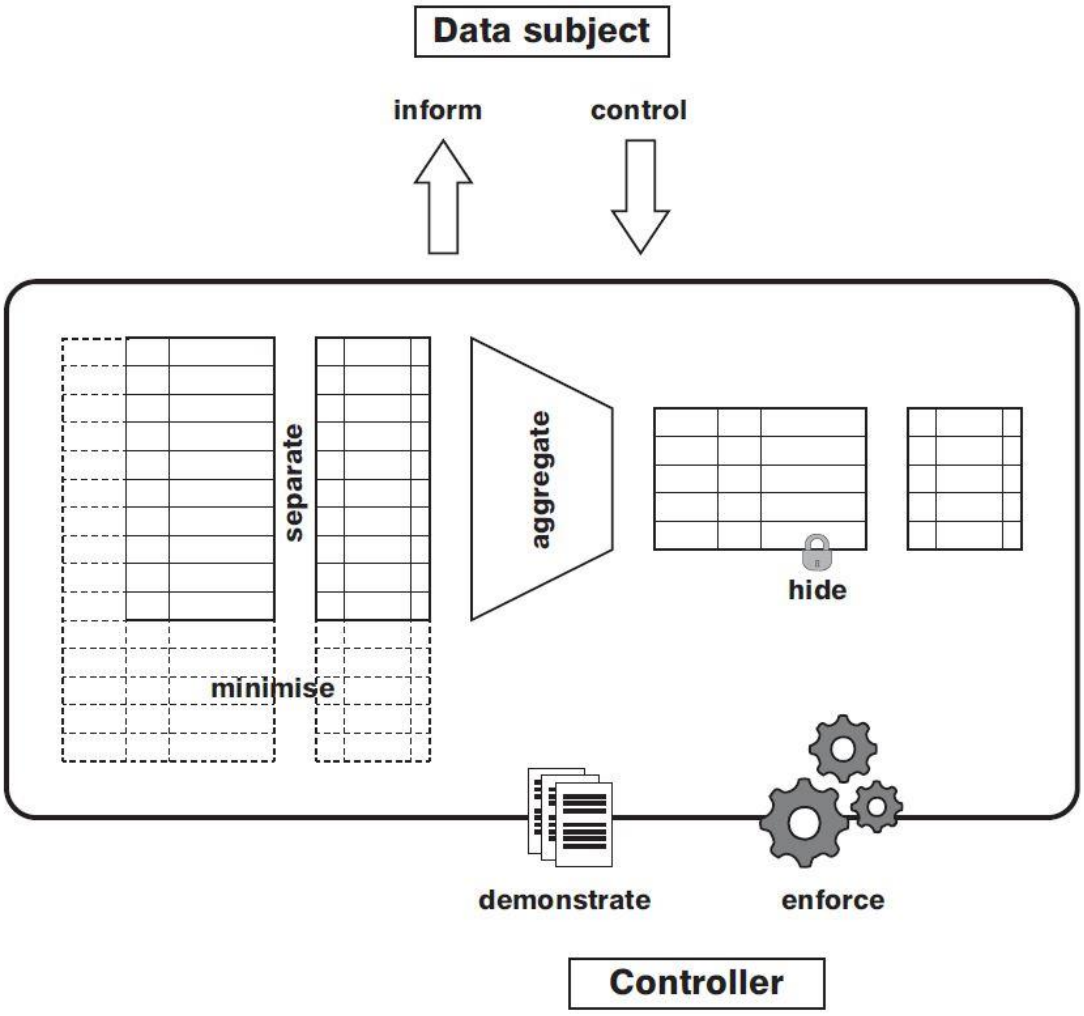

Abbildung 3: Anwendung der PbD Strategien auf eine Datenbank (Hoepman, 2013; S. 7).

Ziel ist es, die bestehenden TO-Maßnahmen dahingehend zu überprüfen, ob sie die Strategien nach Hoepman auch ausreichend umsetzen. Der Verantwortliche will das Prinzip PbD auf die in einer Datenbank gespeicherten Gesundheitsdaten anwenden. *Abbildung 3* zeigt eine skizzierte Implementierung der Strategien auf solch eine Datenbank. Aus der Abbildung schön zu erkennen, ist die Trennung in datenorientierte und prozessorientierte Strategien. Wohingegen die datenorientierten Strategien in der Datenbank selbst, auf technischer Ebene zur Anwendung kommen, unterstützen die prozessorientierten Strategien diese Implementierung, indem sie auf die organisatorischen Strukturen eingehen. Vor allem auf das Verhältnis des Betroffenen zum System und dem Verantwortlichen (vgl. *Abbildung 3*: „Data subject“) und auf das Verhältnis des Verantwortlichen zum System und dem Betroffenen (vgl. *Abbildung 3*: „Controller“) wird dabei eingegangen.

Der Verantwortliche schaut sich in Zusammenarbeit mit dem IT-Administrator nun die bereits implementierten TO-Maßnahmen an und überprüft, inwiefern sie den Strategien gerecht werden.

Minimise: Die in der Arztpraxis gesammelten Daten werden bereits auf ein Minimum reduziert. Das System sieht es nur vor, relevante Daten aufzunehmen, die für die Durchführung der Arbeit der Ärzte benötigt werden. Andere Daten können durch das System nicht erfasst werden. Für den Betrieb der Chat-Funktion werden bisher personenbezogene Daten der Patienten gesammelt und zu anderen Daten der Patienten hinzugefügt. Da die Chat-Funktion ausschließlich für unverbindliche, kleinere Beratungen gedacht ist ist das Sammeln von Daten nicht wichtig für den Betrieb der Arztpraxis. Eine Maßnahme an dieser Stelle wäre beispielsweise das Cachen der Daten, die nach Ablauf der Sitzung wieder sicher gelöscht werden.

Hide: Die Daten werden bereits mit einer dem Stand der Technik entsprechenden Verschlüsselung versehen. Auch der Kommunikationsweg der Chat-Funktion ist durch Verschlüsselungsverfahren abgesichert. Diese Strategie ist demnach bereits erfüllt.

Separate: Eine Separierung der gespeicherten Daten macht in der Arztpraxis nicht immer Sinn. Die gesammelten Daten sind nichts anderes, als eine digitale Patientenakte. Es ist somit wichtig, dass die Daten gesammelt vorliegen um ein einheitliches Krankenbild der Patienten zu ermöglichen. Jedoch könnte jeder Arzt die Daten seiner Patienten (sofern sinnvoll) physisch getrennt von den anderen Daten auf jeweils separaten Festplatten mit unterschiedlicher Authentifizierung speichern.

Aggregate: Das Zusammenführen macht wie bei der Separierung nicht immer Sinn. Die Daten sollten aufgrund der Geschäftspraktiken jederzeit den individuellen Patienten zugeordnet werden können. Der Datenschutzbeauftragte gibt dem Verantwortlichen allerdings den Hinweis, dass diese Strategie auf die Erhebung von Statistiken angewendet werden kann. Immer wieder werden Statistiken an Versicherungsunternehmen und andere Dritte weitergeleitet, um neuste Entwicklungen im Rahmen von Wissenschaft und Forschung verfolgen zu können. An dieser Stelle können jedoch zusätzlich TO-Maßnahmen implementiert werden, um Datensätze zusammenzufügen. Dadurch können Rückschlüsse auf die Patienten erschwert werden. So können die gesammelten Daten zur statistischen Erhebung auf Personengruppen bezogen werden. Diese Datensätze können anschließend von den Dritten nicht mehr nach einzelnen Personen gefiltert werden, sind aber für den benötigten Zweck immer noch nutzbar.

Inform: Die bereits bestehenden Verfahren zur Benachrichtigung betroffener Personen (nach BDSG), sollten überprüft werden und es sollte sichergestellt werden, dass diese an die Anforderungen gemäß Art. 12 – 14 DSGVO angepasst werden. Zusätzlich sollte in Erwägung gezogen werden, auch die getroffenen TO-Maßnahmen zum Schutz der Daten mit den Betroffenen zu kommunizieren. Der IT-Administrator macht den Vorschlag, zusätzliche Informationen auf der Website zu veröffentlichen, die die Betroffenen dort nachschlagen können um zu erfahren, wie die Daten geschützt werden.

Control: Bereits nach den in Kapitel 3 der DSGVO zu findenden Anforderungen muss der Verantwortliche sicherstellen, dass die dem Betroffenen eingeräumten Rechte umgesetzt werden können. Um dem Prinzip von PbD gerecht zu werden empfiehlt der Datenschutzbeauftragte dem Verantwortlichen zusätzlich mit dem IT-Administrator abzusprechen, inwiefern auch technische Verfahren umgesetzt werden können, damit der Betroffene seine Rechte geltend machen kann. Im Gespräch sind hierbei Webportale, in denen der Betroffene seine Rechte durchsetzen kann. Allerdings unterliegt der Verantwortliche an dieser Stelle auch weiteren Rechtsvorschriften. Gemäß nationalem Recht müssen die Ärzte beispielsweise die Gesundheitsdaten der Patienten eine bestimmte Zeit aufbewahren. Somit soll es nicht möglich sein, dass der Betroffene seine Daten selbst löschen kann. Stattdessen würde der IT-Administrator gerne ein Webportal einrichten, dass es den Betroffenen erlaubt bestimmte Anfragen direkt und automatisiert zu stellen, auf die der Verantwortliche dann gemäß der in der DSGVO geschilderten Regelungen entsprechend

reagieren muss. Somit kann dem Betroffenen eine gewisse Kontrolle über seine Rechte eingeräumt werden.

Enforce: Der Verantwortliche erarbeitet zusammen mit dem Datenschutzbeauftragten eine Verhaltensregel, die die Punkte gemäß Art. 40 Abs. 2 DSGVO berücksichtigt. Diese Verhaltensregel dient dazu, die Umsetzung der beschlossenen Maßnahmen zu begründen und ein internes Regelwerk zu schaffen, dass zur Umsetzung der beschlossenen Maßnahmen dient. Ein derartiges Regelwerk besteht in der Arztpraxis derzeit noch nicht.

Demonstrate: Auch an dieser Stelle ist der Verantwortliche bereits gemäß Art. 40 Abs. 4 DSGVO aufgefordert, die Einhaltung der erlassenen Verhaltensregeln nachweisen zu können. Um dieser Forderung gerecht zu werden, entscheidet sich der Verantwortliche für ein internes Auditverfahren in Absprache mit dem Datenschutzbeauftragten. Anhand eines halbjährigen Auditverfahrens soll demonstriert und nachgewiesen werden, dass die intern aufgestellten Verhaltensregeln, sowie alle notwendigen und geforderten Maßnahmen ordnungsgemäß umgesetzt wurden und wirksam sind. Das genaue Auditverfahren soll in Absprache mit dem Datenschutzbeauftragten erarbeitet werden. Gegebenenfalls soll hier auf externe Dienstleister zurückgegriffen werden, die das Audit durchführen.

