Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Tobias Malte Kretzmann

Analyse und Implementierung eines Datenschutzmanagementsystems (DSMS) gemäß Datenschutz-Grundverordnung (DSGVO) in ein bestehendes Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 am Beispiel eines mittelständischen Unternehmens

Fakultät Medizintechnik
Department Life Sciences

Tobias Malte Kretzmann

Analyse und Implementierung eines Datenschutzmanagementsystems (DSMS) gemäß Datenschutz-Grundverordnung (DSGVO) in ein bestehendes Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 am Beispiel eines mittelständischen Unternehmens

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Gefahrenabwehr / Hazard Control
am Department Medizintechnik
der Fakultät Life Sciences
der Hochschule für Angewandte Wissenschaften Hamburg

in Zusammenarbeit mit:

ANMATHO AG

[redacted]

[redacted]

Erstprüfer: Prof. Dr.-Ing. Boris Tolg
Zweitprüfer: Dipl.-Kfm. Christan Westerkamp, LL.M.

Abgabedatum: 28.09.2017

Zusammenfassung

Tobias Malte Kretzmann

Thema der Bachelorarbeit

Analyse und Implementierung eines Datenschutzmanagementsystems (DSMS) gemäß Datenschutz-Grundverordnung (DSGVO) in ein bestehendes Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 am Beispiel eines mittelständischen Unternehmens

Stichworte

Datenschutz, DSGVO, DSAnpUG-EU, DSFA, DSMS, ISMS, ISO 27001, ISO 27002

Kurzzusammenfassung

Diese Arbeit umfasst die Analyse und Implementierung eines Datenschutzmanagementsystems (DSMS) nach den neuen datenschutzrechtlichen Grundlagen der EU und der Bundesrepublik Deutschland, die am 25.05.2016 in Kraft getreten und bis 25.05.2018 verpflichtend umzusetzen sind. Bei der Implementierung des DSMS besteht die Besonderheit, dass ein bestehendes Informationssicherheitsmanagementsystem als Grundlage für das DSMS genutzt wird.

Danksagung

Ich danke der ANMATHO AG, insbesondere Herrn Christian Westerkamp, für die Ermöglichung und Betreuung meiner Bachelorarbeit.

Zusammenfassung

In dieser Arbeit wird die Implementierung eines Datenschutzmanagementsystems (DSMS) in ein bestehendes Informationssicherheitsmanagementsystem (ISMS), welches bereits nach ISO 27001 zertifiziert ist, anhand des Unternehmens LieferUs GmbH erläutert. Das DSMS soll hierbei die rechtlichen Anforderungen der Datenschutz-Grundverordnung (DSGVO) und des Datenschutz-Anpassungs- und Umsetzungs-gesetztes umsetzen. Um die Integrierung des DSMS in ein ISMS zu erleichtern, werden zurzeit mehrere Standards von der Internationale Organisation für Normung erarbeitet.

Ein ISMS dient der Informationssicherheit. Es hat damit das Ziel, Informationen des Unternehmens vor Angriffen zu schützen. Ein DSMS hingegen soll die Rechte der betroffenen Personen in Bezug auf den Datenschutz sicherstellen. Zur Umsetzung dieser Anforderungen haben beide Managementsysteme eine ähnliche Struktur, nutzen einen kontinuierlichen Verbesserungsprozess sowie ein Dokumenten- und Risikomanagement. Beim Aufbau des DSMS bildet die Aufbauorganisation die Strukturen des Systems ab, während die Ablauforganisation die im System verwendeten Prozesse und Methoden beschreibt.

Im Methodenteil der Arbeit werden die Methoden zur Analyse eines Unternehmens in Bezug auf den Datenschutz sowie zur Implementierung eines DSMS erläutert. Zur Analyse des Unternehmens eignet sich die GAP-Analyse, mit der Abweichungen zu den Anforderungen aufgezeigt werden können. Um die genaue Unternehmensstruktur und Abläufe im Unternehmen in Erfahrung zu bringen, können Interviews mit den einzelnen Abteilungen des Unternehmens geführt werden. Des Weiteren wird der prozessorientierte Ansatz, mit dem ein DSMS im Unternehmen eingeführt werden kann, dargestellt. Im Rahmen des Risikomanagements des DSMS wird die Methode der Datenschutz-Folgeabschätzung (DSFA) zur Bewertung von besonders risikoreichen Verarbeitungen von personenbezogenen Daten angewendet.

Die Einführung des DSMS im Unternehmen gliedert sich in zwei Schritte. Der erste Schritt ist die Bestandsaufnahme, bei der alle relevanten Informationen des Unternehmens zusammengetragen und gebündelt werden. Im zweiten Schritt wird mit Hilfe dieser Informationen das DSMS im Unternehmen implementiert. Hierfür müssen Aufbau- und Ablauforganisation umgesetzt, sowie das Verfahren der DSFA im Risikomanagement des Unternehmens etabliert werden.

Bei der Implementierung des DSMS sind einige Herausforderungen zu beachten. Durch die DSGVO werden neue Anforderungen an den Datenschutz gestellt, die einen hohen Dokumentationsaufwand bedeuten und auch auf bereits erhobene Daten angewendet werden müssen. Zudem gibt es in der Auslegung einiger Anforderungen rechtliche Unsicherheiten, die beispielsweise durch unterschiedliche Interpretationen des Kopplungsverbotes in Artikel 7 Absatz 4 und dem zugehörigen Erwägungsgrund 43 Satz 2 der DSGVO entstehen. Darüber hinaus kann es durch die unterschiedlichen Zielsetzungen des DSMS und des ISMS zu Konflikten zwischen beiden Systemen kommen, da das ISMS unternehmenseigene Interessen vertritt, während das DSMS die Rechte Dritter schützen soll und die Gesetzgebung zum Datenschutz umsetzen muss.

Für die Umsetzung der DSGVO und die Implementierung eines DSMS ist ein Zeitraum von zwei Jahren bis zum 25.05.2018 vorgegeben. Aufgrund der rechtlichen Unsicherheiten haben viele Unternehmen jedoch mit der Umsetzung gezögert, sodass sie nun in Zeitnot geraten. Es ist zudem so, dass die Implementierung eines DSMS allein nicht ausreicht, um die Anforderungen der DSGVO umzusetzen, da die Mitarbeiter im Unternehmen ein Datenschutzrisiko darstellen. Um also einen umfassenden Datenschutz sicherzustellen, müssen diese geschult und für die Thematik sensibilisiert werden.

Als Ergebnis dieser Arbeit lässt sich sagen, dass die Implementierung eines DSMS in ein bestehendes ISMS für das Unternehmen erhebliche Vorteile bietet, da sich diese Beiden nicht nur strukturell sehr ähnlich, sondern auch thematisch eng miteinander verknüpft sind.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	*Absatz*
ADV	*Auftragsdatenverarbeitung*
Art.	*Artikel*
BDSG	*Bundesdatenschutzgesetz*
DSAnpUG-EU	*Datenschutz-Anpassungs- und -Umsetzungsgesetz EU*
DSFA	*Datenschutz-Folgeabschätzung*
DSGVO	*Datenschutz-Grundverordnung*
DSMS	*Datenschutzmanagementsystem*
ErwG.	Erwägungsgrundsatz
EU	*Europäische Union*
ISMS	*Informationssicherheitsmanagementsystem*
ISO	*Internationale Organisation für Normung*
IT	*Informationstechnik*
KVP	*kontinuierlicher Verbesserungsprozess*
TOM	*technische und organisatorische Maßnahme*
WP	*Working Paper*

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die Datenschutz-Grundverordnung (DSGVO), die am 25.05.2018 in Kraft treten wird, fordert von Unternehmen weitreichende Änderungen und Anpassungen in Bezug auf den Schutz personenbezogener Daten von betroffenen Personen. Insbesondere die Forderung, ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (TOMs) zur Gewährleistung der sicheren Verarbeitung personenbezogener Daten zu implementieren, stellt Unternehmen vor eine große Herausforderung, da dies mit einem hohen zeitlichen, organisatorischen und dokumentarischen Aufwand verbunden ist. Dieser Herausforderung kann man mittels eines Datenschutzmanagementsystems (DSMS) begegnen, denn mit diesem können im Unternehmen einheitliche und strukturierte Verfahren zur Umsetzung dieser Forderung etabliert werden. Bei einem Managementsystem handelt es sich um eine Zusammenstellung aufeinander abgestimmter Methoden und Prozesse zur Erreichung eines vorher definierten Zieles, mit dem Anspruch einer stetigen Verbesserung des Systems. Hierbei kann das DSMS auf vorhandene Managementsysteme, wie das Informationssicherheits-managementsystem (ISMS), aufgebaut werden, wodurch ein integriertes Managementsystem gebildet werden kann. Durch die Nutzung bestehender Managementsysteme lassen sich zudem Synergieeffekte, die in Kapitel 1.3.5 näher erläutert werden, bei der Implementierung eines DSMS nutzen, da auf vorhandene Prozesse und Ressourcen zurückgegriffen werden kann.

1.1 Zielsetzung

Ziel dieser Bachelorarbeit ist die Erläuterung der Einführung eines DSMS auf der Basis eines ISMS, um die neuen nationalen und europäischen Anforderungen der Datenschutzgesetzgebung zu erfüllen. Hierfür wird die Einführung an einem Beispielunternehmen dargestellt. Diese Arbeit soll mittelständischen Unternehmen mit Sitz in der Bundesrepublik Deutschland als Orientierung bei der Umsetzung der DSGVO im eigenen Unternehmen dienen.

1.2 Rechtliche Grundlagen

Nach Art. 2 des Grundgesetzes hat in Deutschland ein jeder das Recht auf die freie Entfaltung seiner Persönlichkeit. Diese Freiheit ist unverletzlich und schließt auch den Schutz personenbezogener Daten mit ein.

Bei personenbezogenen Daten handelt es sich laut §3 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) um Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Die europäische Datenschutzrichtlinie besagt, dass eine Person dann als bestimmbar angesehen wird, wenn die Zuordnung zu einer Kennnummer oder einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind, möglich ist (Art. 2 Buchst. a Europäisches Parlament, 1995). Um diese Aussage zu konkretisieren, hat die Artikel-29-Datenschutzgruppe - ein unabhängiges Beratungsgremium der Europäischen Union (EU) - mit dem WP (working paper) 136 eine Stellungnahme zum Begriff der personenbezogenen Daten herausgegeben (Artikel-29-Datenschutzgruppe, 2007). Basierend auf dieser Stellungnahme gehören unter anderem der Name, die Telefonnummer, die Kontodaten, das Aussehen, aber auch Aufzeichnungen über Arbeitszeiten (EuGH, 2013) oder die IP-Adresse (BGH, 2017) zu den personenbezogenen Daten.

Die EU-weiten Regelungen bezüglich des Schutzes dieser personenbezogenen Daten wurden 2016 überarbeitet, um sie an heutige Bedürfnisse anzupassen und mit dem Ziel, innerhalb der EU eine Harmonisierung des Datenschutzes zu schaffen (Europäisches Parlament, 2016). Aufgrund dieser Reform müssen in Deutschland die rechtlichen Regelungen, bisher unter anderem in Form des BDSG, novelliert werden. Um in Unternehmen die neuen Anforderungen an den Datenschutz umsetzen zu können, ist die Implementierung eines DSMS erforderlich.

Im Folgenden werden die für die Implementierung eines DSMS auf Basis eines ISMS maßgeblichen Gesetze und Normen genauer betrachtet.

1.2.1 EU-Datenschutz-Grundverordnung (DSGVO)

Bereits 1995 hat sich die EU auf ein gemeinsames Datenschutzniveau geeinigt und eine EU-Datenschutz-Richtlinie verabschiedet (Europäisches Parlament, 1995). EU-Richtlinien müssen von den einzelnen Mitgliedsstaaten durch nationale Gesetze umgesetzt werden, wofür diesen zwei Jahre Zeit zur Verfügung stehen. Bei dem Prozess, die EU-Datenschutz-Richtlinie in nationale Gesetze umzuwandeln, wurde der Inhalt der Richtlinie von den einzelnen Staaten jeweils sehr unterschiedlich ausgelegt, sodass das Ziel, ein einheitliches EU-weites Datenschutzniveau zu erreichen, verfehlt wurde (Voßhoff, 2017, S. 7).

Um diesen Missstand zu beheben, wurde am 08.04.2016 durch den Rat der EU und am 14.04.2016 durch das EU-Parlament ein neuer Rechtsrahmen beschlossen: Die EU-Datenschutzreform (Europäisches Parlament, 2016). Auf diese hatte sich die EU-Kommission am 15.12.2015 im sogenannten Trilog - einem Vermittlungsausschuss aus EU-Kommission, Rat der EU und EU-Parlament - geeinigt (EU-Kommission, 2015).

Hauptziel der EU-Datenschutzreform ist es, ein einheitliches Niveau zum Schutz personenbezogener Daten innerhalb der EU zu erreichen und den Bürgern der europäischen Staaten die Entscheidung, was mit ihren persönlichen Daten geschehen darf, zurückzugeben (Europäisches Parlament, 2016).