Durch die Umsetzung dieser Strategien kann der Verantwortliche von einer sehr hohen Konformität mit dem Prinzip PbD und den Datenschutzgrundsätzen der DSGVO ausgehen.

5 Datenschutz-Folgenabschätzung

Wie bereits in den Artikeln 32 und 25 DSGVO gefordert, muss bei der Wahl geeigneter TO-Maßnahmen „[die …] Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen“ berücksichtigt werden. Um also bestehende TO-Maßnahmen anhand der neuen Anforderungen zu evaluieren oder bei der Implementierung neuer TO-Maßnahmen, muss das Risiko ausgehend von den personenbezogenen Daten erfasst und beurteilt werden. Diese sogenannte Datenschutz-Folgenabschätzung (DSFA) wird in Art. 35 DSGVO erläutert. Wie genau diese DSFA durchgeführt werden soll bzw. kann wird aus Art. 35 jedoch nicht ersichtlich. Lediglich die allgemeinen Anforderungen an eine DSFA werden darin genannt.

In einigen Ländern, darunter auch europäische Länder, ist das Prinzip der DSFA bereits seit einigen Jahren gefestigt worden und entsprechend gibt es Empfehlungen, wie solch eine DSFA aussehen sollte und wie man diese durchführen kann. So haben sowohl die britische Datenschutzaufsichtsbehörde (Information Commissioner’s Office), als auch die französische Behörde für Datenschutz und Informationsfreiheit (Commission Nationale de l’Informatique et des Libertés) Handlungsempfehlungen zur Erstellung einer DSFA veröffentlicht (Information Commissioner's Office [ICO], 2014 & Commission Nationale de l’Informatique et des Libertés [CNIL], 2012 & CNIL, 2015a & CNIL, 2015b). In Bezug auf deren Rechtskonformität mit der nun veröffentlichten DSGVO, erfüllt das von der britischen Datenschutzaufsichtsbehörde erlassene Dokument die Anforderungen der DSGVO laut Friedewald, Obersteller, Nebel, Bieker & Rost (2016) nur teilweise, wohingegen die Dokumente der französischen Behörde für Datenschutz und Informationsfreiheit die Anforderungen in vollem Umfang erfüllen.

5.1 Anforderungen an eine DSFA

Aus Art. 35 DSGVO („Datenschutz-Folgenabschätzung“) können Mindestanforderungen an eine DSFA extrahiert werden. Zunächst einmal ist zu klären, wann eine DSFA durchzuführen ist. Hier besagt Art. 35 Abs. 1, dass eine DSFA insbesondere dann durchzuführen ist, sofern „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge

hat“. Auch die Verwendung neuer Technologien soll gemäß Abs. 1 berücksichtigt werden. In Art. 35 Abs. 3 werden noch spezifischere Angaben gemacht. So können insgesamt drei Fälle isoliert werden, bei denen eine DSFA insbesondere durchzuführen ist:

> *„a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;*
>
> *b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder*
>
> *c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.“ (Art. 35 Abs. 3 DSGVO)*

Zusätzlich sollen gemäß Art. 35 Abs. 4 und Abs. 5 die Aufsichtsbehörden Listen erstellen, mit Verarbeitungsvorgängen für die eine DSFA erforderlich ist, bzw. für die eine DSFA nicht erforderlich ist. Somit können beispielsweise Verarbeitungsvorgänge, die weit verbreitet sind und von vielen Verantwortlichen durchgeführt werden, durch die Aufsichtsbehörde klassifiziert werden. Es obliegt dann nicht mehr nur alleine dem Verantwortlichen festzustellen, ob eine DSFA gefordert wird oder nicht. Diese Listen (sofern diese veröffentlicht werden), sollten entsprechend herangezogen werden, um vor der Initialisierung eines DSFA-Prozess festzustellen, ob eventuell bereits festgelegt wurde, dass keine DSFA im entsprechenden Szenario gefordert wird.

Ist eine DSFA gefordert, so müssen laut Art. 35 Abs. 7 DSGVO mindestens folgende Punkte enthalten sein:

> *„a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;*
>
> *b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;*
>
> *c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und*
>
> *d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür*

> *erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird." (Art. 35 Abs. 7 DSGVO)*

Zusätzlich zu diesen Mindestanforderungen sollte der Verantwortliche:

- Verhaltensregeln, die gemäß Art. 40 DSGVO genehmigt wurden einhalten,
- den Standpunkt Betroffener einholen, sofern möglich
- überprüfen, ob die Verarbeitung gemäß der Ergebnisse der DSFA durchgeführt wird, vor allem wenn sich das Risiko ändern sollte (Art. 35 Abs. 8-10 DSGVO).

Wie genau die Umsetzung zu erfolgen hat (oder kann), wird in der DSGVO, wie bereits erwähnt, nicht weiter erläutert. In den folgenden Abschnitten soll deshalb eine Methode nach Friedewald, et al. (2016) skizziert werden, wie eine solche DSFA umgesetzt werden kann und welche wesentlichen Inhalte und Schritte sie umfassen sollte.

5.2 Methode zur Durchführung einer DSFA

Laut Danezis, et al. (2014; S. 12), besteht der Prozess einer DSFA aus mindestens fünf Kern-Schritten. Diese umfassen:

> *(1) "the identification of stakeholders and consulting of these stakeholders,*
> *(2) the identification of risks (taking into account the perception of the stakeholders),*
> *(3) the identification of solutions and formulation of recommendations,*
> *(4) the implementation of the recommendations,*
> *(5) reviews, audits and accountability measures."*

Diese Schritte finden sich auch im Aufbau in der von Friedewald, et al. (2016) beschriebenen Vorgehensweise wieder. Nach Friedewald, et al. wird der Prozess der DSFA in insgesamt drei übergreifende Phasen unterteilt (*siehe Abbildung 4*). Eine Vorbereitungsphase, eine Bewertungsphase und eine Berichts- und Maßnahmenphase. Wichtig bei der Durchführung einer DSFA ist dabei diese aus Sichtweise der Betroffenen durchzuführen und nicht aus Sicht des Unternehmens bzw. der Organisation. Es soll in erster Linie nicht um die Erfassung von Risiken für das Unternehmen gehen, die bei Nicht-Einhaltung von geltendem Recht entstehen können, sondern um die Risiken für die Betroffenen, um deren Daten es geht (Friedewald, et al. 2016).

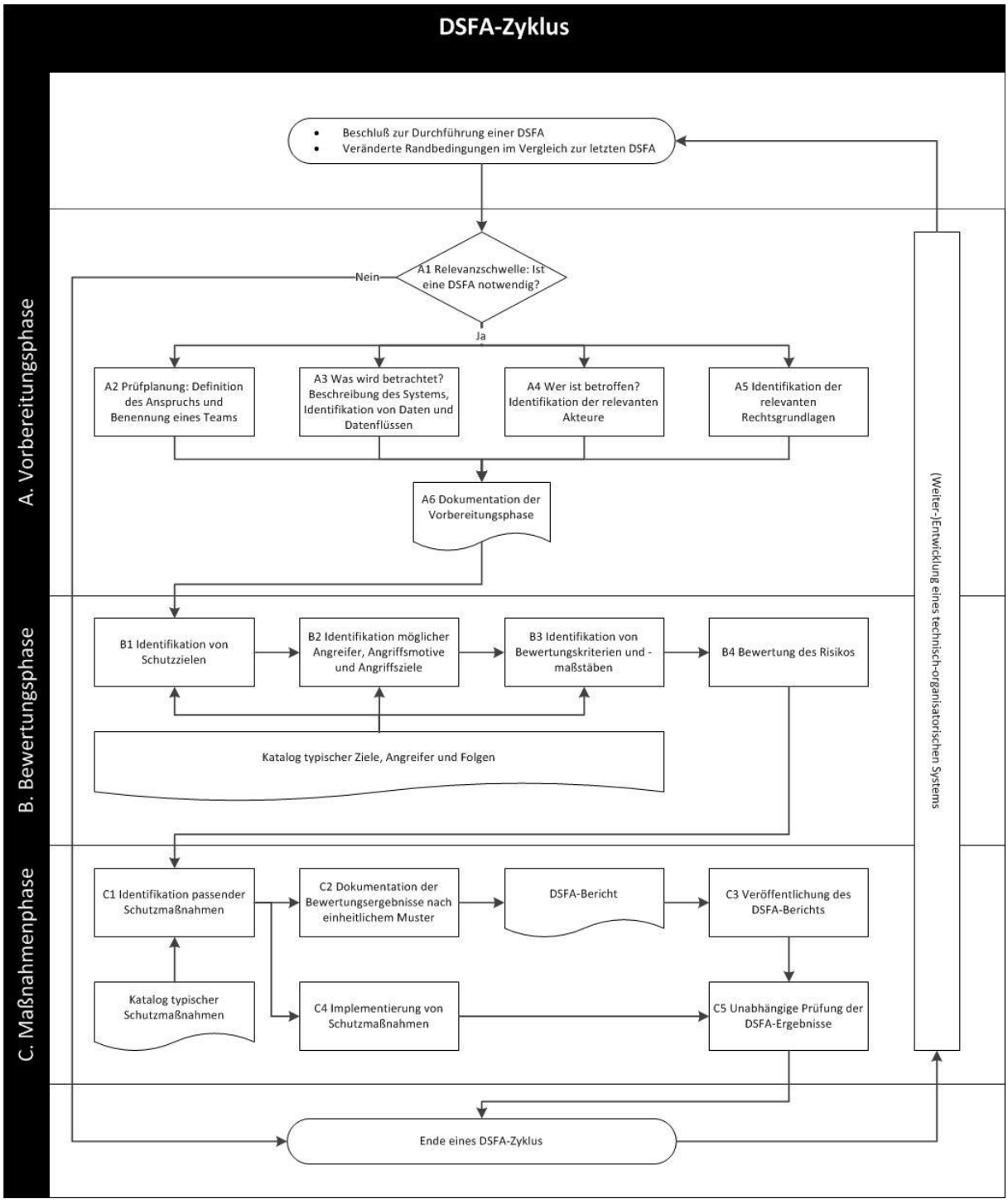

Abbildung 4: DSFA-Zyklus. (In Anlehnung an Friedewald, et al. 2016; S. 19. Verändert durch den Verfasser).

5.2.1 Vorbereitungsphase

Während der Vorbereitungsphase soll die eigentliche DSFA vorbereitet und geplant werden. Ziel ist es den Rahmen zu definieren, sowie alle Akteure und relevante Systeme zu definieren und zu dokumentieren.

A1 – Relevanzschwelle

Im ersten Schritt soll untersucht werden, ob eine DSFA notwendig ist oder nicht. Hier gilt es den Anforderungen gemäß *Abschnitt 5.1* Folge zu leisten und zu entscheiden, ob eine DSFA im jeweiligen Fall vorgeschrieben ist oder nicht.

Anzumerken ist hierbei, dass zur Feststellung, ob bei der Datenverarbeitung ein hohes Risiko für Betroffene gegeben ist (Vgl. Art. 35 Abs. 1 DSGVO), bereits eine entsprechende Risikoabschätzung durchgeführt worden sein muss. Hier scheint sich in gewisser Weise ein Konflikt offenzulegen. Um zu entscheiden, ob eine DSFA überhaupt notwendig ist, muss bereits eine Art DSFA durchgeführt werden. Kommt man hier zu dem Ergebnis, dass eine DSFA nicht gefordert ist, so wird der DSFA-Zyklus bereits unterbrochen bzw. beendet (Friedewald, et al. 2016).

A2 – Prüfplanung

Nachdem eine entsprechende Relevanz zur Durchführung einer DSFA gegeben ist, müssen die Ziele der DSFA definiert und ein Team zur Durchführung der DSFA gebildet werden.

Das Team sollte die benötigten Kompetenzen innehaben und auch in der Lage sein durch Vertretung von Verantwortlichkeiten Entscheidungen treffen und auch entsprechend umsetzen zu können. Gemäß Art. 35 Abs. 2 ist bei der Durchführung der DSFA der Rat des Datenschutzbeauftragten hinzuzuziehen (falls ein Datenschutzbeauftragter bestellt ist).

Nachdem ein Team zusammengestellt wurde muss dieses den Charakter der DSFA festlegen. Hierbei wird zwischen drei verschiedenen Typen unterschieden (Friedewald, et al. 2016):

- Marketing-DSFA
- Standard-DSFA
- Wissenschaftliche-DSFA

Laut Friedewald, et al. (2016) erfüllt nur die Standard-DSFA die gesetzlich geforderten Anforderungen. Entsprechend soll die Standard-DSFA alleiniges Spektrum der weiteren Betrachtung sein. Ziel der Standard-DSFA ist der Nachweis, dass geeignete TO-Maßnahmen

gemäß den gesetzlichen Vorgaben getroffen und angemessen umgesetzt wurden. Die zur Bewertung herangezogenen Kriterien, sowie die festgelegten Schutzmaßnahmen sollten vordefinierten Katalogen entnommen werden, sodass eine standardisierte Dokumentation vorgenommen werden kann und die Ergebnisse von der Aufsichtsbehörde und der Öffentlichkeit leicht nachvollzogen werden können (Friedewald, et al. 2016).

A3 – Was wird betrachtet?

Zusätzlich zur Festlegung des Typs der DSFA ist festzulegen, was durch die DSFA erfasst und betrachtet werden soll. Friedewald, et al. (2016) unterscheidet zwischen fünf Komponenten, die zur Beschreibung des zu betrachteten Rahmens zu beachten sind:

- Zweck
- Kontext
- Daten (inklusive deren Formate und verwendeten Protokolle)
- IT-Systeme (inklusive Schnittstellen)
- Prozesse

Abhängig von der Zielsetzung gibt es wiederum verschiedene Typen der DSFA:

- konkrete DSFA
- generische DSFA

Die beiden Typen unterscheiden sich dabei hauptsächlich dadurch, was Betrachtungsgegenstand ist. Während die generische DSFA Verfahren, Technologien oder Komponenten unabhängig ihrer jeweiligen Einsatzumgebung betrachtet, werden bei der konkreten DSFA alle Prozesse betrachtet, die mit der Datenverarbeitung in Zusammenhang stehen (Friedewald, et al. 2016). Während sich eine generische DSFA vor allem für Hersteller von Technologien eignet, sollten Verantwortliche, zur Erfüllung der Vorgaben gemäß Art. 35 DSGVO eine konkrete DSFA durchführen. Diese kann nach Friedewald, et al. (2016) durchaus auf einer generischen DSFA aufbauen, die beispielsweise durch den Hersteller einer erworbenen Technologie bereitgestellt wird.

A4 – Beteiligte Akteure

Bei der Berücksichtigung der beteiligten Akteure geht es vor allem um die Personen, die nicht nur mit der Entwicklung oder dem Betreiben der jeweiligen Technologien oder Verfahren betraut sind, sondern vor allem um die betroffenen Personen, die von der

Datenverarbeitung betroffen sind und um deren personenbezogene Daten es letztendlich geht (Friedewald, et al. 2016). Friedewald, et al. nennt hier konkret fünf Gruppen, die genauer zu betrachten sind:

- Hersteller von Technologien und Verfahren
- Betreiber der Technologien und Verfahren (Auftragsverarbeiter)
- Mitarbeiter, der für die Verarbeitung Verantwortlichen
- Betroffene Personen (Kunden, Patienten, Bürger,…)
- Dritte (z.B.: Sicherheitsbehörden oder Personen die zufällig Kenntnis von personenbezogenen Daten erhalten)

Es ist jeweils zu erfassen, welches Interesse die jeweiligen Akteure verfolgen, welche Rolle sie bei der Datenverarbeitung einnehmen und in welcher Rechtsbeziehung sie zu den anderen Akteuren stehen (Friedewald, et al. 2016).

A5 – Identifikation der relevanten Rechtsgrundlage

Bei der Identifikation der relevanten Rechtsgrundlage wird es hauptsächlich um die Einhaltung der DSGVO gehen, bzw. es ist festzustellen, ob die DSGVO im jeweiligen Fall Anwendung findet. Ist dies der Fall, wird sie maßgebend sein. Gemäß der Normenhierarchie müssen zusätzlich zur DSGVO auch noch eventuelle nationale Regelungen beachtet werden, die im Rahmen der Öffnungsklauseln der DSGVO umgesetzt wurden um die offenen, nicht von der DSGVO im Detail geregelten Bestände, abschließend zu regeln. Andere Rechtsgrundlagen – wie beispielsweise AGBs und Verbraucherrechte – werden laut Friedewald, et al. (2016) nur in bestimmten Fällen relevant sein und sollten im Rahmen der Compliance behandelt werden.

A6 – Dokumentation der Vorbereitungsphase

Laut Friedewald, et al. (2016) sollten die Ergebnisse und Erkenntnisse der Vorbereitungsphase in einer standardisierten Form dokumentiert und festgehalten werden. Diese Dokumentation dient entsprechend als Grundlage für die nächste Phase (die Bewertungsphase) und auch hier sollten später die Ergebnisse in der entsprechenden, standardisierten Form festgehalten werden. Wie genau diese Darstellung aussehen kann wird weder von Friedewald, et al. (2016) weiter erläutert oder erklärt, noch gibt es hierzu Empfehlungen der Aufsichtsbehörden.

5.2.2 Bewertungsphase

B1 – Identifikation von Schutzzielen

Zusätzlich zu den in der Informationssicherheit üblichen und etablierten Schutzzielen („Verfügbarkeit“, „Integrität“ und „Vertraulichkeit“) werden speziell für den Datenschutz drei zusätzliche Schutzziele eingeführt. Diese sind „Transparenz“, „Nichtverkettbarkeit“ und „Intervenierbarkeit“ (Rost & Bock, 2011).

- *Transparenz*: Laut Probst (2012) versteht man unter dem Schutzziel der Transparenz, dass „die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann“.
- *Nichtverkettbarkeit*: Nichtverkettbarkeit soll gewährleisten, dass erhobene Daten nur für den eigentlichen Zweck genutzt werden können, indem die Daten nicht mit anderen Daten verknüpft, bzw. verkettet werden (Probst, 2012). Durch eine derartige Verkettung von Daten könnten weitere Rückschlüsse gemacht werden, die über die eigentlichen Zwecke der Datenverarbeitung hinausgehen.
- *Intervenierbarkeit*: Dieses Schutzziel soll die Rechte der Betroffenen durchsetzen, sodass diese durch Eingreifen ihre Interessen und Rechte direkt und ohne große Umstände umsetzen können (Probst, 2012).

Tabelle 6: Datenschutzgrundsätze bezogen auf die Datenschutz-Schutzziele. (Erstellt von dem Verfasser, 2016).

Grundsätze gemäß DSGVO *Grundsatz*	*Gesetzesreferenz*	**Schutzziele (Beispiele)**
Zweckbindung	Art. 5 Abs. 1 lit. b	Nichtverkettbarkeit
Datenminimierung	Art. 5 Abs. 1 lit.c	Nichtverkettbarkeit
Richtigkeit	Art. 5 Abs. 1 lit. d	Integrität
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Art. 5 Abs. 1 lit. a	Transparenz
Rechte der betroffenen Person (z.B.: Recht auf Berichtigung)	Kap. 3, Absch. 3 (Art. 16)	Intervenierbarkeit
Recht auf Vergessenwerden	Art. 17	Intervenierbarkeit
Integrität und Vertraulichkeit	Art. 5 Abs. 1 lit. f	Vertraulichkeit
Recht auf Datenübertragbarkeit	Art. 20	Intervenierbarkeit
○ Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde ○ Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person	Art. 33 Art. 34	Transparenz
Rechenschaftspflicht	Art. 5 Abs. 2	Transparenz

Diese Schutzziele lassen sich mindestens einem oder mehreren der in *Abschnitt 4.3* aufgeführten Datenschutzgrundsätzen zuordnen (*siehe Tabelle 6*) (Friedewald, et al. 2016). Zusätzlich müssen eventuelle Schutzziele, die in der obigen Auflistung noch nicht inbegriffen sind einzeln erfasst und ebenfalls berücksichtigt werden (Friedewald, et al. 2016).

B2 – Identifikation möglicher Angreifer, Angriffsmotive und Angriffsziele

Nach Festlegung der Schutzziele ist zu identifizieren, von welchen Akteuren ein Risiko für die Betroffenen ausgeht. An dieser Stelle soll noch einmal verdeutlicht werden, dass es, wie einleitend bereits geschildert, um die Risiken der Betroffenen und nicht um die Risiken für das Unternehmen geht (im Gegensatz zur Vorgehensweise in der Informationssicherheit). Hier ist eine objektive Sichtweise zwingend erforderlich, da auch der für die Verarbeitung Verantwortliche ein gewisses Risiko für die Betroffenen darstellt und insofern als Angreifer gesehen werden kann (Friedewald, et al. 2016).