Die EU-Datenschutzreform besteht aus zwei Teilen, der EU-Datenschutz-Richtlinie für Polizei und Justiz und der für diese Arbeit relevanten DSGVO, welche am 25.05.2016 in Kraft getreten und bis zum 25.05.2018 verpflichtend umzusetzen ist. Damit es nicht erneut zu verschieden Interpretationen des Datenschutzes kommen kann, wurde dieses Mal in Form der DSGVO statt einer Richtlinie eine Verordnung verfasst. Der Unterschied zu einer Richtlinie besteht darin, dass eine Verordnung unmittelbar mit Inkrafttreten in allen Mitgliedsstaaten gilt, und nicht erst der Inhalt durch ein nationales Gesetz umgesetzt werden muss.

Die DSGVO besteht aus 99 Artikeln und 173 Erwägungsgründen (ErwG.). Die Erwägungsgründe sind die Ziele, die mit den Artikeln erreicht werden und sollen dabei helfen, diese im Sinne der EU zu interpretieren.

Sie haben keinen weisenden Charakter, sondern enthalten die Begründungen für die verfügenden Bestimmungen der Artikel (Europäische Union, 2011, S. 41). Zudem enthalten die Artikel der DSGVO über 70 Öffnungsklauseln, die den Mitgliedstaaten die Möglichkeit geben soll, bestimmte Teile des Datenschutzes durch nationale Gesetze zu regeln (Kühling et al., 2016).

1.2.2 Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU)

Um für die Bundesrepublik Deutschland die Öffnungsklauseln der DSGVO zu füllen und nationale Vorrausetzungen zur Einführung der DSGVO zu schaffen, wurde am 27.04.2017 das Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU) vom Bundestag verabschiedet (Bundestag, 2017). Es erhielt am 12.05.2017 die Zustimmung des Bundesrates (Bundesrat, 2017).

Das DSAnpUG-EU ist ein Artikelgesetz, bestehend aus acht Artikeln. Als Artikelgesetz wird ein Gesetz bezeichnet, welches zeitgleich unterschiedliche Inhalte oder mehrere Gesetze in sich vereint. Diese Gesetzgebungspraxis wird im Besonderen bei Änderungsgesetzen angewendet (Lachner, 2007). Im ersten Artikel steht das neue BDSG. In den Artikeln 2 bis 6 werden Gesetze, die die Sicherheitsbehörden sowie das Artikel-10-Gesetz (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) betreffen, an EU-Datenschutz-Vorgaben angepasst. Art. 7 regelt Teile des Geschäftsbereiches der Bundesdatenschutz-beauftragten. Des Weiteren wird mit Art. 7 das geltende BDSG um den Paragrafen 42b erweitert. Den deutschen Aufsichtsbehörden soll hiermit bereits vor Inkrafttreten der DSGVO der Rechtsweg für ein Klagerecht eröffnet werden. Art. 8 besagt, dass das Gesetz zeitgleich mit der DSGVO in Kraft tritt. Ausgenommen hiervon ist Art. 7, der bereits am Tag nach der Verkündung des Gesetzes in Kraft tritt (Düwell, 2017).

Mit dem DSAnpUG-EU muss somit am 25.05.2018 nicht nur die DSGVO in Deutschland umgesetzt werden, es tritt auch das neue BDSG in Kraft. Dieses wird dabei das alte BDSG vollständig ersetzen. Abweichend zur DSGVO ist im neuen BDSG unter anderem die Stellung des Datenschutzbeauftragten wesentlich stärker ausgeprägt.

1.2.3 ISO 27001 und ISO 27002

Die Internationale Organisation für Normung (ISO) hat mit der ISO 27001 eine international anerkannte Norm zur Zertifizierung eines ISMS veröffentlicht. Als Grundlage für die ISO 27001 wurde der zweite Teil des britischen Standards BS 7799-2:2002 genutzt (Völker, 2004). Mit der ISO 27001 wird ein risikobasierter Ansatz genutzt, um die durch das ISMS zu schützenden Unternehmenswerte zu ermitteln.

Neben der ISO 27001 als Hauptnorm gibt es in der Normreihe 27000 des Weiteren die unterstützenden und ergänzenden Normen 27002 bis 27007. In den unterstützenden Normen werden bestimmte Sachverhalte aus der Hauptnorm vertiefend dargestellt. Die ISO 27002 beschreibt hierbei Sicherheitsmaßnahmen für die Informationssicherheit. Sie beinhaltet Vorschläge, wie bestimmte Maßnahmen umgesetzt werden können. Im Gegensatz zur ISO 27001 ist sie nicht bindend, sondern soll lediglich die „best practice“ der Informationssicherheit darstellen.

1.2.4 ISO Normen zum Datenschutz im Entwurf

Aktuell werden durch die ISO mehrere Standards im Bereich Datenschutz entwickelt. Für ein DSMS sind hierbei zwei Normen besonders interessant, da diese eine Grundlage für das DSMS bilden können, die ISO 29151 und die ISO 27552.

Die Normreihe ISO 29100 ist ein Rahmenwerk zum Datenschutz, in dem die einschlägige Datenschutzterminologie definiert wird, sowie die zum Schutz der Privatsphäre betroffener Personen zu berücksichtigenden Aspekte beschrieben werden (ISO 29100:2011). Die ISO 29151 – als Teil der Normreihe ISO 29100 - mit dem Titel „Leitfanden für den Schutz personenbezogener Daten (Code of Practice for personally identifiable information protection)“ wird vorrausichtlich im April 2018 veröffentlicht. Sie soll datenschutzspezifische Ziele, Maßnahmen und Empfehlungen für Verantwortliche enthalten, um die nach einer Risikobewertung identifizierten Risiken angemessen adressieren zu können (Kranig et al., 2017, S. 171).

Die ISO 27552 soll die ISO 27001 um Datenschutzaspekte erweitern, wodurch die Möglichkeit geschaffen werden soll, ein DSMS als integriertes Datenschutz-Managementsystem in ein ISMS nach ISO 27001 zu integrieren (Kranig et al., 2017, S. 171). Ein Veröffentlichungsdatum dieser Norm steht noch nicht fest.

1.3 Vergleich von ISMS und DSMS

In diesem Abschnitt werden das ISMS und das DSMS vorgestellt, und die Parallelen und Unterschiede beider Managementsysteme aufgezeigt.

1.3.1 Beschreibung eines ISMS

Ein ISMS ist ein Managementsystem für die Sicherheit von Informationen. Nach der ISO 27002 ist Informationssicherheit als Schutz von Informationen vor Angriffen definiert, mit dem Ziel, die Kontinuität des Geschäfts (Geschäftsfortführung) zu sichern, Geschäftsrisiken zu minimieren und den Return on Investment (ROI), Profit sowie die Geschäftsopportunitäten und Geschäftschancen zu maximieren (ISO 27002:2017; Sowa, 2017, S. 10).

Die Aufgabe des ISMS ist die Sicherstellung der Grundwerte der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit von Informationen (BSI, 2012). Die Informationen können dabei nicht nur in digitaler Form, sondern auch als Papierdokumente oder in anderer Form existieren. Je nach Schutzbedürfnis des Unternehmens müssen mit dem ISMS noch weitere Schutzziele, wie Authentizität und Verbindlichkeit, abgedeckt werden. Zur Ermittlung der zu schützenden Informationen, wird nach dem risikobasierten Ansatz der ISO 27002 ein Risikomanagement im ISMS eingesetzt.

1.3.2 Anforderungen an ein ISMS

Die wichtigsten Anforderungen an ein ISMS sind demnach die Formulierung der Sicherheitsziele, die Bestimmung der zu schützenden Unternehmenswerte, das Risikomanagement mit der Risikobeurteilung und der Risikobehandlung sowie die kontinuierliche Verbesserung des ISMS.

Die Sicherheitsmaßnahmen, die mit Hilfe eines ISMS umgesetzt werden sollen, sind in der ISO 27002:2017 beschrieben. Die insgesamt 114 Sicherheitsmaßnahmen sind in die folgenden 14 Abschnitte zusammengefasst:

- Informationssicherheitsrichtlinie (Information security policies)
- Organisation der Informationssicherheit (Organization of information security)
- Personalsicherheit (Human resource security)
- Verwaltung der Werte (Asset management)
- Zugangssteuerung (Access control)
- Kryptographie (Cryptography)
- Physische und umgebungsbezogene Sicherheit (Physical and environmental security)
- Betriebssicherheit (Operations security)
- Kommunikationssicherheit (Communications security)
- Anschaffung, Entwicklung und Instandhaltung von Systemen (System acquisition, development and maintenance)
- Lieferantenbeziehungen (Supplier relationships)
- Handhabung von Informationssicherheitsvorfällen (Information security incident management)
- Informationssicherheitsaspekte beim Business Continuity Management (Information security aspects of business continuity management)
- Compliance

Um ein ISMS nach ISO 27001 zertifizieren zu können, müssen die in Kapitel 4 bis 10 der Norm genannten Anforderungen an ein ISMS zwingend umgesetzt werden (Kersten et al., 2016).

1.3.3 Beschreibung eines DSMS

Bei einem DSMS handelt es sich um ein Managementsystem, welches das Ziel verfolgt, in einem Unternehmen ein einheitliches Datenschutzniveau sicherzustellen, das den gesetzlichen, vertraglichen und internen Datenschutzanforderungen genügt (Loomans et al., 2010). Zudem soll das DSMS eine klare Lenkung und Leitung des Unternehmens in Bezug auf den Datenschutz ermöglichen (Loomans et al., 2014). Unternehmen sollen mittels des DSMS in der Lage sein, Auskunft über die Verarbeitung personenbezogener Daten zu geben, sowie Forderungen in Bezug auf die Rechte betroffener Personen umzusetzen.

1.3.4 Anforderungen an ein DSMS

In der DSGVO wird ein DSMS nicht namentlich genannt. Jedoch fordert der Art. 32 Abs. 1 DSGVO ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten. Zudem besagt Art. 5 Abs. 2 DSGVO, dass der Verantwortliche für den Datenschutz einer Rechenschaftspflicht in Bezug auf die Grundsätze für die Verarbeitung personenbezogener Daten unterliegt. Dies bedeutet, dass das Unternehmen in einem Streitfall nachweisen muss, dass es die DSGVO umgesetzt hat. Das betrifft unter anderem die Beschwerden von betroffenen Personen, aber auch die Abwehr von Schadenersatzansprüchen (Wybitul, 2016, S. 1078). Des Weiteren erstreckt sich die Rechenschaftspflicht auf alle Anforderungen, die die DSGVO an die Verarbeitung von personenbezogenen Daten stellt (Lambertz, 2016). Hierzu gehört auch die Datenschutz-Folgeabschätzung (DSFA) nach Art. 35 und 36 DSGVO, eine Methode zur Bewertung von Risiken und deren möglichen Folgen. Bei der Rechenschaftspflicht ist ein besonderes Augenmerk auf die TOMs zu legen, da diese vom Verantwortlichen umgesetzt, dokumentiert und nachgewiesen werden müssen (Feil, 2017).

Neben diesen Forderungen der DSGVO, die die Einführung eines DSMS sinnvoll, wenn nicht gar notwendig erscheinen lassen, gibt es die Möglichkeit, Datenschutzmanagement als Wettbewerbsvorteil zu sehen. Richtig angewendet kann ein DSMS die Effizienz betrieblicher Abläufe erheblich steigern, und die Zertifizierung des DSMS kann zur Vertrauensbildung beim Kunden genutzt werden (Borchers, 2006).

Mit einem DSMS lassen sich die Anforderungen und Pflichten (Abbildung 1), die sich aus der DSGVO ergeben, nachweisbar umsetzen. Zu diesen Pflichten gehören, wie in der Abbildung ersichtlich, auch geeignete TOMs zur Sicherstellung der Datenschutzanforderungen. Ein Teil dieser ist die Wahrung der Vertraulichkeit durch geeignete Maßnahmen der Informationssicherheit.

Abbildung 1: Anforderungen an das Management von Datenschutzrisiken (Kranig et al. 2017 S. 163)

Die wichtigste Anforderung an ein DSMS ist bei alledem die Sicherstellung des Datenschutzes im Unternehmen. Damit ein DSMS dieses garantieren kann, muss es die volle Unterstützung der Geschäftsführung besitzen.

1.3.5 Parallelen und Unterschiede zwischen ISMS und DSMS

Zwischen einem ISMS und einem DSMS gibt es einige Parallelen, die die Integrierung eines DSMS in ein ISMS vereinfachen. Beide Managementsysteme nutzen einen risikobasierten Ansatz und den kontinuierlichen Verbesserungsprozess (KVP) nach Kaizen zur kontinuierlichen Verbesserung und Anpassung an neue Gegebenheiten und Anforderungen, der im Methodenteil näher erläutert wird. Des Weiteren wurde bereits für das ISMS zu Nachweißzwecken ein Dokumentenmanagementsystem eingeführt, welches um die Dokumente des DSMS erweitert werden kann. Hierfür sind keine weiteren Anpassungen des Dokumentenmanagementsystems nötig. Ebenfalls ist im ISMS bereits ein Risikomanagement implementiert, welches jedoch nicht ohne weiteres für das DSMS übernommen werden kann, da die DSGVO andere Anforderungen an das Risikomanagement stellt als die ISO 27002.