Folgende Organisationen sollten nach Friedewald, et al. (2016; S. 26) auf deren Motive und mögliche Risiken für die Betroffenen hin überprüft werden:

- *„Staatliche Stellen, z. B.*
  - *Sicherheitsbehörden: Innenministerien, Polizei, Geheimdienste, Militär etc.*
  - *Staatliche Leistungsverwaltung: Leistungsträger für Arbeitslosengeld II („Hartz IV"), Rentenversicherungsträger etc.*
  - *Statistische Ämter*
  - *Versagende Aufsichtsbehörden, die durch das Hinterlassen rechtsfreier Räume Angriffe anderer Akteure ermöglichen*
- *Unternehmen, z. B.*
  - *Technologiehersteller, Systemintegratoren, IT-Diensteanbieter (Zugang, Inhalte etc.)*
  - *Banken, Versicherungen*
  - *Wirtschaftsauskunfteien, Adress- und Datenhandel, Marktforschung*
  - *Werbebranche*
  - *Interessenvereinigungen, Verbände*
  - *Arbeitgeber*
- *Gesundheitswesen, z. B.*
  - *Krankenhäuser, Ärzte*
  - *gesetzliche und private Krankenversicherungen*
- *Forschung, z. B.*
  - *Medizinforschung*
  - *Sozialforschung*
  - *Universitäten"*

B3 – Identifikation von Bewertungskriterien und –maßstäben

Zur Bewertung der Risiken empfiehlt sich ein am IT-Grundschutzmodell ausgerichtetes System, wobei die traditionelle Beurteilung anhand Eintrittswahrscheinlichkeit und Schadenshöhe nicht sinnvoll anwendbar ist. Stattdessen verweist Friedewald, et al. (2016; S. 27) auf folgende Einteilung des Schutzniveaus:

- *„**Normal**: Es werden personenbezogene Daten verarbeitet, ohne dass Verarbeitungsszenarien mit potenziell erhöhter Eingriffsintensität gegeben sind.*
- ***Hoch**: Es werden personenbezogene Daten verarbeitet, die der Kategorie „besonderer Arten personenbezogener Daten“ zuzuordnen sind und als solche de lege lata hohen Schutzbedarf aufweisen, und/oder die Betroffenen sind von den Entscheidungen bzw. Leistungen der Organisation abhängig, wobei*
  - *die hohe Eingriffsintensität der Datenverarbeitung zu erheblichen Konsequenzen für die Betroffenen führen kann und/oder*
  - *keine effektiven Interventions-/Selbstschutzmöglichkeiten für die Betroffenen bestehen; hierzu zählt auch das Fehlen realistischer Möglichkeiten gerichtlicher Überprüfung.*
- ***Sehr hoch**: Es werden personenbezogene Daten mit hohem Schutzbedarf verarbeitet, und zusätzlich sind die Betroffenen von den Entscheidungen bzw. Leistungen der Organisation unmittelbar existenziell abhängig und es bestehen zusätzliche Risiken durch unzureichende Informationssicherheit oder unzulässige Zweckänderung seitens der Organisation, ohne dass die Betroffenen solche direkt bemerken und/oder korrigieren können.“*

Wie bereits aus dem Prozess des IT-Grundschutzes bekannt, kann auch gemäß dieser Einteilung des Schutzniveaus ein Kumulationseffekt eintreten, der entsprechend berücksichtigt und das Schutzniveau ggf. angepasst werden muss (Friedewald, et al. 2016).

Bei der späteren Einstufung des Schutzniveaus anhand der oben genannten Kriterien ist zu bemerken, dass sich die Schutzziele auch gegenseitig beeinträchtigen. Die oben genannten Schutzziele können jeweils in zweier Paaren angeordnet werden, wobei sich die jeweiligen gegenüberstehenden Schutzziele beeinträchtigen können. Hat man beispielsweise festgestellt, dass das Schutzziel „Vertraulichkeit“ als sehr hoch eingestuft wird, so müssen Maßnahmen getroffen werden, die sich direkt auf das Schutzziel „Verfügbarkeit“ auswirken können (beispielsweise durch eine Reihe von Zugangsberechtigungsmaßnahmen). Dieses Spannungsfeld soll gemäß *Abbildung 5* verdeutlicht werden. Die sich jeweils gegenüberstehenden Schutzziele können sich dabei gegenseitig beeinflussen. Dies muss bei der Einstufung beachtet werden und ggf. Prioritäten identifiziert werden (Friedewald, et al. 2016).

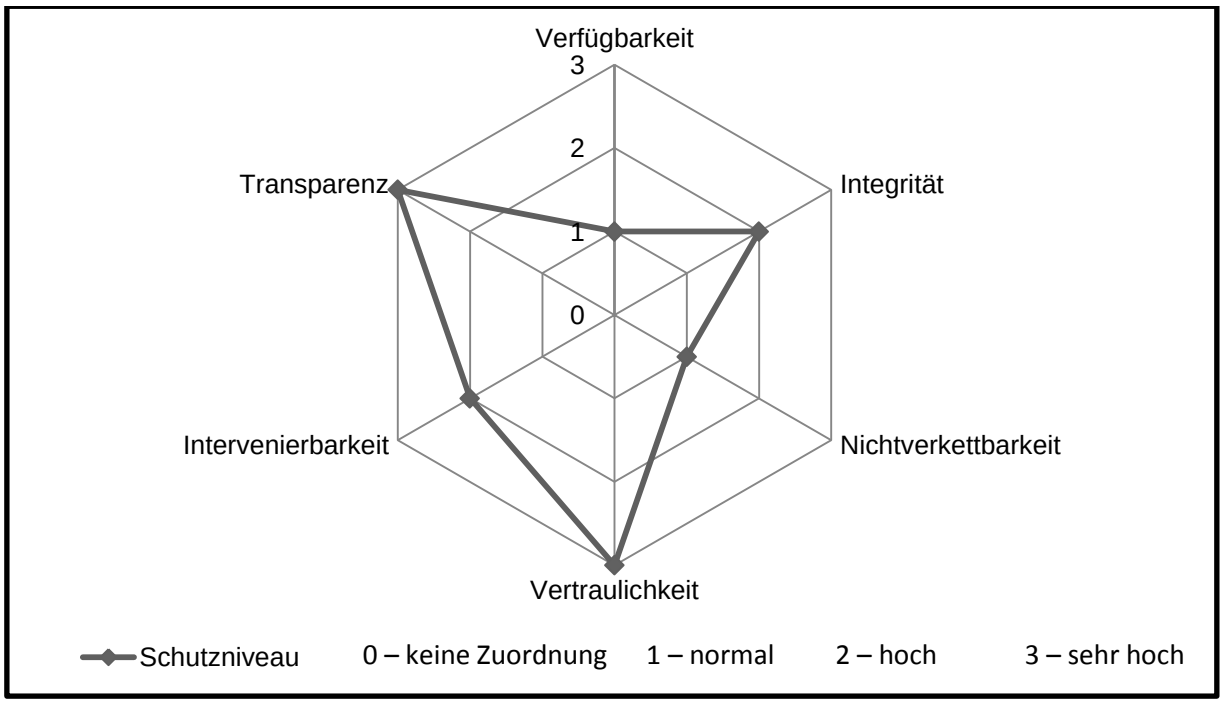

Abbildung 5: Grafische Darstellung der Schutzzieleinstufung (eigene Darstellung, 2016).

Die festgelegten Schutzziele könnten gemäß *Abbildung 5* in einer Art Netzdiagramm dargestellt werden. Aus dieser Darstellung können die Schwerpunkte leicht abgelesen werden. So liegt im obigen Beispiel der Schwerpunkt auf den Schutzzielen Vertraulichkeit und Transparenz. Durch das Hinzufügen einer zusätzlichen, neutralen Ebene („0“) wird das Diagramm übersichtlicher und ermöglicht eine einfache und gut ablesbare Zuordnung der verschiedenen Schutzniveaus.

B4 – Bewertung des Risikos

Für die Bewertung der Risiken sollten die zur Umsetzung geplanten Maßnahmen mit Referenzmaßnahmen verglichen werden (*siehe Tabelle 7*). Ein solcher Katalog sollte umfangreiche Maßnahmen nennen, die zur Erreichung der jeweiligen Schutzziele, bezogen auf die drei Komponenten Daten, Systeme und Prozesse, ergriffen werden können. Probst (2012; S. 5 (443)) hat bereits eine etwas umfangreichere Liste veröffentlicht. Laut Friedewald, et al. (2016) wird auch auf Ebene der Aufsichtsbehörden bereits an solchen Referenzmaßnahmen-Katalogen gearbeitet. Ein einheitliches Sammelwerk an Maßnahmen scheint hier sinnvoll, zumal auch eine spätere Überprüfung der Aufsichtsbehörden dadurch vereinfacht werden kann. Sollte man von den Referenzmaßnahmen abweichen, sollte dies entsprechend begründet und dokumentiert werden. Da die Aktualität dieser Referenzmaßnahmen maßbeglich ist, sollten diese von den Aufsichtsbehörden erstellt und gepflegt werden.

Tabelle 7: Referenzmaßnahmen-Beispiele (Friedewald, et al. 2016; S. 28).

Schutzziel	Komponente	Maßnahmen
Verfügbarkeit	Daten	Redundanz, Schutz, Reparaturstrategie
	Systeme	Redundanz, Schutz, Reparaturstrategie
	Prozesse	Redundanz, Schutz, Reparaturstrategie
Integrität	Daten	Hash-Wert-Vergleich
	Systeme	Einschränkung von Schreibrechten, regelmäßige Integritätsprüfungen
	Prozesse	Festlegung von Minimal-/ Maximal-Referenzen, Steuerung der Regulation
Vertraulichkeit	Daten	Verschlüsselung
	Systeme	Verschlüsselung
	Prozesse	Rechte und Rollenkonzepte
Nichtverkettbarkeit	Daten	Pseudonymität, Anonymität, attributbasierte Credentials
	Systeme	Trennung (Isolierung) von Datenbeständen, Systemen und Prozessen
	Prozesse	Identity Management, Anonymitätsinfrastruktur, Audits
Transparenz	Daten	Dokumentation, Protokollierung
	Systeme	Systemdokumentation, Protokollierung von Konfigurationsänderungen
	Prozesse	Dokumentation von Verfahren, Protokollierung
Intervenierbarkeit	Daten	Zugriff auf Betroffenen-Daten durch den Betroffenen (Auskunft, Berichtigung, Sperrung, Löschung)
	Systeme	---
	Prozesse	Aus-Schalter, einheitlicher Ansprechpartner für Änderungen, Korrekturen, Löschen

Was aus den Tabellen bisher noch nicht hervorgeht, ist eine unterschiedliche Einteilung der Maßnahmen gemäß Schutzniveau. So ist es den hier aufgeführten Listen nicht zu entnehmen, ob die Maßnahme für alle Schutzniveaus (normal, hoch, sehr hoch) herangezogen werden kann, oder ob hier entsprechend der Einstufung des Schutzniveaus eventuell unterschiedliche Maßnahmen betrachtet werden sollten.
Weiter ist anzumerken, dass Maßnahmen aus dem Referenzmaßnahmen-Katalog durchaus auch zur Erfüllung mehrerer Schutzziele geeignet sind und sich nicht zwangsweise auf das Schutzziel beschränken, unter dem diese Maßnahmen aufgeführt wurden (Probst, 2012).

Abschließend sollte nach Friedewald, et al. (2016) noch eine „klassische“ Risikoanalyse durchgeführt werden, um festzustellen, „ob und mit welcher Wahrscheinlichkeit die Organisation die Datenschutzbestimmungen nicht einhalten wird (organisationsinterne

Gründe)“. Dabei sollte der Fokus darauf liegen, wie wahrscheinlich es ist, dass der Zweck der Verarbeitung geändert werden kann bzw. inwiefern hier ein Interesse bestünden könnte, ob es zu Konflikten der Informationssicherheit (für Geschäftsprozesse) und des Datenschutzes kommen kann und ob Daten in Drittländern mit evtl. weniger Rechtssicherheit verarbeitet werden.

5.2.3 Berichts- und Maßnahmenphase

C1 – Identifikation passender Schutzmaßnahmen

Entsprechend der Ergebnisse aus *Unterabschnitt 5.2.2*, sollten nun die entsprechenden Maßnahmen identifiziert werden, die zur Erreichung der Schutzziele umgesetzt werden sollen. Hierbei kann wiederum der Referenzmaßnahmenkatalog (vgl. Probst, 2012; S. 5 (443)) herangezogen werden, um geeignete Maßnahmen zu finden (Friedewald, et al. 2016).

C2 – Dokumentation der Bewertungsergebnisse nach einheitlichem Muster

Die Dokumentation der Ergebnisse ist ein wichtiger Schritt der DSFA. Zum einen ist die Dokumentation wichtig für die Überprüfung der DSFA, um festzustellen, ob diese gemäß den Anforderungen durchgeführt wurde und zum anderen sollte sie dazu dienen, die Ergebnisse im Sinne der Transparenz zugänglich zu machen (Friedewald, et al. 2016).

Dabei sollte wie bereits beim Vorbereitungsbericht ein einheitliches Muster verwendet werden. Dies soll die Prüfung der Aufsichtsbehörden erleichtern und soll auch ermöglichen, dass die Ergebnisse mit den Ergebnissen anderer DSFA verglichen werden können (Friedewald, et al. 2016). Wie genau solch eine standardisierte Dokumentation aussehen könnte, wird nicht weiter erwähnt. Hier wäre es wieder sinnvoll, ein vorgegebenes Muster der Aufsichtsbehörden heranzuziehen, sofern verfügbar.

C3 – Veröffentlichung des DSFA-Berichts

Der DSFA-Bericht sollte anschließend öffentlich zugänglich gemacht werden. Dies wird gemäß DSGVO zwar nicht explizit gefordert, sollte im Sinne der Transparenz jedoch gemacht werden (Friedewald, et al. 2016). Auch in anderen Ländern ist dies bereits Bestandteil einer DSFA. So drängen auch die „Best-Practice-Handbücher“ der ICO und CNIL dazu, die DSFA im Sinne der Transparenz anschließend zu veröffentlichen (ICO, 2014 & CNIL, 2015a).

C4 – Implementierung von Schutzmaßnahmen

Für die Implementierung der bereits identifizierten Maßnahmen eignet sich ein Maßnahmenplan, wie bereits von anderen risikobasierten Verfahren bekannt. Ein Maßnahmenplan nach Friedewald, et al. (2016) könnte beispielsweise, wie in *Tabelle 8* dargestellt, aussehen.

Tabelle 8: Beispiel eines Maßnahmenplans in Anlehnung an Friedewald, et al. (2016). (Erstellt von dem Verfasser, 2016).

Projekt:			**Datum:**		
			Ersteller:		
Maßnahme	**Schutzziele**	**Verantwortliche**	**Ressourcen**	**Umsetzung bis…**	**Prüfmethode**
…	…	…	…	…	…
…	…	…	…	…	…
…	…	…	…	…	…

Dies könnte ein Beispiel für einen Maßnahmenplan sein, wie er mindestens aussehen sollte. Entsprechend kann dieser Plan den Vorstellungen der jeweiligen Organisation angepasst werden, wobei die hier integrierten Kriterien als eine Art Mindeststandard erhalten bleiben sollten.

C5 – Unabhängige Prüfung der DSFA-Ergebnisse

Eine unabhängige Überprüfung des DSFA-Berichts durch eine unabhängige Stelle sollte gemäß Friedewald, et al. (2016) durchgeführt werden. Dabei soll vor allem sichergestellt werden, dass

- *„angemessen mit Interessenkonflikten umgegangen wurde,*
- *die Interessen der Betroffenen bei der Risikobewertung und der Auswahl von Schutzmaßnahmen in ausreichendem Umfang berücksichtigt wurden,*
- *die Öffentlichkeit in ausreichendem Umfang über die Ergebnisse der DSFA informiert wird und*
- *die Implementierung der vorgeschlagenen Schutzmaßnahmen tatsächlich in Angriff genommen wurde.“ (Friedewald, et al. 2016; S. 33)*

Nach Abschluss der DSFA sollte darauf geachtet werden, dass der Prozess evtl. erneut durchgeführt werden muss. Je nach Veränderung des Systems oder der Weiterentwicklung von Technik kann es erforderlich sein, den Prozess zu wiederholen, um neuen Anforderungen gerecht zu werden und sicherzustellen, dass auch während der restlichen Lebenszeit das Risiko für die Betroffenen berücksichtigt wird und die Maßnahmen diesem Risiko weiterhin gerecht werden (Friedewald, et al. 2016).

5.3 *Beispiel*: Wie eine DSFA aussehen könnte

Mit der DSGVO wird erstmals von dem Verantwortlichen verlangt, eine Risikobetrachtung für Datenschutzbelange durchzuführen. Zwar sind die bisherigen TO-Maßnahmen in der Arztpraxis auf die Verhältnismäßigkeit angepasst, allerdings wurde eine Risikobetrachtung in der nun geforderten Weise noch nie durchgeführt. Bisher gibt es auch noch keine offiziell empfohlene Vorgehensweise, wie eine solche Betrachtung aussehen kann. Um den Anforderungen der DSGVO gerecht zu werden, entscheidet sich der Verantwortliche eine DSFA gemäß der Empfehlungen von Friedewald, et al. (2016) durchzuführen.
Im Folgenden soll der Ablauf einer DSFA aufgezeigt werden, wie er in der Praxis aussehen könnte. Vor allem bei der Identifizierung spezifischer TO-Maßnahmen sollen hierbei lediglich einige Maßnahmen beispielhaft aufgezeigt werden. Auch die Dokumentation der DSFA soll nur beispielhaft beschrieben werden.

Vorbereitungsphase

Um festzustellen, ob eine DSFA für die Arztpraxis überhaupt vorgeschrieben ist, wirft der Verantwortliche einen Blick in die DSGVO. Dort wird in Art. 35 definiert, wann eine DSFA gefordert ist, und wann nicht. Aufgrund des hohen Risikos, dass von der Verarbeitung der Gesundheitsdaten in der Arztpraxis ausgeht und es sich um eine Verarbeitung besonderer Kategorien von personenbezogenen Daten handelt, ist eine DSFA in diesem Fall erforderlich (vgl. Art. 35 Abs. 3 lit. b DSGVO).
Für die Erarbeitung der DSFA soll den Verantwortlichen der IT-Administrator, sowie seine Ärztekollegen unterstützen. Der Datenschutzbeauftragte steht dabei ebenfalls beratend zur Verfügung. Dabei erfüllt er zugleich die Anforderungen der DSGVO (vgl. Art. 35 Abs. 2 DSGVO).
Ziel der DSFA soll die Konformität mit der DSGVO sein. Es wird vereinbart eine Standard-DSFA durchzuführen, mit dem Ziel die Daten der Betroffenen ausreichend zu schützen.
Das Team legt zudem fest, was für die DSFA betrachtet werden soll. Es sollen zum einen die technischen Systeme und IT-Anlagen berücksichtigt werden, genauso wie die Daten und ihre Formate. Auch organisatorische Faktoren werden dabei berücksichtigt, wie die Zwecke, weshalb die Daten verarbeitet werden und die damit zusammenhängenden Prozesse. Durch die Einbindung der eigentlichen Datenverarbeitung in ein kontextbezogenes Umfeld wird aus der Standard-DSFA gleichzeitig auch eine konkrete DSFA.
Für die DSFA von Bedeutung sind die in *Tabelle 9* zu findenden Akteure.

Tabelle 9: Bei der DSFA betrachtete Akteure am Beispiel Arztpraxis. (Erstellt von dem Verfasser, 2016).

Akteure	Interesse
Hersteller von Technologien und Verfahren	Die Hersteller könnten Interesse an statistischen Daten haben um ihre Systeme zu verbessern.
Auftragsverarbeiter	N/A
Mitarbeiter der Arztpraxis	Müssen Zugriff auf alle Daten haben um den Geschäftsprozess aufrecht zu erhalten.
Patienten	Wollen nicht, dass ihre Daten von unberechtigten Personen eingesehen werden können.
Dritte (z.B.: Personen die zufällig Kenntnis von personenbezogenen Daten erhalten)	Dritte könnten von den Daten profitieren, da sie für unrechtmäßige Zwecke verwendet werden könnten.

Zusätzlich zur DSGVO müssen für die Arztpraxis auch noch weitere nationale Gesetze berücksichtigt werden, die sich auf die Berufsausübung der Ärzte erstrecken und ggf. Regelungen beinhalten, wie beispielsweise Umgang mit Patientenakten (beispielsweise § 203, Strafgesetzbuch [StGB], 2016). Es ist ebenfalls zu berücksichtigen, dass möglicherweise nationale Gesetze zusätzlich zur DSGVO erlassen werden, um die im Erwägungsgrund 53 der DSGVO genannten Punkte zu spezifizieren.

Bewertungsphase

Nachdem die Grundlagen der DSFA definiert wurden, muss das Team nun die Bewertung des Risikos durchführen. Dazu werden zunächst die möglichen Angreifer und deren Motive identifiziert (*siehe Tabelle 10*).

Tabelle 10: Mögliche Angreifer und deren Motive am Beispiel Arztpraxis. (Erstellt von dem Verfasser, 2016).