Durch das bestehende Risikomanagement sind allerdings schon die Grundstrukturen für die Risikobeurteilung und Risikobehandlung sowie unterstützende Prozesse und Ressourcen vorhanden. Demzufolge können einige vorhandene Prozesse und Strukturen des ISMS mit geringem Aufwand an die Bedürfnisse eines DSMS angepasst werden, wenn in einem Unternehmen bereits ein ISMS nach ISO 27001 existiert.

ISMS und DSMS unterscheiden sich bezüglich ihrer Zielsetzungen. Das ISMS stellt den Schutz aller das Unternehmen betreffenden Information sicher, und soll Unternehmensrisiken minimieren. Im Gegensatz dazu bezieht sich das DSMS nur auf den Schutz personenbezogener Daten und die Reduzierung von Datenschutzrisiken. Der größte Unterschied zwischen den beiden ist hierbei das Managementziel. Ein ISMS dient dem Schutz unternehmenseigener Interessen und Vermögenswerte, während ein DSMS den Schutz und die Interessen Dritter in den Vordergrund stellt, und somit die Grundrechte dieser sichert. Daraus folgt, dass das DSMS im Unternehmen einen so hohen Stellenwert besitzen muss, dass es andere Managementsysteme, wie das ISMS, auf Grundrechtskonformität überprüfen und deren Maßnahmen gegebenenfalls einschränken kann (Rost, 2013, S. 295).

In Tabelle 1 sind die verschiedenen Ansätze und Zielsetzungen der beiden Managementsysteme zusammengefasst. Hierbei ist ein besonderes Augenmerk darauf zu legen, dass zum Gegenstand der Informationssicherheit auch der Schutz personenbezogener Daten gehört.

Tabelle 1: Informationssicherheit vs. Datenschutz (Kranig et al. 2017 S. 169)

Abgrenzung	**Informationssicherheit**	**Datenschutz**
Ziel	Schutz der Organisation	Schutz der Betroffenen
Umfang / Gegenstand	Alle Informationen, einschließlich personenbezogener Daten und Geschäftsprozesse	Personenbezogene Daten, Datenverarbeitung
Berücksichtigung von:	Unternehmensrisiken, einschließlich Compliance- und finanzieller Risiken	Datenschutzrisiken und Folgen für Betroffene

1.4 Aufbau eines DSMS

Damit die Anforderungen und Pflichten, die sich aus der DSGVO ergeben, durch das DSMS nachweisbar umgesetzt werden können, muss es folgende Punkte beinhalten und abdecken:

- Definition der Datenschutz-Ziele
- Definition der Datenschutz-Governance-Struktur
- Festlegung der Datenschutzleitlinie
- Prozessdefinitionen von Verarbeitungsvorgängen, bei denen personenbezogene Daten genutzt werden
- Prozesse zur Sicherstellung der Betroffenenrechte
- Prozesse zur Handhabung von Datenschutzverletzungen

Die ersten drei Punkte können dabei der Aufbauorganisation zugeordnet werden, da sie die Struktur des DSMS bestimmen und beschreiben. Die letzten drei Punkte werden der Ablauforganisation zugeordnet, da mit ihnen Prozesse definiert werden.

1.4.1 Aufbauorganisation (Datenschutzstrukturen)

Die Aufbauorganisation beschreibt in einem Unternehmen die hierarchischen Strukturen. Hierunter fallen die Zuständigkeiten der einzelnen Abteilungen, sowie der Aufbau der vertikalen Unternehmensstruktur (Jacob, 2013). Die kleinste Organisationseinheit in der Aufbauorganisation ist die Stelle. Stellen werden zu Gruppen und Abteilungen zusammengefasst (Daum et al., 2010, S. 107). Mit anderen Worten beschreibt die Aufbauorganisation, welche Stelle mit welchen Mitteln agiert und wie die Zusammenhänge zwischen den einzelnen Stellen, Gruppen und Abteilungen aussehen.

Zur Aufbauorganisation zählen die Datenschutzziele, die Datenschutz-Governance-Struktur, die Datenschutzleitlinie sowie die Verpflichtungserklärung.

Die Datenschutzziele legen fest, wie sich das Unternehmen im Bereich Datenschutz positioniert. Sie werden wie andere Unternehmensziele, beispielsweise Umweltschutz- oder Informationssicherheitsziele, von der Geschäftsführung verabschiedet. Zur Ermittlung der Datenschutzziele sind die internen und externen Anforderungen an den Datenschutz maßgeblich. Hierbei ist zu beachten, dass unter Umständen neben der DSGVO auch andere Gesetze, wie das Telekommunikationsgesetz, Anforderungen an die zu erreichenden Ziele stellen. Sollten Teile des Unternehmens außerhalb Deutschlands ihren Sitz haben, sind die dort geltenden Gesetze ebenso zu berücksichtigen. Dies trifft unter anderem auf den Bereich Arbeitsrecht zu, da im Art. 88 der DSGVO explizit nationale Regelungen für Beschäftigtendaten vorgesehen sind.

Die Datenschutzziele entstehen aus den Datenschutzgrundsätzen, indem diese durch die Geschäftsführung auf das Unternehmen bezogen formuliert werden. Die Datenschutzgrundsätze wiederum sollen sich nach den Anforderungen des führenden Gesetzes richten, innerhalb der EU ist dies die DSGVO. Gemäß Art. 5 Abs. 1 der DSGVO handelt es sich dabei um folgende Datenschutzgrundsätze:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung

- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Die Datenschutz-Governance-Struktur beinhaltet die für den Datenschutz im Unternehmen verantwortlichen Personen und ist eine Lenkungsstruktur für die rechtlichen Anforderungen an diese (Schneider, 2004). Die DSGVO sieht das Unternehmen in der rechtlichen Verantwortung, die Datenschutzvorschriften einzuhalten (Art. 5 Abs. 2 DSGVO). Da das Unternehmen nach außen durch die Geschäftsführung vertreten wird und diese für Datenschutzrechtsverletzungen überdies haftbar gemacht werden kann, ist sie für die Einhaltung der Datenschutzvorschriften verantwortlich, und kann diese Verantwortung auch nicht delegieren. Daraus folgt, dass der Verantwortliche für den Datenschutz gleichzusetzen mit dem Geschäftsführer oder einem Mitglied der Geschäftsführung ist. Dieser hat Entscheidungs- und Umsetzungskompetenzen und ist für die Einhaltung der Datenschutzziele verantwortlich.

Neben dem Verantwortlichen für den Datenschutz gibt es nach Art. 37 DSGVO den Datenschutzbeauftragten. Er hat im Gegensatz zum Verantwortlichen für den Datenschutz eine rein beratende Funktion. Art. 37 Abs. 4 DSGVO bietet durch die Öffnungsklausel für die Benennungspflicht die Möglichkeit, die Anforderungen für die Benennung eines Datenschutzbeauftragten zu verschärfen (Marschall und Müller, 2016). Durch das neue BDSG § 38 wird diese Öffnungsklausel genutzt, und die Benennung eines Datenschutzbeauftragen für nichtöffentliche Unternehmen schon ab einer Unternehmensgröße von 10 Mitarbeitern festgelegt (Kühling et al., 2017, S. 671). Er hat nach Art. 39 DSGVO die Funktion eines internen Kontrollorgans. Des Weiteren hat er die Pflicht, mit den Aufsichtsbehörden aktiv zusammenzuarbeiten.

Der Datenschutzbeauftragte und der Verantwortliche für den Datenschutz können funktions- und organisatorisch bedingt nicht ein und dieselbe Person sein, da der Datenschutzbeauftragte keinerlei Weisungs- oder Entscheidungsbefugnisse gegenüber der ihn benennenden Stelle besitzt (Kühling et al., 2017, S. 692).

Die Datenschutzleitlinie drückt die Verantwortlichkeit der Geschäftsführung zum Datenschutz aus. In ihr werden die Überlegungen zu den Datenschutzzielen und der Datenschutz-Governance-Struktur dokumentiert. Mit der Einführung der Datenschutzleitlinie wird der Datenschutz und die festgelegten Datenschutzziele zu einem Teil des Unternehmensleitbildes (Kranig et al., 2017, S. 35).

Damit ein DSMS auch wirksam in einem Unternehmen eingesetzt werden kann, müssen die Mitarbeiter zur Umsetzung der Datenschutzleitlinie und den Datenschutzrichtlinien verpflichtet werden. Hierfür muss jeweils eine Verpflichtungserklärung abgegeben werden.

1.4.2 Ablauforganisation (Datenschutzprozesse)

Im Gegensatz zur Aufbauorganisation beschreibt die Ablauforganisation Unternehmensprozesse. Im Rahmen des Datenschutzes sind die Prozesse zur Verarbeitung personenbezogener Daten, zum Risikomanagement, zur Sicherstellung der Betroffenenrechte und zur Handhabung von Datenschutzverletzungen von besonderer Bedeutung.

Bei jedem Unternehmensprozess, bei dem personenbezogene Daten verarbeitet werden, muss die Konformität zu den Datenschutzvorgaben der DSGVO sichergestellt sowie eine Risikobewertung für die Sicherheit der Rechte der betroffenen Personen durchgeführt werden. Diese Rechte werden in der DSGVO in Kapitel 3 beschrieben. Zu ihnen gehört unter anderem das Recht auf Vergessenwerden sowie das Recht auf Datenübertragbarkeit. Betroffene im Sinne der DSGVO sind die Personen, deren Daten verarbeitet werden. Das Unternehmen muss sicherstellen, dass diese Rechte eingehalten werden.

Sollte es trotz getroffener Maßnahmen zum Schutze der personenbezogenen Daten zu einer Datenschutzverletzung kommen, sieht die DSGVO die Informierung der Aufsichtsbehörden und unter bestimmten Umständen auch der Betroffenen vor.

Bei einer Datenschutzverletzung im Sinne des Art. 4 Nr. 12 DSGVO handelt es sich um eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung der personenbezogenen Daten führt und damit zum Verlust der Verfügbarkeit bzw. Integrität oder zur unberechtigten Offenlegung von personenbezogenen Daten, was einen Verlust der Vertraulichkeit darstellt (Kranig et al., 2017, S. 68).

1.5 Beispiel für ein mittelständisches Unternehmen

Um die Umsetzung eines DSMS anschaulicher darzustellen, wird sie in dieser Arbeit beispielhalft an dem im Folgenden beschriebenen mittelständischen Unternehmen durchgeführt. Bei einem mittelständischen Unternehmen handelt es sich nach der Definition des Bundesministeriums für Bildung und Forschung um ein Unternehmen, welches zwischen 50 und 250 Mitarbeiter beschäftigt oder zwischen 10 und 50 Millionen Euro Jahresumsatz verbucht (Europäische Union, 2015).

Das hier beschriebene Unternehmen LieferUs GmbH ist im Bereich des E-Commerce tätig und hat seinen Sitz in Hamburg, dieses ist der einzige Firmensitz. Im Unternehmen sind 70 Mitarbeiter beschäftigt. In Abbildung 2 ist die Struktur des Unternehmens dargestellt.

Die Verwaltung gliedert sich in die Abteilungen Personal, Recht, Informationstechnik, Buchhaltung und Facility-Management. Die Personalabteilung ist für alle die Mitarbeiter betreffenden Bereiche, einschließlich der Personalbuchhaltung, zuständig. In der Rechtsabteilung werden alle Verträge des Unternehmens ausgearbeitet. Zudem steht sie der Geschäftsführung in Rechtsbelangen beratend zur Seite. Die Abteilung Informationstechnik (IT) ist für den sicheren Betrieb der IT-Infrastruktur und der darauf laufenden Anwendungen verantwortlich. In der Buchhaltung werden alle Themen, die den Bereich Finanzen betreffen, bearbeitet. Die einzige Ausnahme bildet hier die bereits erwähnte Personalbuchhaltung. Zum Facility-Management gehören neben Bereichen wie der Gebäudereinigung und Instandhaltung auch der Bereich Objektsicherheit, der sich mit den Themen Gebäudesicherheit und Zugangsschutz befasst.

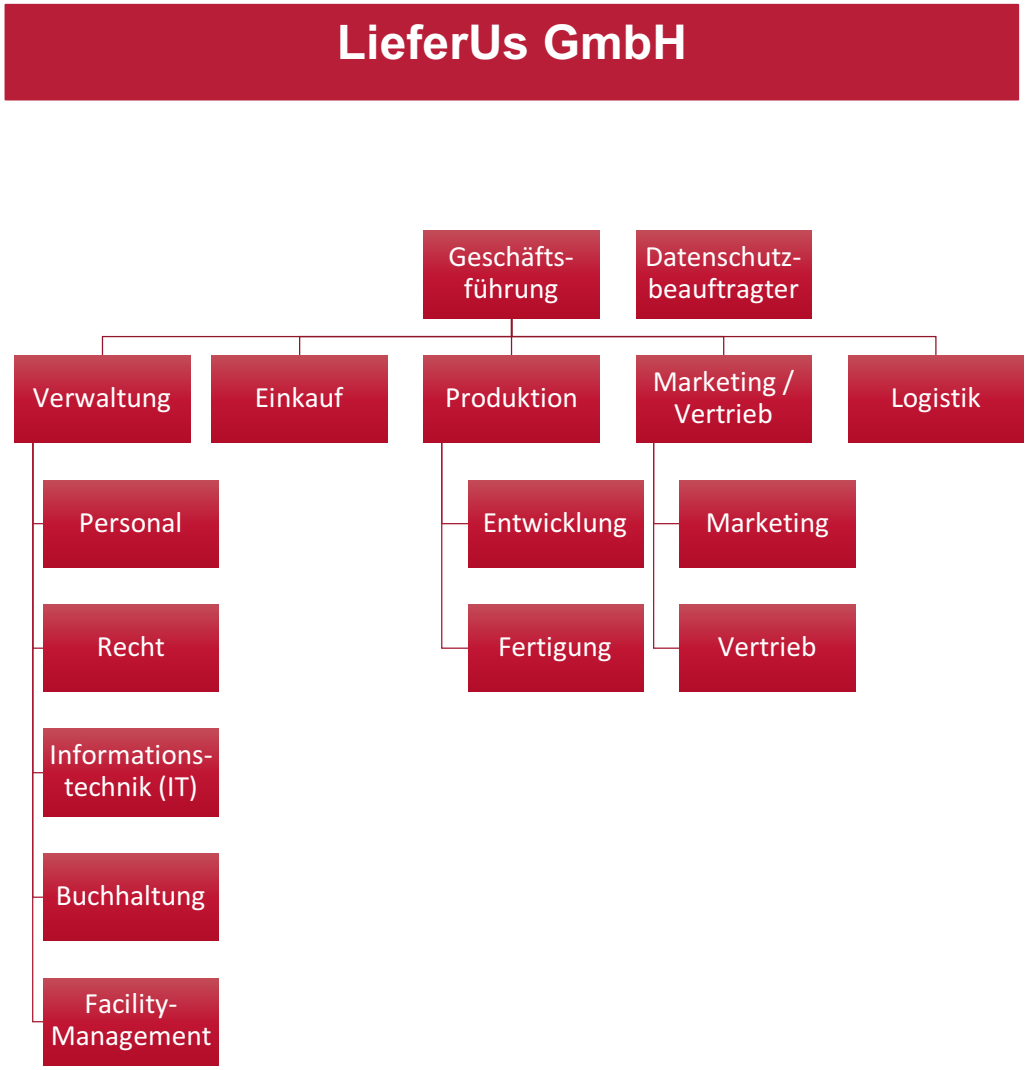

Abbildung 2: Organigramm der Unternehmensstruktur

Die Waren der LieferUs GmbH werden in der Abteilung Produktion erzeugt, die sich in die Bereiche Entwicklung und Fertigung gliedert.

Neben den Bereichen Verwaltung und Produktion gibt es die Abteilungen Marketing und Vertrieb, die einen gemeinsamen Vorgesetzten haben. Das Marketing ist für die Gestaltung und Verbreitung der Werbemittel sowie für die Kundenakquise verantwortlich. Der Vertrieb ist für den Verkauf der produzierten Güter zuständig.

Der Einkauf befasst sich mit dem Erwerb von Waren, die Logistik ist für den Bereich Transport zuständig.

Die Geschäftsführung der LieferUs GmbH besteht aus:

- dem CEO - Vorsitzender der Geschäftsführung und verantwortlich für Rechtsbelange
- dem CFO - Verantwortlicher für Finanzen, Einkauf und Logistik
- dem COO - Verantwortlicher für Vertrieb und Marketing
- dem CSO - Verantwortlicher für die organisatorische und physische Sicherheit sowie für das ISMS

Das DSMS fällt wie das ISMS in den Aufgabenbereich des CSO. Die Geschäftsführung wird durch einen Datenschutzbeauftragten in Belangen des Datenschutzes unterstützt, der zu ihr einen weisungsfreien Zugang besitzt. Das Unternehmen besitzt bereits ein nach ISO 27001 zertifiziertes ISMS.

2 Methoden

In diesem Teil werden die für die Implementierung und den Betrieb eines DSMS relevanten Methoden vorgestellt und erläutert. Hierbei wird zwischen Methoden zur Analyse und Implementierung eins DSMS und Methoden, die in einem DSMS verwendet werden, unterschieden. Zudem wird die DSFA als neue Methode innerhalb des Risikomanagements hier gesondert betrachtet.

2.1 Methoden zur Analyse und Implementierung eines DSMS

Um ein DSMS in einem Unternehmen erfolgreich einführen zu können, bedarf es einer gründlichen Analyse des Unternehmens, insbesondere der datenschutzrelevanten Aspekte. Hierzu gehören vor allem die Unternehmensstruktur, die Unternehmens-organisation, Unternehmensprozesse, Unternehmensziele, Geschäftsfelder und der kulturelle Hintergrund des Unternehmens. Für die Analyse kann zunächst die Unternehmensdokumentation herangezogen werden. Viele für den Datenschutz relevanten Informationen sind jedoch häufig nicht zentral dokumentiert, sodass diese aus den einzelnen Abteilungen zusammengetragen werden müssen.

Als Methoden für die Durchführung der Analyse des Unternehmens eignen sich die GAP-Analyse sowie strukturierte Interviews auf Basis vorgefertigter Fragebögen.

2.1.1 GAP-Analyse

Die GAP-Analyse ist ein von Ansoff entwickeltes strategisches Controlling-Instrument, mit dem es möglich ist, Abweichungen zwischen geplanten und vorrausichtlich zu erwartenden Entwicklungen zu ermitteln. Ursprünglich kommt die GAP-Analyse aus dem Bereich des Finanzcontrollings, allerdings lässt sich die Methode auch auf andere Bereiche anwenden (Buchholz, 2013, Kap. 2.6.2). In dieser Arbeit wird die Methode zur Ermittlung der Compliance im Bereich Datenschutz angewendet.

Mit Hilfe der GAP-Analyse kann der Erfüllungsgrad in Bezug auf die Anforderungen der DSGVO und des neuen BDSG ermittelt werden. Hierzu werden die Aussagen der Kapitel 2 bis 5 der DSGVO auf ihren Erfüllungsgrad geprüft. Jede relevante Aussage wird mit „erfüllt“ oder „nicht erfüllt“ bewertet.

Bereiche, die teilweise erfüllt oder noch in Planung sind, fallen demnach in die Kategorie „nicht erfüllt“, da mit dieser Analyse der aktuelle Stand im Unternehmen abgebildet werden soll. Folgende Bereich der DSGVO werden in Form eines Fragebogens überprüft:

- Grundsätze des Datenschutzes
    - Im zweiten Kapitel der DSGVO geht es um grundsätzliche Belange des Datenschutzes, wie die Grundsätze für die Verarbeitung personenbezogener Daten, Rechtmäßigkeit der Verarbeitung sowie die Einwilligung zur Verarbeitung der Daten und besondere Datenkategorien.
- Rechte der betroffenen Personen
    - Im dritten Kapitel geht es um die Rechte der betroffenen Personen, die in Kapitel 3.3.2.3 näher erläutert werden.
- Verantwortlicher und Auftragsverarbeiter
    - Das vierte Kapitel behandelt Haftungsfragen und Belange der Auftragsdatenverarbeitung (ADV)
- Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen
    - Das letzte betrachtete Kapitel der DSGVO ist für Unternehmen relevant, die personenbezogenen Daten in Drittländer senden oder dort verarbeiten.

Die gewonnenen Erkenntnisse aus dem Fragebogen werden mittels Excel als Netzdiagramm grafisch aufbereitet, sodass Defizite, aber auch Bereiche, in denen der bestehende Datenschutz ausreicht, hervortreten.

Um die beantworteten Fragen in das Netzdiagramm zu überführen, wird die Anzahl der erfüllten Bedingungen durch die Gesamtzahl der Bedingungen je Kapitel geteilt, sodass das Ergebnis einen Wert zwischen 0 und 1 annehmen kann. Dieser Wert wird im Anschluss als Prozentwert in das Netzdiagram übertragen.

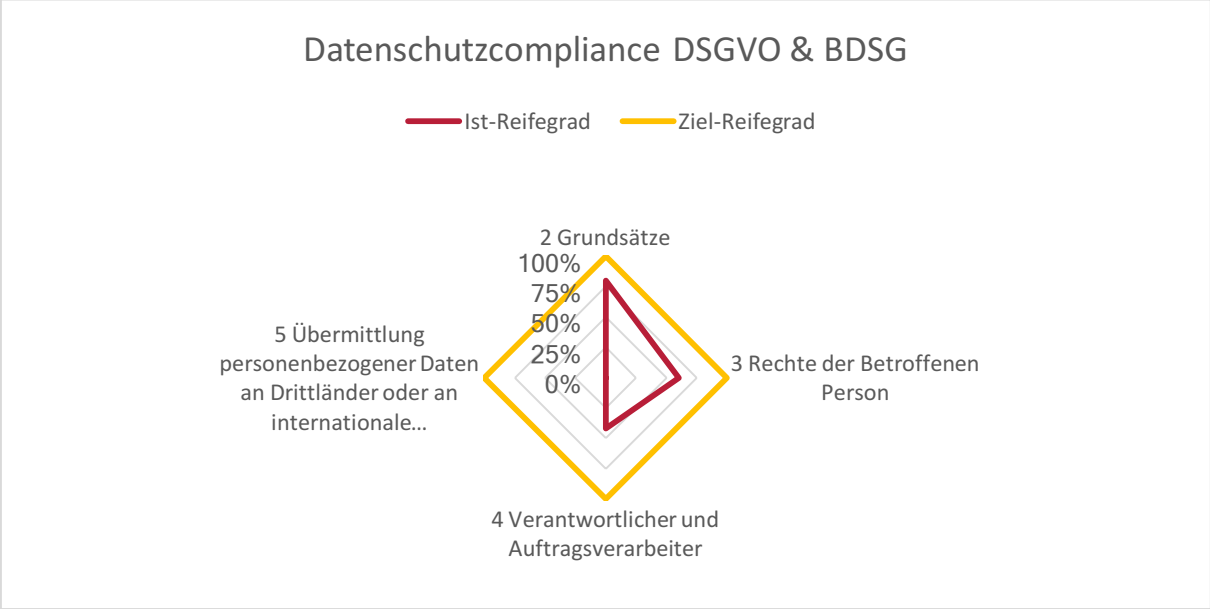

Abbildung 3: Ergebnis der GAP Analyse

Mittels dieser Informationen kann der Aufwand, ein DSMS einzuführen, abgeschätzt werden, da Abweichungen zur Zielvorgabe sofort ins Auge fallen und davon ausgegangen werden kann, dass eine größere Abweichung mit einem höheren Aufwand korreliert. Auch als Kontrollmechanismus ist die GAP-Analyse geeignet, um den Fortschritt bei der Einführung und die Kontrolle der Wirksamkeit der eingeführten Maßnahmen zu dokumentieren.

2.1.2 Interview

Mit Hilfe von vorgefertigten Fragebögen ist ein strukturiertes Interview über die Verarbeitung von personenbezogenen Daten mit den einzelnen Abteilungen eines Unternehmens möglich. Hierbei ist es von Vorteil mit der Geschäftsführung zu beginnen, um festzulegen für welche Unternehmensbereiche und mit welchem Fokus ein DSMS eingeführt werden soll. Die Geschäftsführung ist des Weiteren in der Lage, Verantwortliche der einzelnen zu befragenden Abteilungen zu benennen. Zusätzlich wird die Wichtigkeit der Einführung eines DSMS im Unternehmen noch einmal unterstrichen.

Nach der Befragung der Geschäftsführung werden die Abteilungen interviewt, in denen personenbezogene Daten verarbeitet werden. Hier ist primär bedeutsam, die genauen Tätigkeiten und Arbeitsabläufe mit Datenschutzrelevanz in der jeweiligen Abteilung zu ermitteln, um die organisatorischen Abläufe zu erfahren. Als letztes wird die IT-Abteilung befragt, da diese einen Überblick über die relevanten IT-Systeme und eingesetzte Software sowie die technischen Maßnahmen zum Schutz des Datenschutzes hat.

2.2 Prozessorientierte Managementmethode in einem DSMS

Für die Umsetzung der gesetzlichen Anforderungen an den Datenschutz in einem DSMS sollte nach einer prozessorientierten Methode vorgegangen werden. Bei dieser handelt es sich um einen systematischen Ansatz zur Umsetzung neuer Anforderungen im Unternehmen. Wenn im Unternehmen bereits ein Managementsystem vorhanden ist, wie es im Falle dieser Arbeit angenommen wird, kann auf diesem aufgebaut werden. Sollte dies nicht der Fall sein, muss erst ein allgemeiner Managementprozess im Unternehmen etabliert werden.

Um das DSMS kontinuierlich zu verbessern und an neue Gegebenheiten anpassen zu können, wird die japanische Management-Philosophie Kaizen angewendet. Unter Kaizen bzw. dem KVP wird ein ständiger Verbesserungsprozess unter Einbindung der Mitarbeiter verstanden. Hierbei liegt der Fokus auf dem zu verbessernden Prozess, und nicht auf dem Ergebnis (Gadatsch, 2017, S. 42). Dies bedeutet, dass primär eine Verbesserung des Managementsystems und nicht des Datenschutzes angestrebt wird, da dieser durch eine Verbesserung des Systems zwangsläufig ebenfalls verbessert wird.