Mögliche Angreifer		Motive
Staatliche Stellen:	▪ Polizeibehörden ▪ Geheimdienste	▪ Unfalluntersuchungen etc. ▪ Informationen über interessante Personen
Unternehmen:	▪ Versicherungen ▪ Arbeitgeber ▪ Adress- und Datenhandel ▪ (Wirtschaftsauskunfteien) ▪ (Marktforschung)	▪ Versicherungsbetrug ▪ Informationen über Arbeitnehmer ▪ Handel mit Daten zur Umsatzgenerierung
Gesundheitswesen:	▪ Krankenhäuser ▪ Arztpraxen	▪ Wiederrechtliche Beschaffung von Patientendaten
Forschung:	▪ Medizinforschung	▪ Informationen über Studienteilnehmer

Anhand der Bedrohungen bewertet das Team nun die Schutzziele. Die Bewertung wird anhand der von Friedewald, et al. (2016) empfohlenen Klassifizierung durchgeführt. Das Schutzniveau ist dabei abhängig davon, welche Verletzung des jeweiligen Schutzniveaus den größten Schaden für den Betroffenen hätte. Im Falle der Arztpraxis einigt sich das Team den Schwerpunkt auf den Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität zu setzen. Also auf den traditionellen Schutzzielen der Informationssicherheit. Die Schutzziele werden entsprechend der Klassifizierung nach Friedewald, et al. (2016) jeweils als hoch eingestuft. *Abbildung 6* soll die Einstufung des Schutzniveaus der einzelnen Schutzziele verdeutlichen.

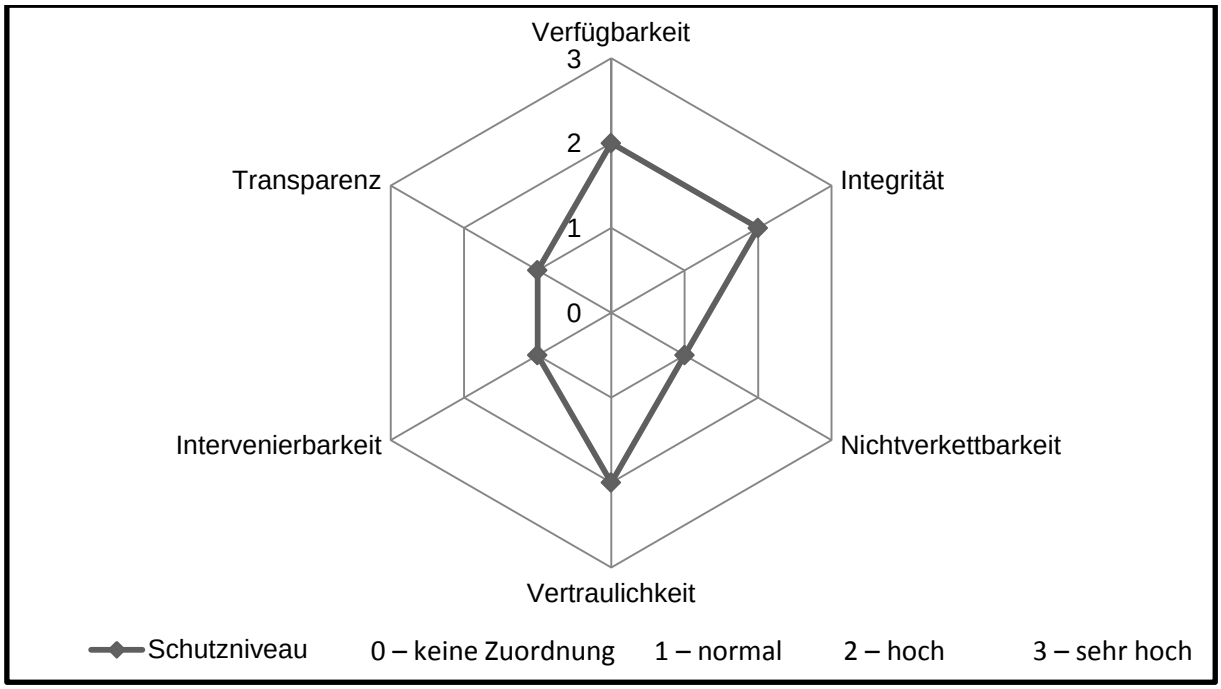

Abbildung 6: Schutzniveaueinstufung am Beispiel Arztpraxis (eigene Darstellung, 2016).

Um den Schutzzielen Rechnung zu tragen vergleicht das Team nun die bereits implementierten TO-Maßnahmen mit den Referenzmaßnahmen (vgl. Probst, 2012; S. 5 (443)). Bei dem Vergleich stellt das Team fest, dass die TO-Maßnahmen die Verfügbarkeit und Vertraulichkeit noch nicht ausreichend gewährleisten. An dieser Stelle müssen weitere TO-Maßnahmen ergriffen werden, um dem hohen Schutzniveau gerecht zu werden.

Berichts- und Maßnahmenphase

Im Nächsten Schritt identifiziert das Team Maßnahmen, die zusätzlich zu den bereits bestehenden TO-Maßnahmen ergriffen werden müssen. Wie bereits festgestellt müssen weitere Maßnahmen in Bezug auf die Verfügbarkeit und die Vertraulichkeit getroffen werden. Diese Maßnahmen werden in einen Maßnahmenkatalog aufgenommen (*siehe Tabelle 11*), anhand dessen die Umsetzung der Maßnahmen durchgeführt werden kann.

Tabelle 11: Auszug aus dem Maßnahmenkatalog der zu implementierenden Maßnahmen am Beispiel Arztpraxis. (Erstellt von dem Verfasser, 2016).

Projekt:	Standard-DSFA Arztpraxis (beispielhafter Auszug)		**Datum:**	10.06.2016
			Ersteller:	Chefarzt
Maßnahme	**Schutzziele**	**Ebene**	**Umsetzung durch…**	**Prüfmethode**
Backup der Daten	Verfügbarkeit	Daten	IT-Admin	▪ Prüfung der Datensicherungen auf Fehler (quartalsweise)
Schutz vor Schadsoftware	Verfügbarkeit	Daten	IT-Admin	▪ Aktualisierungen (täglich) ▪ on-Demand Scans (quartalsweise)
Hardwareredundanz	Verfügbarkeit	Systeme	IT-Admin Chefarzt	▪ Prüfung der Funktionsfähigkeit aller Hardwarekomponenten (quartalsweise)
Ausweichprozesse	Verfügbarkeit	Prozesse	Chefarzt	▪ Prüfung der Ausweichprozesse (quartalsweise)
Verschlüsselung auf Systemebene	Vertraulichkeit	Systeme	IT-Admin	▪ Penetrationstests (jährlich)
Verschwiegenheits-vereinbarungen	Vertraulichkeit	Prozesse	Chefarzt	▪ Kontrolle interner Vereinbarung auf deren Aktualität und Vorhandensein (quartalsweise)
Geeignete Organisation bei der Vergabe von Zugriffsrechten („need-to-know“)	Vertraulichkeit	Prozesse	Chefarzt	▪ Kontrolle interner Rechtevergabe auf deren Aktualität und Vorhandensein (quartalsweise)

Bei der Betrachtung dieses Beispiels wurde die Ressourcenverteilung unbeachtet gelassen und stattdessen die Anwendungsebene hinzugefügt, auf die sich die zu integrierenden Maßnahmen beziehen.

Die Ergebnisse der DSFA werden anschließend durch den IT-Administrator auf der Website der Arztpraxis veröffentlicht.

Abschließend wird die DSFA in einem Audit-Verfahren einer unabhängigen Prüfung unterzogen, um festzustellen ob die Ergebnisse und die Vorgehensweise den Anforderungen entsprechen. Diese Prüfung wird im Fall der Arztpraxis von einem Dienstleistungsunternehmen durchgeführt.

6 Konsequenzen für Unternehmen

Mit Blick auf die in den *Kapiteln 3-5* beschriebenen Anforderungen an die TO-Maßnahmen gemäß DSGVO wird sich für Unternehmen vor allem die Vorgehensweise ändern. Der Fokus wird eindeutig im Bereich der risikobasierten Maßnahmenergreifung liegen. Die Prinzipien von PbD und der DSFA sind zwar nicht neu, aber sie sind zum ersten Mal Bestandteil von EU-Recht und somit auch in Deutschland zum ersten Mal rechtskräftig vorgeschrieben. Entsprechend sind die TO-Maßnahmen nicht mehr nur eine Liste verschiedener Kontrollmaßnahmen, sondern sie sind noch stärker an andere Anforderungen geknüpft als es bisher im BDSG der Fall war. Zwar sind die Anforderungen an die TO-Maßnahmen grundsätzlich allgemeiner gehalten, aufgrund der Implementierung von PbD und DSFA jedoch scheint der Prozess zur Implementierung von geeigneten TO-Maßnahmen umfangreicher. Durch die zusätzlichen Änderungen bei der Vergabe von Geldbußen sollte es zudem zukünftig noch stärker im Interesse des Verantwortlichen liegen, den Anforderungen der DSGVO nachzukommen. So können Verletzungen der Art. 25 (PbD), 32 (Sicherheit der Verarbeitung) und 35 (DSFA) bis zu 10 Millionen Euro, bzw. bis zu 2% des weltweiten Jahresumsatzes des Unternehmens Strafe nach sich ziehen (DSGVO, 2016).

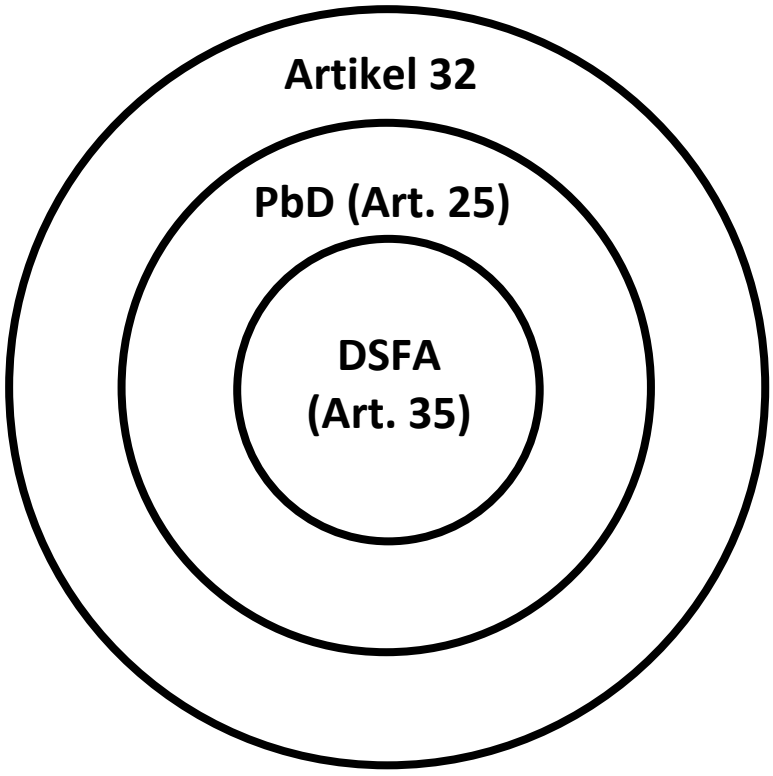

Abbildung 7: TO-Maßnahmen in der DSGVO (eigene Darstellung, 2016).