Um mittels des KVP eine kontinuierliche Verbesserung des DSMS zu erreichen, wird der PDCA-Zyklus genutzt.

Der PDCA-Zyklus, auch als Deming-Kreis bekannt, ist eine Methode zur schrittweisen Verbesserung von Abläufen. Er besteht aus vier Teilschritten, die der Reihe nach durchlaufen werden.

Abbildung 4: PDCA-Zyklus

Plan: In dieser Phase werden die Maßnahmen geplant, die zum Erreichen des Soll-Zustandes und der an das Managementsystem gerichteten Anforderungen erforderlich sind.

Do: In diesem Teilschritt werden die geplanten Maßnahmen umgesetzt.

Check: Wurden die geplanten Maßnahmen umgesetzt, so sind diese zu beobachten und das Ergebnis zu evaluieren.

Act: Im letzten Teilschritt werden auf Basis der Evaluation Verbesserungen und Abweichungen vom Soll-Zustand erkannt und Maßnahmen durchgeführt, um diese Abweichungen zu schließen.

Durch das fortwährende Durchlaufen des PDCA-Zyklus entsteht ein Kreislauf der kontinuierlichen Verbesserung.

In der Praxis lassen sich die einzelnen Phasen nicht so klar voneinander abgrenzen, wie es hier beschrieben ist. Es besteht vielmehr ein fließender Übergang von einem Teilschritt in den nächsten. Vor allem bei den Teilschritten Do und Check ist es sinnvoll, geplante Maßnahmen schon während ihrer Umsetzung zu kontrollieren (Loomans et al., 2014, Kap. 5.1).

2.3 Datenschutz-Folgeabschätzung

Die DSFA ist nach Art. 35 DSGVO eine Methode des Datenschutz-Risikomanagements, um die Auswirkung einer Sicherheitsverletzung auf betroffene Personen im Vorwege zu beurteilen und einzuschätzen, ob eine Konsultation der Datenschutzaufsichtsbehörden nach Art. 36 Abs. 1 DSGVO erforderlich ist. Sie ist durchzuführen, wenn nach dem Risikomanagement die Datenverarbeitung voraussichtlich ein hohes Datenschutzrisiko mit sich bringt (Friedewald et al., 2016).

Die DSFA nach ISO 29134 besteht aus den in Abbildung 5 ersichtlichen Teilprozessen.

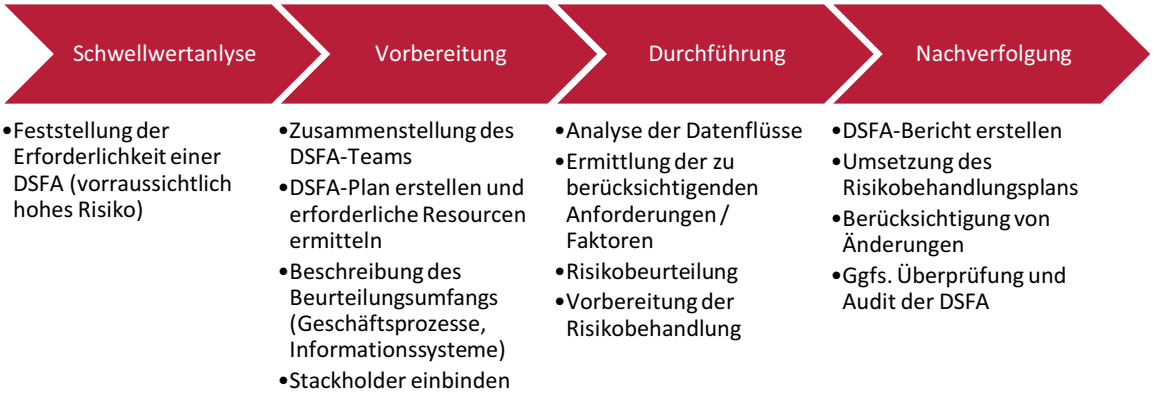

Abbildung 5: DSFA-Prozess nach ISO 29134 (Kranig u. a. 2017:101)

Bei der Schwellwertanalyse wird untersucht, ob sich durch die Datenverarbeitung ein hohes Risiko für die betroffenen Personen ergeben könnte und somit die Notwendigkeit besteht, eine DSFA durchzuführen.

Bei der Durchführung der DSFA werden zuerst Risikoszenarien für mögliche Angriffsziele erstellt. Im Anschluss werden die daraus resultierenden Risiken nach Schadensausmaß und Eintrittswahrscheinlichkeit bewertet, und in Risikobereiche eingeteilt. Je nach Risikobereich können verschiedene Maßnahmen zur Reduzierung des Risikos ergriffen werden, die im Risikobehandlungsplan festgelegt werden.

In der Nachverfolgung wird der Risikobehandlungsplan umgesetzt und die DSFA dokumentiert.

3 Implementierung eines DSMS in ein bestehendes ISMS

Im Folgenden wird beschrieben, wie in der LieferUs GmbH ein DSMS auf der Grundlage eines ISMS implementiert werden kann. Um von vornherein die Vorteile eines prozessorientierten DSMS zu nutzen, wird der PDCA-Zyklus schon bei der Erarbeitung und Umsetzung des DSMS angewendet. Hierfür wird zuerst die aktuelle Situation inklusive des ISMS im Unternehmen erfasst.

Auf Grund der Tatsache, dass das Unternehmen seinen einzigen Firmensitz in Hamburg hat, sind bei der Betrachtung nur die deutschen und europäischen Anforderungen zu beachten.

3.1 Voraussetzungen für die Erweiterung eines ISMS

Um bei der Implementierung eines DSMS die Vorteile, die ein bestehendes ISMS im Unternehmen bietet, nutzen zu können, müssen durch das ISMS folgende Anforderungen im Unternehmen bereits erfüllt sein (Kranig et al., 2017, Kap. 10.4.1):

- Durch das bestehende ISMS muss im Unternehmen bereits eine einheitliche Struktur für Managementsysteme etabliert sein. Hierbei ist es von Vorteil, wenn sich diese Struktur an der ISO-„High-Level-Struktur“ orientiert, einer übergeordneten Gliederung für die Vereinheitlichung neuer und überarbeiteter ISO-Standards (Staska, 2015). Hierdurch können auch weiterer ISO-Managementsysteme leichter umgesetzt werden.
- Die in der ISO 27002 geforderten Sicherheitsmaßnahmen müssen vollständig umgesetzt sein, da hierdurch auch bereits ein großer Anteil der datenschutzrelevanten TOMs umgesetzt ist.
- Im Unternehmen muss ein unternehmensweites Risikomanagement existieren.
- Die Strukturen für regelmäßige Bewertungen und Überprüfungen der Wirksamkeit von getroffenen Maßnahmen im ISMS müssen vorhanden sein.
- Im Rahmen des ISMS muss ein Prozess der kontinuierlichen Verbesserung von Managementsystemen nach dem Vorbild des KVP etabliert sein.
- Im Unternehmen muss ein Dokumentenmanagementsystem etabliert sein.

Dadurch, dass das ISMS der LieferUs GmbH nach ISO 27001 zertifiziert wurde, sind die oben aufgeführten Punkte bereits im Unternehmen umgesetzt.

Insbesondere die Erweiterung des ISMS um TOMs des Datenschutzes macht aus einem ISMS ein integriertes DSMS. Hierfür bietet es sich an, die ISO 29151 zu nutzen. Die ISO 29151 bezieht sich auf die in der ISO 29100 definierten Datenschutzgrundsätze und empfiehlt darauf aufbauende Datenschutz-Maßnahmen, die mit der ISO 27002 kompatibel sind (ISO 29151 2017).

3.2 Bestandsaufnahme

Mit den in Kapitel 2.1 beschriebenen Methoden wird der bestehende Datenschutz im Unternehmen analysiert. Um einen ersten Überblick über die Datenschutzsituation im Unternehmen zu erlangen, wird zusammen mit der Geschäftsführung die Datenschutzcompliance mittels GAP-Analyse ermittelt. Bei der weiteren Bestandsaufnahme werden durch die in Kapitel 2.1.2 beschriebenen Interviews mit Hilfe von Fragebögen die datenschutzrelevanten Prozesse in den Abteilungen aufgenommen.

3.2.1 Planung

Um einen reibungslosen Ablauf der Bestandsaufnahme zu ermöglichen, muss dieser zusammen mit dem Unternehmen geplant werden. Hierfür wird zunächst ein Termin mit der Geschäftsführung und dem Datenschutzbeauftragten zur Klärung der Rahmenparameter und Durchführung der GAP-Analyse vereinbart. Im Anschluss wird ein Zeitplan für die Durchführung der Interviews erstellt, der zwei Tage umfasst und an die Gegebenheiten im Unternehmen angepasst ist.

Tabelle 2: Zeitplan für die Interviews

Tag 1				
Thema	Ansprechpartner	E-Mail-Adresse	Dauer (Stunden)	Uhrzeit (circa)
Vorgespräch mit der Geschäftsführung			1, 5	
Buchhaltung/ Personal			1	
Rechtsabteilung			2	
Datenschutzbeauftragter			3	

Tag 2				
Thema	Ansprechpartner	E-Mail-Adresse	Dauer (Stunden)	Uhrzeit (circa)
Marketing/ Vertrieb			3	
Einkauf			1	
Informationstechnik			2	
Abschlussgespräch mit der Geschäftsführung			1	

In Absprache mit dem Unternehmen werden die Termine und Ansprechpartner der zu befragenden Abteilungen und Bereiche vereinbart, und die für die Befragung benötigten Dokumente bereitgestellt. Bei diesen handelt es sich um ADV-Verzeichnisse und ADV-Verträge, sowie Verfahrensverzeichnisse, auf denen das DSMS später aufbaut.

3.2.2 Durchführung

Die Bestandaufnahme wird gemäß dem vereinbarten Zeitplan durchgeführt, wobei vorab die GAP-Analyse durchzuführen ist. Das erste Interview wird ebenfalls mit der Geschäftsführung geführt, um den Kontext, das Kerngeschäft und Zuständigkeiten im Unternehmen zu erfahren.

Die Abteilungen Marketing und Vertrieb werden erst am zweiten Tag befragt, um die Informationen, die sich aus dem Gespräch mit der Geschäftsführung ergeben haben, vorher auswerten und für die weiteren Interviews nutzen zu können. Als letztes wird die IT-Abteilung befragt, um die Fragen bezüglich der TOMs gezielt nach den in den vorherigen Gesprächen identifizierten, relevanten IT-Systemen und Software-Anwendungen stellen zu können. Wenn alle benötigten Daten erhoben wurden, findet ein Abschlussgespräch mit der Geschäftsführung statt, um die Ergebnisse der Bestandsaufnahme zu präsentieren.

3.2.3 Auswertung

Um die während der Bestandaufnahme erhobenen Daten für die Implementierung eines DSMS nutzen zu können, müssen diese ausgewertet und in eine sinnvolle Struktur gebracht werden.

Die Auswertung der GAP-Analyse erfolgt automatisch in Excel und findet vor der Durchführung der Interviews statt. Hierfür werden die Daten aus dem Fragebogen in einem Netzdiagramm dargestellt. Die Bereiche, in denen Handlungsbedarf besteht, werden in die Planung und Durchführung der Interviews mit aufgenommen.

Für die LieferUs GmbH ergibt die GAP-Analyse folgendes Bild:

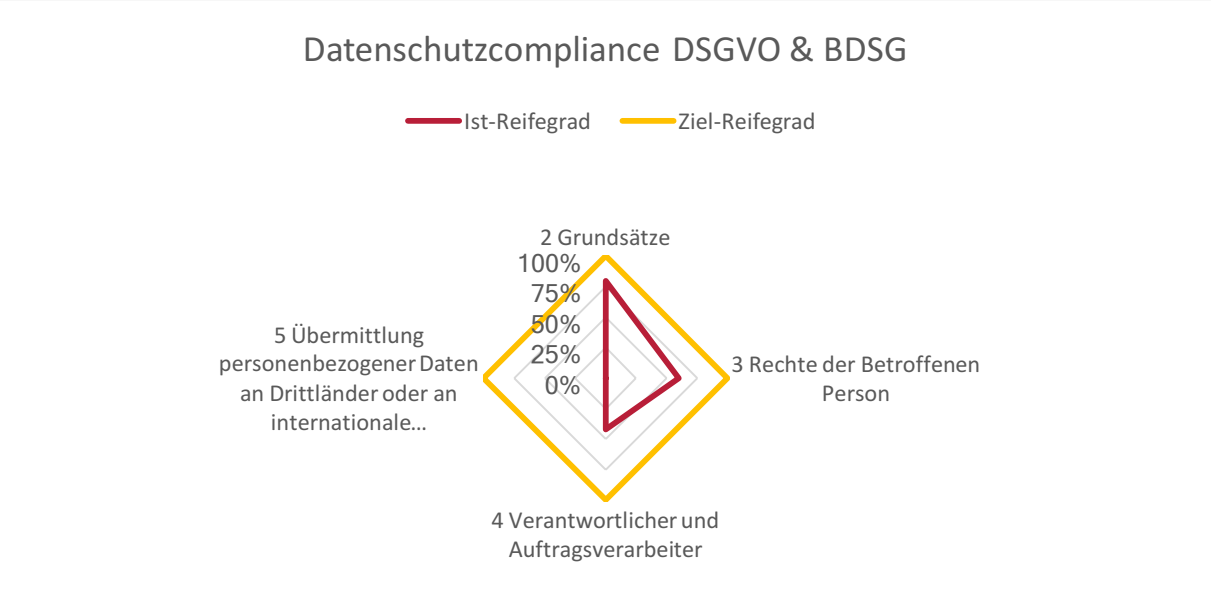

Abbildung 6: Auswertung der GAP-Analyse der LieferUs GmbH

Anhand dieser Auswertung ist zu sehen, dass es im Unternehmen noch große Abweichungen im Bereich „Verantwortlicher und Auftragsdatenverarbeiter“ zum Ziel-Reifegrad gibt. Der Punkt 5 „Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen“ wurde bei der GAP-Analyse nicht betrachtet, da die LieferUs GmbH keine personenbezogenen Daten außerhalb des europäischen Wirtschaftsraumes verarbeitet. Für die Implementierung des DSMS ergibt sich hieraus ein geschätzter Aufwand von 70 Tagen. Diese Schätzung orientiert sich an Erfahrungswerten der ANMATHO AG für die Implementierung eines ISMS in einem vergleichbaren Unternehmen (Westerkamp, 2017).