Abbildung 7 soll den Zusammenhang der relevanten Artikel zur Umsetzung der TO-Maßnahmen verdeutlichen. Kern zur Umsetzung der TO-Maßnahmen ist dabei die DSFA. Sie ist Grundlage zur Erfüllung der nach Art. 25 und Art. 32 geforderten Maßnahmen. Auch wenn eine DSFA letztendlich nicht gefordert ist, so ist doch bereits eine gewisse Risikoabschätzung notwendig, um zu diesem Ergebnis zu kommen (*siehe Unterabschnitt 5.2.1*). Dies stellt einen wesentlichen Unterschied zum BDSG dar. Während im BDSG zur Umsetzung der TO-Maßnahmen lediglich die in § 9 (inklusive Anlage) geforderten Maßnahmen umgesetzt werden mussten, ist nun die in Art. 35 geforderte DSFA ausschlaggebend für die Umsetzung geeigneter TO-Maßnahmen (vgl. Erwägungsgrund 84). Aufbauend auf die DSFA muss anschließend dem Prinzip PbD Rechnung getragen und gemäß Art. 25 umgesetzt werden (vgl. Erwägungsgrund 78). Letztendlich wird der Prozess durch die Vorgaben in Art. 32 komplementiert. Somit stellt der Artikel mit den eigentlichen TO-Maßnahmen (Art. 32) nicht den Kern zur Findung geeigneter TO-Maßnahmen dar. Stattdessen müssen zuvor die Art. 35 und 25 berücksichtigt werden. Unternehmen sollten diese Zusammenhänge entsprechend bei der Implementierung zukünftiger TO-Maßnahmen berücksichtigen. Die alleinige Implementierung von PETs ist genauso wirkungslos wie eine reine DSFA. Erst durch die Kombination der verschiedenen Prinzipien und Methoden wird ein ganzheitliches Datenschutzniveau erreicht. Eine genaue Trennung der einzelnen Prinzipien und Methoden kann jedoch nur sehr schwer vorgenommen werden. Aufgrund der sehr generellen Formulierungen sind die Übergänge der einzelnen Anforderungen recht fließend. So ist im Grunde nicht eindeutig festzustellen, wo die DSFA aufhört und PbD anfängt. Bereits während der DSFA (bei der Identifikation des Risikos und der Festlegung geeigneter Maßnahmen) wird auch dem Prinzip PbD Rechnung getragen.

Unternehmen sollten sich auch die neue Terminologie der DSGVO aneignen, die sich in einigen Punkten von der Terminologie des BDSG unterscheidet. Vor allem in Bezug auf die Begriffe „Zugang“, „Zutritt“ und „Zugriff“ dürfen die verschiedenen Bedeutungen nicht mit der neuen Terminologie der DSGVO durcheinander gebracht werden (*siehe Abschnitt 3.3*).

Zuletzt sollten auch die in *Unterabschnitt 3.2.3* genannten neuen Anforderungen gemäß Art. 32 beachtet werden. Im Vergleich zum BDSG werden durch die DSGVO auch zum ersten Mal Anforderungen an die Systeme selbst gestellt. So wird in Zukunft nicht nur der Schutz der Daten an sich eine Rolle spielen, sondern auch der Schutz der mit der Verarbeitung zusammenhängenden Systeme. Ebenso muss zukünftig die Forderung nach einer Wirksamkeitskontrolle beachtet werden. Die reine Implementierung der TO-Maßnahmen

und deren Dokumentation sind nicht mehr ausreichend. Zusätzlich muss auch die Wirksamkeit der Maßnahmen regelmäßig geprüft und nachgewiesen werden können.

Wie die Umsetzung der hier vorgestellten Anforderungen chronologisch vorgenommen werden sollte, soll im folgenden Abschnitt noch einmal kurz verdeutlicht werden, wobei die einzelnen Schritte in der optimalen Reihenfolge kurz wiederholt werden sollen.

6.1 Vorgehen bei der Umsetzung von TO-Maßnahmen

Zur Überprüfung, ob bestehende TO-Maßnahmen eines Datenverarbeitungsverfahrens ausreichend sind, bei der Erarbeitung von TO-Maßnahmen für ein neues Datenverarbeitungsverfahren oder bei der Integration neuer Technologien in ein bestehendes Datenverarbeitungsverfahren sollten folgende Schritte unternommen werden:

Schritt 1 – Durchführung einer DSFA (*siehe Abschnitt 5.2*)

1.1 Ist eine DSFA notwendig?

1.2 Zusammenstellung eines Teams

1.3 Betrachtungsgegenstand festlegen

1.4 Akteure identifizieren

1.5 Rechtsgrundlagen berücksichtigen (ggf. zusätzliches nationales Recht)

1.6 Schutzziele definieren

1.7 Angreifer und Angriffsszenarien identifizieren

1.8 Risiko bewerten (Vergleich mit Referenzmaßnahmen)

1.9 Maßnahmen festlegen

1.10 Ergebnis dokumentieren

1.11 Maßnahmen umsetzen

1.12 Unabhängige Prüfung der Ergebnisse

Schritt 2 – Umsetzung von PbD (*siehe Abschnitt 4.3*)

a) Wenn eine DSFA vorgeschrieben ist

2.A.1 DSFA bildet bereits Grundlage zur Umsetzung von PbD (Schritt 1.1 – 1.8) (Danezis, et al. 2014)

2.A.2 Welche Strategien werden durch Ergebnis der DSFA bereits erfüllt?

2.A.3 Welche Strategien müssen zusätzlich noch berücksichtigt werden?

2.A.4 Wo müssen ggf. noch Anpassungen durchgeführt werden?

2.A.5 Ergebnisse sollten ggf. in Schritt 1.9 der DSFA ergänzt werden (Danezis, et al. 2014)

2.A.6 PbD in Unternehmensabläufen integrieren bzw. verankern

b) Wenn eine DSFA nicht vorgeschrieben ist

2.B.1 Auch ohne DSFA müssen die Risiken entsprechend berücksichtigt werden

2.B.2 Umsetzung der Strategien zur Wahrung der Datenschutzgrundsätze

2.B.3 Welche TO-Maßnahmen müssen ergriffen werden?

2.B.4 Wie können die geforderten TO-Maßnahmen umgesetzt werden?

2.B.5 PbD in Unternehmensabläufe integrieren bzw. verankern

Schritt 3 – Implementierung von Maßnahmen gemäß Artikel 32 (*siehe Kapitel 3*)

a) Wenn eine DSFA vorgeschrieben ist

3.A.1 Überprüfen, ob die Ergebnisse auch alle in Art. 32 DSGVO geforderten Maßnahmen erfüllen

3.A.2 Zusätzliche Maßnahmen ggf. umsetzen und in DSFA integrieren

b) Wenn eine DSFA nicht vorgeschrieben ist

3.B.1 Überprüfen, ob die Maßnahmen zur Erfüllung der Strategien von PbD bereits alle in Art. 32 DSGVO geforderten Maßnahmen erfüllen

3.B.2 Zusätzliche Maßnahmen gemäß Art. 32 DSGVO ggf. umsetzen

Werden diese Schritte in der hier dargelegten Reihenfolge durchlaufen und ordnungsgemäß bearbeitet, so sind allen Anforderungen an TO-Maßnahmen gemäß DSGVO Rechnung getragen. Diese Liste, inklusive der wichtigsten Punkte der verschiedenen Schritte, kann in *Anhang A: Checkliste zur Umsetzung von TO-Maßnahmen gemäß DSGVO* nachgeschlagen werden. Anhand der Checkliste kann Schritt für Schritt verfolgt werden, ob die jeweiligen Schritte ordnungsgemäß berücksichtigt wurden und ob das Verfahren zur Umsetzung von TO-Maßnahmen nach DSGVO verstanden wurde.

6.2 Zusammenführung der *Beispiele*

Bei einer separaten Betrachtet der Beispiele der jeweiligen Kapitel fällt auf, dass diese sich in einigen Punkten überschneiden. So wird beispielsweise sowohl nach Art. 32 eine Verschlüsselung gefordert, als auch gemäß den Strategien zur Umsetzung von PbD. Auch bei

der DSFA sind Verschlüsselungsverfahren erneut Bestandteil der zu ergreifenden Maßnahmen. Daraus folgt, dass die einzelnen Artikel nicht als isolierter Prozess gesehen werden dürfen. Viel mehr sind die verschiedenen Anforderungen der DSGVO eng miteinander verbunden.

Um den Anforderungen der DSGVO gerecht zu werden, ist es für die Arztpraxis ratsam die jeweiligen Anforderungen der Art. 25, 32 und 35 nicht isoliert zu betrachten, sondern gemäß der in *Abschnitt 6.1* vorgestellten Reihenfolge vorzugehen. Zu Beginn sollte der Verantwortliche mit der Erstellung einer DSFA beginnen. Diese kann wie in *Abschnitt 5.3* geschildert durchgeführt werden, wobei das gesamte System, inklusive aller bereits getroffenen TO-Maßnahmen mit aufgenommen werden sollte. Am Ende der DSFA sollten dann bereits Maßnahmen in einen Maßnahmenkatalog aufgenommen worden sein, die es umzusetzen gilt. Aufbauend auf diesen Ergebnissen sollte die Konformität mit dem Prinzip PbD untersucht werden. Hierzu kann ebenfalls wieder wie in *Abschnitt 4.4* beschrieben verfahren werden. An diesem Punkt ist zu erwarten, dass bereits viele der Strategien zur Umsetzung von PbD erfüllt sind. Entsprechend wird es darum gehen, möglicherweise noch offene Lücken zu isolieren und rückwirkend mit in die DSFA aufzunehmen bzw. im bereits bestehenden Maßnahmenkatalog zu ergänzen. Anstatt eine separate Dokumentation zu erstellen, empfiehlt es sich die Ergebnisse von PbD in die Dokumentation der DSFA mitaufzunehmen. Abschließend sollte dann sichergestellt werden, dass alle in Art. 32 genannten Anforderungen und Maßnahmen durch die bereits durchgeführte Betrachtung erfasst und berücksichtigt wurden. Ist dies nicht der Fall, muss auch an dieser Stelle die DSFA bzw. der Maßnahmenkatalog rückwirkend vervollständigt werden.

Werden diese Schritte ordnungsgemäß durchgeführt, kann der Verantwortliche davon ausgehen, dass den Anforderungen der neuen Rechtsvorschrift Rechnung getragen ist und die Daten in der Arztpraxis entsprechend gut geschützt sind.

7 Ausblick

Es ist zu erwarten, dass sich noch einiges in Bezug auf die DSGVO ergeben wird. Vor allem bis zu ihrem Gelten im Jahre 2018. Bis dahin müssen alle Anforderungen umgesetzt werden, was auch die TO-Maßnahmen beinhaltet. Vermutlich werden in der Zwischenzeit verschiedene Behörden bzw. Institutionen auf Landes-, Bundes- oder EU-Ebene Hilfestellungen bieten, auch in Bezug auf die TO-Maßnahmen. Gerade mit Blick auf die DSFA ist zu erwarten, dass es hier weitere, detailliertere Empfehlungen geben wird, die bei der Umsetzung helfen werden. Wünschenswert wäre es, wenn vor allem auf EU-Ebene Handlungsempfehlungen erlassen werden, die direkt auf die DSGVO angepasst sind und letztendlich ein einheitliches Vorgehen sicherstellen, dass von allen Mitgliedstaaten gleichermaßen übernommen werden kann.

Allgemein ist zu hoffen, dass die EU durch zusätzliche Veröffentlichungen einige der doch sehr generischen Vorschriften weiter spezifiziert. Mit Blick auf die TO-Maßnahmen wäre es wünschenswert gewesen, wenn bereits in der DSGVO spezifischere Anforderungen integriert worden wären. So bleibt trotz intensiver Befassung mit dem Thema immer noch ein unsicherer Nachgeschmack zurück. Sofern nicht die EU selbst Empfehlungen darüber macht, wie die Verfahren, wie zum Beispiel die DSFA, auszusehen haben, muss immer mit einem gewissen Maß an Rechtsunsicherheit gerechnet werden. Fehlen einem Unternehmen die Mittel, um zusätzliche Maßnahmen zu ergreifen, so wird es schwer fallen, die Grenze zwischen dringend geforderten und erwünschten Maßnahmen zu ziehen.

Gerade für kleinere und mittelständische Unternehmen (KMU) kann es ggf. sehr aufwendig sein, die Anforderungen, wie das Durchführen einer DSFA, selbst durchzuführen. Es ist gut vorstellbar, dass sich hier ein Markt eröffnet, sodass die Durchführung von DSFA von Dienstleistungsunternehmen übernommen werden. Dies bedeutet vor allem für KMU, dass Datenschutz künftig noch stärker zum finanziellen Aspekt wird. Andererseits können so Kompetenzen eingekauft werden und man läuft weniger Gefahr, dass die Anforderungen nicht eingehalten werden oder nur unzureichend erfüllt werden. Inwiefern die Aufsichtsbehörden oder EU-Institutionen hier Unterstützung vor allem für KMU bieten wird sich zeigen. Letztendlich wird es aber in der Verantwortung der Unternehmen liegen, die Anforderungen ordnungsgemäß zu erfüllen.

Allgemein betrachtet können die neuen TO-Maßnahmen allerdings als Zugewinn gesehen werden, die bei ordentlicher Implementierung mehr Datenschutz bedeuten können.

Literaturverzeichnis

BfDI Datenschutz WIKI (ohne Datum). *Technische und organisatorische Maßnahmen*. [Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – Online Wiki]. Zugriff am 18. Mai 2016 unter https://www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Maßnahmen

Bundesdatenschutzgesetz [BDSG]. Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66). Zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814).

Cavoukian, A. (2011). *Privacy by Design – The 7 Foundational Principles*. Information & Privacy Commissioner Ontario, Canada.

Cavoukian, A., & Prosch, M. (2010). *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*. In: A. Cavoukian, *Privacy by Design – From Rhetoric to Reality*. Sammelwerk (S. 101 – 129). Ontario: Information & Privacy Commissioner of Ontario.

Commission Nationale de l'Informatique et des Libertés [CNIL]. (2012). *Measures for the Privacy Risk Treatment*. [Veröffentlichung der französischen Behörde für Datenschutz und Informationsfreiheit].

Commission Nationale de l'Informatique et des Libertés [CNIL]. (2015a). *Privacy Impact Assessment: Methodology (how to carry out a PIA)*. [Veröffentlichung der französischen Behörde für Datenschutz und Informationsfreiheit].

Commission Nationale de l'Informatique et des Libertés [CNIL]. (2015b). *Privacy Impact Assessment: Tools (templates and knowledge bases)*. [Veröffentlichung der französischen Behörde für Datenschutz und Informationsfreiheit].

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R. & Schiffner, S. (2014). *Privacy and Data Protection by Design – from policy to engineering*. [European Union Agency for Network and Information Security (ENISA)].

Friedewald, M., Obersteller, H., Nebel, M., Bieker, F., Rost, M. (2016). *Datenschutz-Folgenabschätzung*. Ein Werkzeug für einen besseren Datenschutz. [White Paper des Fraunhofer-Instituts für System- und Innovationsforschung ISI].

Hoepman, J.-H. (2013, 6. Mai). *Privacy Design Strategies*. [eprint arXiv:1210.6621].

Information Commissioner's Office [ICO]. (2014). *Conducting privacy impact assessments code of practice*. [Veröffentlichung der britischen Datenschutzaufsichtsbehörde].

ISO/IEC 29100. (2011). ISO/IEC 29100:2011(E) Information technology — Security techniques — Privacy framework. [First edition 2011-12-15]. Genf: International Organization for Standardization.

Probst, T. (2012). *Generische Schutzmaßnahmen für Datenschutz-Schutzziele*. DuD – Datenschutz und Datensicherheit, Volume 36, Issue 6, 439-444.

Regulation (EU) 2016/679 [GDPR]: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Richtlinie 95/46/EG: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24 . Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Rost, M. & Bock, K. (2011). *Privacy By Design und die Neuen Schutzziele*. DuD – Datenschutz und Datensicherheit, Volume 35, Issue 1, 30-35.

Strafgesetzbuch [StGB]: Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322). Zuletzt geändert durch Artikel 1 des Gesetzes vom 30. Mai 2016 (BGBl. I S. 1254).

Verordnung (EU) 2016/679 [DSGVO]: Verordnung (EU) 2016/679 des Europäischen Parlaments und des 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).

Vertrag über die Arbeitsweise der Europäischen Union [AEUV]: Vertrag über die Arbeitsweise der Europäischen Union (Konsolidierte Fassung) vom 26. Oktober 2012.

Anhang

Anhang A: Checkliste zur Umsetzung von TO-Maßnahmen gemäß DSGVO

Tabelle 12: Checkliste zur Umsetzung von TO-Maßnahmen gemäß DSGVO. (Erstellt von dem Verfasser, 2016).

Checkliste zur Umsetzung von TO-Maßnahmen gemäß EU-DSGVO			
Schritt 1 – Durchführung einer DSFA		*JA*	*NEIN*
1.1	Ist eine DSFA notwendig?	☐	☐
	Fall 1: hohes Risiko für die Rechte und Freiheiten natürlicher Personen Fall 2: systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen Fall 3: umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 Fall 4: umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 Fall 5: systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche Fall 6: Vorgabe durch Aufsichtsbehörde			
1.2	Zusammenstellung eines Teams	☐	☐
1.3	Betrachtungsgegenstand festlegen	☐	☐
	Was wird betrachtet? ▪ Zweck ▪ Kontext ▪ Daten (inklusive deren Formate und verwendeten Protokolle) ▪ IT-Systeme (inklusive Schnittstellen) ▪ Prozesse DSFA-Typ wählen: ▪ Marketing-DSFA ▪ Standard-DSFA ▪ Wissenschaftliche-DSFA ▪ konkrete DSFA ▪ generische DSFA		
1.4	Akteure identifizieren	☐	☐
	▪ Hersteller von Technologien und Verfahren ▪ Auftragsverarbeiter ▪ Mitarbeiter des Verantwortlichen ▪ Betroffene Personen (Kunden, Patienten, Bürger,…) ▪ Dritte (z.B.: Sicherheitsbehörden oder Personen die zufällig Kenntnis von personenbezogenen Daten erhalten)		
1.5	Rechtsgrundlagen berücksichtigen (ggf. zusätzliches nationales Recht)	☐	☐
1.6	Schutzziele definieren	☐	☐
	▪ Verfügbarkeit ▪ Integrität ▪ Vertraulichkeit ▪ Transparenz ▪ Nichtverkettbarkeit ▪ Intervenierbarkeit		

1.7	Angreifer und Angriffsszenarien identifizieren	☐	☐
1.8	Risiko bewerten (Vergleich mit Referenzmaßnahmen)	☐	☐
1.9	Maßnahmen festlegen	☐	☐
1.10	Ergebnis dokumentieren	☐	☐
1.11	Maßnahmen umsetzen	☐	☐
1.12	Unabhängige Prüfung der Ergebnisse	☐	☐
Schritt 2 – Umsetzung von PbD			
a)	*Wenn eine DSFA vorgeschrieben ist (DSFA bildet Grundlage)*		
2.A.1	Welche Strategien werden durch Ergebnis der DSFA bereits erfüllt?	☐	☐
	▪ Minimise ▪ Inform ▪ Hide ▪ Control ▪ Separate ▪ Enforce ▪ Aggregate ▪ Demonstrate		
2.A.2	Welche Strategien müssen zusätzlich noch berücksichtigt werden?	☐	☐
2.A.3	Wo müssen ggf. noch Anpassungen durchgeführt werden?	☐	☐
2.A.4	Ergebnisse sollten ggf. in Schritt 1.9 der DSFA ergänzt werden	☐	☐
2.A.5	PbD in Unternehmensabläufen integrieren bzw. verankern	☐	☐
b)	*Wenn eine DSFA nicht vorgeschrieben ist*		
2.B.1	Risiken auch ohne vorherige DSFA berücksichtigen	☐	☐
2.B.2	Umsetzung der Strategien zur Wahrung der Datenschutzgrundsätze	☐	☐
	▪ Minimise ▪ Inform ▪ Hide ▪ Control ▪ Separate ▪ Enforce ▪ Aggregate ▪ Demonstrate		
2.B.3	Welche TO-Maßnahmen müssen ergriffen werden?	☐	☐
2.B.4	Wie können die geforderten TO-Maßnahmen umgesetzt werden?	☐	☐
2.B.5	PbD in Unternehmensabläufe integrieren bzw. verankern	☐	☐
Schritt 3 – Implementierung von Maßnahmen gemäß Artikel 32			
c)	*Wenn eine DSFA vorgeschrieben ist*		
3.A.1	Erfüllen Ergebnisse auch alle in Art. 32 geforderten Maßnahmen?	☐	☐
	Vor allem: (neu) ▪ Vertraulichkeit, Integrität, Verfügbarkeit der Systeme ▪ Wirksamkeitsüberprüfung der TO-Maßnahmen		
3.A.2	Zusätzliche Maßnahmen ggf. umsetzen und in DSFA integrieren	☐	☐
d)	*Wenn eine DSFA nicht vorgeschrieben ist*		
3.B.1	Erfüllen Maßnahmen von Schritt 2.B.3 bereits alle in Art. 32 geforderten Maßnahmen?	☐	☐
	Vor allem: (neu) ▪ Vertraulichkeit, Integrität, Verfügbarkeit der Systeme ▪ Wirksamkeitsüberprüfung der TO-Maßnahmen		
3.B.2	Zusätzliche Maßnahmen gemäß Art. 32 ggf. umsetzen	☐	☐