Bei der Auswertung der Interviews werden die Ergebnisse in mehrere Dokumente übertragen. Sämtliche aufgenommenen Prozesse und Datenverarbeitungen werden in einem Verarbeitungsverzeichnis zusammengeführt. Bereits existierende Verfahrensverzeichnisse werden dabei aktualisiert und in ein unternehmensweites Verarbeitungsverzeichnis überführt. Dieses Verarbeitungsverzeichnis bildet die Grundlage des DSMS, da aus diesem alle relevanten Prozesse, die personenbezogene Daten verarbeiten, ersichtlich sind. Alle Verträge zur ADV werden in einer ADV-Dienstleistungsübersicht aufgelistet und in diesem Zuge zusammen mit der Rechtsabteilung überprüft, ob sie den Anforderungen der DSGVO schon genügen oder angepasst werden müssen. Des Weiteren werden die betrachteten Datenverarbeitungen bezüglich der Notwendigkeit einer DSFA bewertet. Diese Bewertung wird ebenfalls dokumentiert, um später einen Nachweis darüber erbringen zu können.

3.3 Implementierung

Anknüpfend an die Bestandsaufnahme werden im nachfolgenden Kapitel die Ergebnisse dieser und die sich aus den rechtlichen Anforderungen ergebenden Bestimmungen an ein DSMS zusammengeführt und im Unternehmen etabliert. Hierfür muss zunächst die Aufbauorganisation und Ablauforganisation des DSMS in das ISMS integriert werden.

Um den Geltungsbereich des DSMS festzulegen, müssen Datenschutzziele durch die Geschäftsführung definiert und fixiert werden. Als nächstes müssen die Prozesse und Verfahren, bei denen personenbezogene Daten verarbeitet werden, identifiziert werden. Aus den Datenschutzzielen ergeben sich eine Reihe von Maßnahmen für den Schutz personenbezogener Daten in den identifizierten Prozessen und Verfahren, die im Rahmen des DSMS umgesetzt werden müssen. Hierfür müssen ausreichend Ressourcen bereitgestellt werden.

3.3.1 Aufbauorganisation (Datenschutzstrukturen)

In Bezug auf den Datenschutz beschreibt die Aufbauorganisation des DSMS die im Unternehmen benötigten Ziele und Strukturen, um die gesetzlichen Anforderungen der DSGVO und des DSAnpUG-EU erfolgreich umzusetzen.

3.3.1.1 Datenschutzziele

Für die LieferUs GmbH wurden in Zusammenarbeit mit der Geschäftsführung folgende Datenschutzziele vereinbart:

- Die von den Kunden zur Verfügung gestellten Daten werden nur zum vereinbarten Zweck genutzt.
- Die Vertraulichkeit der gespeicherten Daten wird unter allen rechtlichen Umständen geschützt und gewahrt.
- Die Richtigkeit der personenbezogenen Daten wird zu jedem Zeitpunkt garantiert.
- Alle nationalen und internationalen Gesetze und Regeln werden eingehalten.
- Rechtliche Vorgaben haben grundsätzlich und zu jeder Zeit Vorrang vor allen Entscheidungen im Sinne unternehmerischer Anforderungen.

Hierbei ist besonderes Augenmerk auf das Spannungsfeld zwischen verschiedenen Unternehmenszielen zu legen. So kann es beispielsweise Zielkonflikte zwischen den Datenschutzzielen und den Marketingzielen geben, da die Datenschutzziele vorschreiben, möglichst sparsam und zweckgebunden mit den personenbezogenen Daten umzugehen, wohingegen nach den Marketingzielen möglichst alle zur Verfügung stehenden Daten zu Werbezwecken genutzt werden sollten. Lösen lässt sich solch ein Konflikt, indem die Unternehmensziele wie oben geschrieben aussagen, dass rechtliche Vorgaben vor unternehmerischen Anforderungen Vorrang haben.

3.3.1.2 Datenschutz-Governance-Struktur

Um die Anforderungen, die der Datenschutz an ein Unternehmen stellt, erfüllen zu können, sind entsprechende Ressourcen notwendig. Diese Ressourcen benötigen, damit sie ihren Aufgaben nachkommen können, gewisse Kompetenzen und Befugnisse. Die Planung der nötigen Ressourcen hängt stark von der Unternehmensgröße ab.

Auf Grund dessen, dass das ISMS bereits beim CSO der LieferUs GmbH angesiedelt ist, wird er als Verantwortlicher für den Datenschutz benannt und ist damit ebenfalls verantwortlich für das DSMS.

Da die LieferUs GmbH mehr als 10 Mitarbeiter hat, die regelmäßig automatisiert personenbezogene Daten verarbeiten, ist nach BDSG bereits ein Datenschutzbeauftragter im Unternehmen benannt. Das Fachwissen des Datenschutzbeauftragten soll für den Aufbau eines DSMS genutzt werden. Aus diesem Grund steht er dem CSO beratend zur Seite.

3.3.1.3 Datenschutzleitlinie und Richtlinien

Die Datenschutzleitlinie ist die Selbstverpflichtung des Unternehmens zur Umsetzung des Datenschutzes. Sie bildet somit den strategischen Rahmen für das DSMS. Für die Leitlinie bietet sich folgende Struktur an (Kranig et al., 2017, S. 36; Loomans et al., 2014, S. 82):

- Kurzbeschreibung der Datenschutzleitlinie
- Einführung / Motivation
- Anwendungsbereich
- Benennung der wichtigsten gesetzlichen Vorschriften und sonstige Grundlagen für die Ableitung der Datenschutzziele
- Datenschutzziele des Unternehmens
- Governance-Struktur
- Verweis auf operative Umsetzung (z.B. mittels DSMS)
- Konsequenzen bei Verstößen
- Dokumentenlenkung (Eigentümer, Revisionszyklen, Definitionen, etc.)

Neben der Datenschutzleitlinie besteht die Dokumentation noch aus weiteren Dokumenten mit Bezug zum Datenschutz. Es hat sich als nicht praktikabel erwiesen, sämtliche Richtlinien und Regelwerke in der Datenschutzleitlinie zusammenzufassen. Hierdurch würden Anpassungen und Erweiterungen erschwert, da Änderungen der Datenschutzleitlinie der Zustimmung der Geschäftsführung bedürfen. Sinnvoller ist es die Themen, die einer häufigen Anpassung bedürfen - wie beispielsweise die Nutzung mobiler Endgeräte - in Richtlinien festzuschreiben, und in der Datenschutzleitlinie dann auf die Richtlinien in ihrer jeweils gültigen Fassung zu verweisen.

3.3.1.4 Verpflichtungserklärung

Damit das DSMS in allen Bereichen des Unternehmens zur Anwendung kommt, muss es für das gesamte Unternehmen verpflichtend eingeführt werden. Dieses wird durch die Verpflichtungserklärung zum DSMS zwischen der LieferUs GmbH und seinen Mitarbeitern gewährleistet. Zudem soll die Verpflichtungserklärung dazu beitragen, ein allgemeines Bewusstsein für den Datenschutz im Unternehmen zu schaffen. Neben der allgemeinen Verpflichtung zur Nutzung des DSMS werden die Mitarbeiter auch zum Datengeheimnis verpflichtet, welches ein elementarer Bestandteil des Datenschutzes ist.

3.3.2 Ablauforganisation (Datenschutzprozesse)

Die Ablauforganisation des DSMS beschreibt die im Unternehmen relevanten Datenschutzprozesse, welche für die Umsetzung der gesetzlichen Anforderungen benötigt werden.

3.3.2.1 Verarbeitung personenbezogener Daten

Bei der LieferUs GmbH gibt es nicht nur einen Prozess, der personenbezogene Daten verarbeitet, sondern eine Vielzahl von Prozessen. Jeder dieser Unternehmensprozesse muss auf die Einhaltung der folgenden Vorgaben geprüft werden (Kranig et al., 2017, S. 37):

- Bei der Erhebung und Verarbeitung personenbezogener Daten müssen die Datenschutzgrundsätze eingehalten werden (Art. 5 Abs.1,2 DSGVO).
- Die Rechtmäßigkeit der Verarbeitung muss auf Basis einer Rechtsgrundlage sichergestellt sein (Art. 6 DSGVO).
- Betroffene Personen müssen ausreichend über die Verarbeitung ihrer personenbezogenen Daten informiert werden (Art.12 DSGVO).
- Jeder Prozess muss die Sicherheit der Verarbeitung durch geeignete TOMs gewährleisten (Art. 24, 32 DSGVO).
- Falls im Rahmen eines Prozesses ADV vorkommt, muss diese durch geeignete TOMs geschützt werden (Art. 28 DSGVO).
- Wenn personenbezogene Daten in Drittländer übermittelt werden, muss ein ausreichendes Schutzniveau sichergestellt werden (Art. 44 DSGVO).
- Die Verarbeitungstätigkeiten müssen dokumentiert werden (Art. 30 DSGVO).

3.3.2.2 Risikomanagement

Für sämtliche Verarbeitungsvorgänge, die bei der Bestandaufnahme erkannt wurden, wird eine Risikobewertung gemäß Risikomanagement durchgeführt und dokumentiert. Sollte das Ergebnisse ein hohes Datenschutzrisiko für die Betroffenen darstellen, so wird eine DSFA durchgeführt und die daraus resultierenden Maßnahmen umgesetzt. Sollte die Durchführung der DSFA ergeben, dass bei der Verarbeitung der personenbezogenen Daten ein inakzeptables Risiko für die Betroffenen entsteht, so sind die Datenschutzaufsichtsbehörden anzurufen.

Diese hat die Möglichkeit, nach einer eigenen Bewertung der Situation technische und / oder organisatorische Auflagen für den betreffenden Verarbeitungsvorgang anzuordnen. Ist die Datenschutz-aufsichtsbehörde zu dem Schluss gekommen, dass es keine sinnvollen TOMs zur Reduktion des Risikos gibt, hat sie das Recht, die Verarbeitung zu untersagen.

3.3.2.3 Sicherstellung der Betroffenenrechte

Grundsätzlich hat jedes Unternehmen eine allgemeine Informationspflicht gegenüber Betroffenen (Art. 12 – 14 DSGVO). Zudem haben Betroffen nach der DSGVO folgende Rechte:

- Auskunftsrecht der betroffenen Person (Art. 15)
    - Jeder Betroffene hat das Recht, Auskunft über die Art und Verarbeitung seiner personenbezogenen Daten zu erhalten.
- Recht auf Berichtigung (Art.16)
    - Jeder Betroffene hat das Recht, unrichtige personenbezogene Daten unverzüglich korrigieren oder ergänzen zu lassen.
- Recht auf Löschung ("Recht auf Vergessenwerden") (Art. 17)
    - Jeder Betroffene hat das Recht, die unverzügliche Löschung seiner Daten zu verlangen, wenn die personenbezogenen Daten nicht mehr vom Unternehmen benötigt werden.
- Recht auf Einschränkung der Verarbeitung (Art. 18)
    - Jeder Betroffene kann die Nutzung seiner personenbezogenen Daten unter bestimmten Voraussetzungen einschränken.
- Recht auf Datenübertragbarkeit (Art. 20)
    - Jeder Betroffene hat das Recht, die von ihm bereitgestellten Daten in einem strukturierten und maschinenlesbaren Format zu erhalten.
- Widerspruchsrecht (Art. 21)
    - Jeder Betroffene hat das Recht, Widerspruch gegen die Erhebung und Verarbeitung personenbezogener Daten zu erheben.

- Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art. 22)
    - Jeder Betroffene hat das Recht, nicht einer ausschließlich auf automatisierten Verarbeitungen – einschließlich Profiling – beruhenden Entscheidung unterworfen zu sein.
- Recht auf Widerruf einer Einwilligung (Art. 7 Abs. 3)
    - Jeder Betroffene hat jederzeit das Recht, eine einmal gegebene Einwilligung zur Verarbeitung von personenbezogenen Daten zu widerrufen. Hierbei muss der Widerruf genauso einfach möglich sein, wie die Erteilung der Einwilligung.

Diese Rechte müssen bei der LieferUs GmbH sichergestellt werden. Hierfür kann zum einen das Verarbeitungsverzeichnis mit allen im Unternehmen vorhanden Verarbeitungsprozessen personenbezogener Daten genutzt werden. Mittels dieses Verzeichnisses ist die LieferUs GmbH in der Lage, Betroffenen Auskunft über die Art der Verarbeitung personenbezogener Daten zu geben. Ferner müssen Prozesse zur Korrektur, Löschung und Einschränkung der Verarbeitung personenbezogener Daten etabliert werden.

3.3.2.4 Handhabung von Datenschutzverletzungen

Sollte es trotz der vorhandenen Prozesse zur Sicherstellung des Datenschutzes zu einer Datenschutzverletzung kommen, hat der Verantwortliche eine Meldepflicht gegenüber der Aufsichtsbehörde. Um dieser Meldepflicht nachzukommen, muss er unverzüglich, spätestens jedoch nach 72 Stunden, eine Meldung abgeben (Art. 33 Abs. 1 DSGVO). In der Meldung müssen folgende Angaben enthalten sein:

- Die Art der Verletzung des Schutzes personenbezogener Daten mit den Angaben, unter welche Kategorien die betroffenen Personen fallen, wie viele Personen betroffen sind und die ungefähre Anzahl und Art der betroffenen Datensätze
- Die Kontaktdaten inklusive Namen des Datenschutzbeauftragen
- Die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

- Die von der LieferUs GmbH getroffenen oder geplanten Maßnahmen zur Behebung der Datenschutzverletzung, sowie gegebenenfalls Maßnahmen, die die nachteiligen Auswirkungen mildern können

Die Information der Betroffenen über eine Datenschutzverletzung muss laut Art. 34 Abs. 1 DSGVO unverzüglich erfolgen, wenn von der Datenschutzverletzung ein hohes Risiko für die Betroffenen ausgeht. Hier wird jedoch keine Frist genannt. Ist dies erforderlich, muss die Meldung an die betroffenen Personen die folgenden Angaben in klarer und leicht verständlicher Sprache enthalten:

- Die Art der Verletzung des Schutzes personenbezogener Daten
- Die Kontaktdaten inklusive Namen des Datenschutzbeauftragen
- Die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- Die von der LieferUs GmbH getroffenen oder geplanten Maßnahmen zur Behebung der Datenschutzverletzung, sowie gegebenenfalls Maßnahmen, die die nachteiligen Auswirkungen mildern können

3.3.3 Datenschutz-Folgeabschätzung

Um für den Fall, dass die Risikobewertung der Datenverarbeitungen zu dem Ergebnis führt, dass die Verarbeitung personenbezogener Daten ein hohes Risiko für die Sicherheit der Rechte der betroffenen Personen birgt, eine DSFA durchführen zu können, sollte diese bereits mit Einführung des DSMS im Unternehmen etabliert werden.

3.3.3.1 Schwellwertanalyse und Vorbereitung

Die Schwellwertanalyse ist Teil des allgemeinen Datenschutzrisikomanagements. Sie ist folglich der DSFA vorangestellt, wird hier aber zum besseren Verständnis als Teil dieser mit aufgeführt.

Folgende Kriterien können auf ein hohes Risiko bei der Verarbeitung von personenbezogenen Daten hinweisen (Datenschutzkanzlei, 2017; Wybitul und Ströbel, 2016):

- Neue Technologien
- Neue Verarbeitungen
- Verarbeitung großer Datenmengen
- Sensibilität der Daten
- Profiling
- Erschwerte Rechtsausübung
- Systematische Verarbeitungen
- Öffentliche Überwachung
- Datentransfers außerhalb der EU
- Daten schutzbedürftiger Personen (Kinder, ältere Menschen, Patienten oder Mitarbeiter)

Die Artikel-29-Datenschutzgruppe der EU empfiehlt, dass mindestens zwei der oben genannten Kriterien erfüllt sein sollten, um eine DSFA verpflichtend durchführen zu müssen (Artikel-29-Datenschutzgruppe, 2017). Des Weiteren sind die Datenschutzaufsichts-behörden dazu angehalten, sogenannte Black- and White-Lists zu erstellen, anhand derer Verarbeitungsvorgänge mit hohem Risiko identifiziert werden und eine einheitliche Bewertung hinsichtlich des Risikos der Datenverarbeitung ermöglicht werden kann. Auf der Black-List (Art. 35 Abs. 4 DSGVO) werden Datenverarbeitungen aufgeführt, für die zwingend eine DSFA durchgeführt werden muss. Auf der White-List (Art. 35 Abs. 5 DSGVO) werden die Datenverarbeitungen aufgeführt, für die keine DSFA erforderlich ist. Bis diese Listen durch die Datenschutzaufsichtsbehörden veröffentlicht werden, werden die oben genannten Kriterien sowie die Empfehlung der Artikel-29-Datenschutzgruppe zur Bewertung des Risikos bei der Verarbeitung personenbezogener Daten herangezogen.

Handelt es sich bei der betrachteten Datenverarbeitung um einen Vorgang mit hohem Risiko, muss folglich eine DSFA durchgeführt werden. Hierfür sind in der Vorbereitung die Personen zu ermitteln, die die DSFA durchführen sollen. In jedem Fall gehört der Datenschutzbeauftragte zu diesem Personenkreis (Klug, 2016). Weiterhin ist ein Durchführungsplan zu erstellen, sowie die benötigten Ressourcen zu ermitteln.

Zudem müssen die zu betrachtenden Geschäftsprozesse und Informationssysteme festgelegt werden. Im Anschluss daran werden die sogenannten Stakeholder (u.a. relevante Bereiche und Abteilungen, Betriebsrat und eventuell betroffene Personen) einbezogen (Kranig et al., 2017, S. 100).

3.3.3.2 Durchführung

Um die Risiken einer Datenverarbeitung umfassend ermitteln zu können, müssen zuerst Risikoszenarien und die daraus resultierenden Folgen erkannt werden. Um nach Möglichkeit alle denkbaren Szenarien erfassen zu können, wird wie in Abbildung 7 dargestellt vorgegangen. Als erstes werden die möglichen Risikoquellen identifiziert, die sowohl von innerhalb des Unternehmens als auch von externen Quellen ausgehen können. Im Anschluss wird betrachtet, welche Handlungen und Aktionen die Risikoquellen in Verbindung mit den unterstützenden Werten ausführen können. Aus den so identifizierten Bedrohungen werden in einem weiteren Schritt die möglichen negativen Folgen bewertet (Kranig et al., 2017, S. 103).

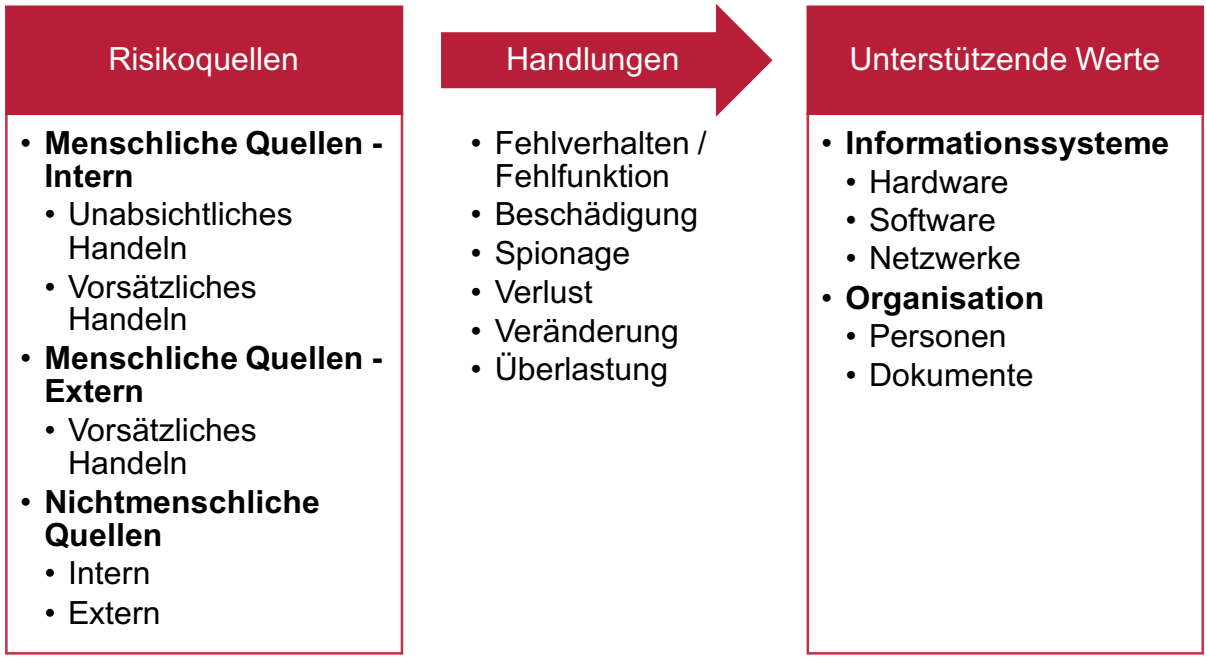

Abbildung 7: Risikoidentifikation (Kranig et al., 2017, S. 103)

Die DSGVO gibt in ErwG. 75 Beispiele für Datenschutzrisiken, die zu einem Schaden führen können, wie beispielsweise Diskriminierung oder Identitätsdiebstahl.

Um im nächsten Schritt das Risiko zu bewerten, werden das Schadensausmaß und die Eintrittswahrscheinlichkeit jeweils einer von vier Kategorien zugeordnet. Die Einteilung der Schwere des Risikos erfolgt nach den vier Kategorien aus Tabelle 3.

Tabelle 3: Kategorien für die Schwere des Risikos (Kranig et al., 2017, S. 104)

Bereich	Auswirkung auf Betroffene	Folgen überwinden können	Beispiele
1. Vernachlässigbar	Nicht betroffen oder nur kleine Unannehmlichkeiten	Unannehmlichkeiten sollten sich problemlos beheben lassen	Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, Irritationen, etc.
2. Begrenzt	Wesentliche Unannehmlichkeiten	Wesentliche Unannehmlichkeiten sollten sich – trotz gewisser Schwierigkeiten – überwinden lassen	Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, leichte körperliche Beschwerden, etc.
3. Wesentlich	Wesentliche Folgen	Wesentliche Folgen sollten sich – trotz gewisser Schwierigkeiten – überwinden lassen	Missbrauch von Geldern, Blacklisting bei Banken, Sachschäden, Arbeitslosigkeit, Vorladung, Verschlechterung des Gesundheitszustandes usw.
4. Maximal	Wesentliche und / oder irreversible Folgen	Irreversible Folgen sind kaum bzw. nicht überwindbar	Finanzielle Not wie Schulden oder Arbeitsunfähigkeit, langfristige psychische oder körperliche Beschwerden, Tod usw.

In Tabelle 4 sind die Kategorien für die Einteilung der Eintrittswahrscheinlichkeit dargestellt.

Tabelle 4: Kategorien für die Eintrittswahrscheinlichkeit des Risikos (Kranig et al., 2017, S. 104)

Bereich	Realisierbarkeit der Bedrohung durch die Risikoquelle in Bezug auf einen Vermögenswert	Beispiele
1. Vernachlässigbar	Scheinbar unmöglich	Diebstahl von Papierdokumenten, die in einem von einem Ausweißlesegerät und einem Zugangscode geschützten Raum gelagert sind
2. Begrenzt	Schwierig (machbar mit gewissem Aufwand)	Diebstahl von Papierdokumenten, die in einem durch ein Ausweislesegerät geschützten Raum aufbewahrt werden
3. Wesentlich	Möglich (machbar auch mit geringem Aufwand)	Diebstahl von Papierdokumenten, die in Büros gelagert sind, welche durch Personenkontrollen geschützt sind
4. Maximal	Einfach	Diebstahl von Papierdokumenten, die in einer Lobby liegen

Zur qualitativen Bewertung des Risikos wird die Risikoschwere und die Eintrittswahrscheinlichkeit in der Risikomatrix (Abbildung 8) abgebildet, um so den Risikobereich zu ermitteln.

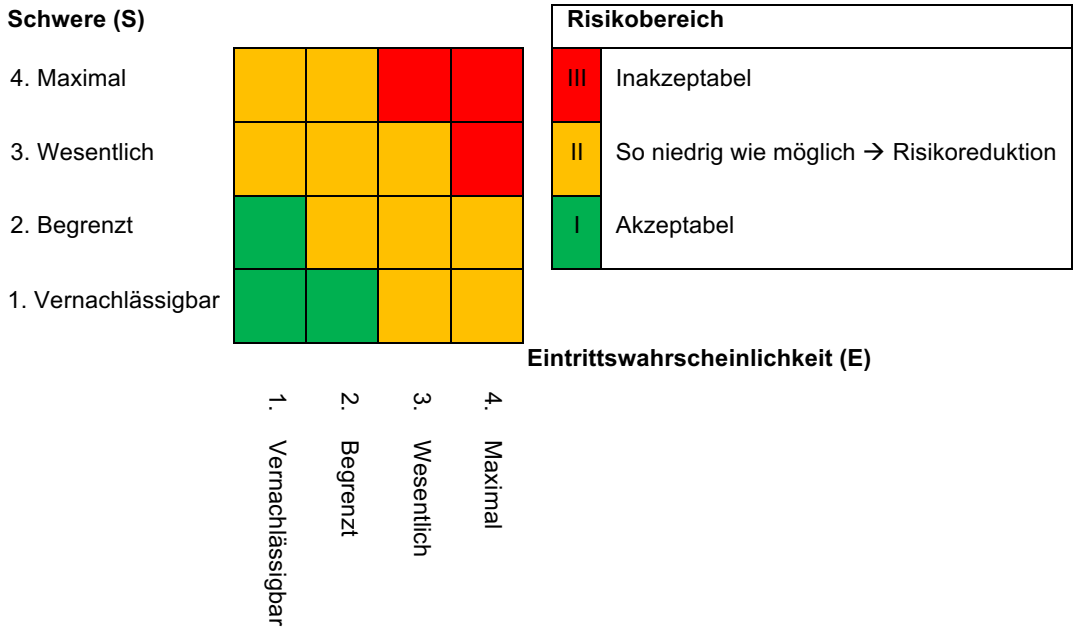

Abbildung 8: Risikomatrix

Je nach Risikobereich kommen verschiedene Risikobehandlungsoptionen in Frage. Grundsätzlich stehen vier Optionen, das Risiko zu minimieren, zur Verfügung (Kranig et al., 2017, S. 106).

- Risikoakzeptanz
    - Wenn sich das Risiko im Risikobereich I befindet, sind keine weiteren Maßnahmen erforderlich.
- Risikoreduktion
    - Wenn sich das Risiko im Risikobereich II befindet, kann es durch angemessene Maßnahmen vermindert werden.
- Risikoübertragung
    - Wenn sich das Risiko im Risikobereich III befindet, und nicht durch eigene geeignete Maßnahmen reduziert werden kann, gibt es die Möglichkeit, das Risiko auf eine externe Partei zu verlagern.

- Risikovermeidung
    - Wenn sich das Risiko im Risikobereich III befindet und es keine Maßnahmen zur Reduzierung des Risikos gibt oder diese in keinem angemessenen Verhältnis stehen, darf die zum Risiko führende Verarbeitung nicht durchgeführt werden.

Nach der Auswahl der geeigneten Risikobehandlungsoption werden angemessene Maßnahmen zur Reduzierung des Risikos festgelegt, und ein Risikobehandlungsplan erstellt. Neben der Risikobewertung muss ebenfalls die Compliance des Verarbeitungsverfahrens sowie der Maßnahmen zur Risikominimierung analysiert werden. Hiermit ist die Bewertung der Einhaltung der bzw. Abweichung von den Datenschutzanforderungen gemeint.

3.3.3.3 Nachverfolgung

Zur Nachverfolgung der DSFA gehört die Umsetzung des Risikobehandlungsplanes, sowie ein DSFA-Bericht, um die Durchführung dieser nachweisen zu können. Der Bericht wird parallel zur Durchführung der DSFA verfasst. Nach Art. 35 Abs. 7 DSGVO besteht der DSFA-Bericht mindestens aus den folgenden Punkten:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und oder Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- 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 die Anforderungen der DSGVO eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird

Um diese Punkte in eine sinnvolle und einheitliche Struktur zu bringen, empfiehlt die ISO 29134 für einen DSFA-Bericht folgende Struktur:

- Umfang der DSFA
    - Verarbeitung
        - Übersicht
        - Systemanforderungen
        - Systemarchitektur
        - Wartung und Betrieb
    - Risikokriterien
    - Beteiligte Personen
    - Konsultierte Stakeholder
    - Datenschutzanforderungen
- Risikobeurteilung
    - Risikoquellen
    - Bedrohungen / Eintrittswahrscheinlichkeiten
    - Folgen / Schwere
    - Risikobewertung (Risikomatrix)
    - Compliance-Analyse
- Maßnahmenplan zur Risikobehandlung
- Fazit und Entscheidungen

Zur Nachverfolgung gehört zudem die Berücksichtigung von Änderungen und die Überprüfung der DSFA. Dies hat zur Folge, dass bei Änderungen der Datenverarbeitung oder festgestellten Mängeln an den Maßnahmen zur Risikobehandlung im Rahmen des KVP eine erneute DSFA notwendig wird.

3.3.4 Vereinbarungen

Wenn die LieferUs GmbH Dritte beauftragt, personenbezogene Daten zu verarbeiten, muss diese ADV durch eine ADV-Vereinbarung abgesichert sein. Bereits bestehende ADV-Vereinbarungen müssen auf die Anforderungen der DSGVO überprüft und angepasst werden. Insbesondere die Frage der Funktions- und Haftungsübertragung ist zu beachten (Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.), 2017). Ebenso muss sichergestellt werden, dass die Nutzung der Daten nur zu dem vertraglich vereinbarten Zweck erfolgt, und dieser Zweck durch die Zweckbindung nach Art. 5 Abs. 1 b gedeckt ist. Durch die Zweckbindung wird zudem bestimmt, welche Daten verarbeitet werden und wie lange die Daten gespeichert werden dürfen (Artikel-29-Datenschutzgruppe, 2013). Die Überprüfung der ADV-Vereinbarungen erfolgt in Zusammenarbeit mit der Rechtsabteilung des Unternehmens.

3.3.5 Überprüfung

Sind alle Anforderungen des DSMS eingeführt, muss kontrolliert werden, ob dieses wirklich alle notwendigen Bereiche abdeckt. Hierfür eignet sich eine erneute GAP-Analyse des Datenschutzes im Unternehmen. Eine weitere Möglichkeit der Überprüfung ist die Nutzung von Audits und Datenschutzzertifizierungen. Ein Audit ist ein systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind (DIN EN ISO 19011:2017). Die Auditkriterien für ein DSMS sind die rechtlichen Vorgaben der DSGVO und des neuen BDSG.

Bei Audits wird zwischen internen und externen Audits unterschieden. Interne Audits werden durch das Unternehmen selber, eventuell mit Unterstützung eines Beraters, durchgeführt. Sie dienen der Überprüfung des DSMS und der Vorbereitung auf ein Zertifizierungsaudit. Bei der LieferUs GmbH werden interne Audits durch den Datenschutzbeauftragten durchgeführt, da dieser die nötige Fachkenntnis besitzt und die Überwachung der Einhaltung der Vorgaben zu seinen originären Aufgaben gehört (Artikel-29-Datenschutzgruppe, 2016a).

Externe Audits können entweder durch Auftraggeber oder durch Zertifizierungsstellen durchgeführt werden. Bei einem Audit durch eine Zertifizierungsstelle erlangt das Unternehmen den Nachweis, dass sein Managementsystem den zugrundeliegenden Normen entspricht (Brauweiler et al., 2015, S. 7). Das dadurch erlangte Zertifikat kann als wichtiger Wettbewerbsvorteil genutzt werden. Mittels Audits durch Auftraggeber können sich diese von der Gesetzeskonformität und Funktionsfähigkeit des DSMS im beauftragten Unternehmen überzeugen. Dieses spielt vor allem in der ADV eine wichtige Rolle, da hier das Unternehmen sicherstellen muss, dass der Auftragnehmer alle Vorgaben der DSGVO einhält.

3.3.6 Verbesserung

Da das DSMS ein Managementsystem im Sinne des KVP ist, fließen die Erkenntnisse aus der Überprüfung des DSMS und eventuell durchgeführter DSFAs in die Struktur und Anpassung des DSMS ein. Hierdurch wird eine laufende Anpassung an neue Anforderungen und Strukturen im Unternehmen ermöglicht. Um eine fortwährende Verbesserung des DSMS zu erreichen, sollte eine regelmäßige Überprüfung erfolgen. Dieses kann beispielsweise durch einen internen Auditplan umgesetzt werden. Hierbei muss nicht jedes Mal das gesamte DSMS auditiert werden. Sinnvoller ist es, bei jedem Audit jeweils nur einen Teilbereich des DSMS zu betrachten, da hierdurch eine genauere Betrachtung ermöglicht wird. Um sicherzustellen, dass das gesamte DSMS überprüft wird, wird vorab ein Auditplan festgelegt, aus dem hervorgeht, welche Teilbereiche zu welchem Zeitpunkt auditiert werden.

4 Herausforderungen bei der Umsetzung

Bei der Umsetzung eines DSMS nach der DSGVO gibt es eine Reihe von Herausforderungen, die besonderer Aufmerksamkeit bedürfen. Die größte Herausforderung ist dabei der zeitliche Rahmen für die Umsetzung des DSMS. Die rechtlichen Unsicherheiten, die sich aus der neuen Gesetzgebung ergeben und bei denen die Rechtsprechung noch nicht abschließend geklärt ist, sorgten dafür, dass viele Unternehmen erst spät mit der Umsetzung der DSGVO begonnen haben, und nun trotz des ursprünglich vorgegebenen Zeitraumes von zwei Jahren in Zeitnot geraten. Neben diesem Problem existieren noch eine Reihe weiterer Herausforderungen, die bei der Umsetzung eines DSMS entstehen und im Folgenden erläutert werden.

4.1 Verarbeitungsverzeichnis

Im Verarbeitungsverzeichnis müssen alle Verarbeitungsverfahren, in denen personenbezogene Daten genutzt werden, dokumentiert werden. Hierbei ist die Herausforderung, dass es häufig für ein Verfahren eine Reihe von Prozessvarianten gibt. Diese müssen ebenfalls alle im Verarbeitungsverzeichnis aufgeführt werden.

Die Sicherstellung der Aktualität und der Vollständigkeit des Verarbeitungsverzeichnisses stellt die Unternehmen damit vor ein Problem, da jede Änderung in einem Verarbeitungsverfahren - wozu beispielsweise auch der Einsatz neuer Anwendungen zählt - dokumentiert werden muss. Diese Änderung betrifft nicht nur dieses Verarbeitungsverfahren, sondern auch alle im Unternehmen zum Einsatz kommenden Varianten des Verfahrens.

Um dieses Problem anzugehen sollte ein Änderungsprozess im Rahmen eines Changemanagements etabliert werden, beispielsweise in Form einer Unternehmensrichtlinie, die die Dokumentation jeglicher Verfahrensänderungen im Verarbeitungsverzeichnis vorschreibt. Durch diesen Prozess kann sichergestellt werden, dass alle Prozessänderungen im Verarbeitungsverzeichnis dokumentiert werden.

4.2 Betroffenenrechte

Auch die Umsetzung der Rechte von betroffenen Personen gestaltet sich als schwierig, da die Anforderungen der DSGVO diesbezüglich weitreichender sind als die bisherigen rechtlichen Anforderungen und auch auf bereits erhobene Daten angewendet werden müssen. Dieses betrifft vor allem das Informations- und Transparenzgebot (Art. 12 DSGVO), welches eine Auskunftspflicht gegenüber Betroffenen darstellt. Diesen müssen in leicht zugänglicher Form sowie in klarer und einfacher Sprache Informationen über die Verarbeitung personenbezogener Daten auf Verlangen herausgeben werden. Innerhalb des Unternehmens müssen Prozesse zur Sicherstellung dieses sowie aller anderen Betroffenenrechte implementiert werden.

Das neue Recht auf Datenübertragbarkeit stellt die Unternehmen vor ganz neue Herausforderungen, da sie gewährleisten müssen, dass gespeicherte personenbezogene Daten zwischen verschiedenen Unternehmen übertragen werden können. Um dieses zu ermöglichen sind die Verantwortlichen dazu angehalten, Download-Tools und Anwendungsschnittstellen zu etablieren. Gemäß Art. 20 Abs. 1 DSGVO müssen die personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden. Bisher gibt es keinen einheitlichen Standard für das Dateiformat, in dem die personenbezogenen Daten zur Verfügung gestellt werden können. Es ist sehr unwahrscheinlich, dass sich nur ein Dateiformat durchsetzen wird, da die Anforderungen an das Format je nach Art der personenbezogenen Daten und Anwendung sehr unterschiedlich sein können. (Artikel-29-Datenschutzgruppe, 2016b).

4.3 Kopplungsverbot

Das bereits aus dem BDSG bekannte Kopplungsverbot wird in Art. 7 Abs. 4 DSGVO erheblich verschärft. Dies wird jedoch erst deutlich, wenn der Art. 7 Abs. 4 DSGVO zusammen mit dem ErwG. 43 Satz 2 gelesen wird. Die DSGVO ist in diesem Punkt nicht klar formuliert, da der Art. 7 Abs. 4 die Kopplung nicht expliziert verbietet, der ErwG. 43 Satz 2 jedoch keine andere Interpretation als ein Verbot zulässt (Härting, 2016).

Durch das Kopplungsverbot muss das Unternehmen in Zukunft, wenn es personenbezogene Daten zu verschiedenen Zwecken verarbeiten möchte, für jeden Zweck eine Einwilligung erhalten. Diese Einwilligungen dürfen nicht voneinander abhängig sein. Dies bedeutet, dass es beispielsweise verboten ist, die Teilnahme an einem Gewinnspiel von der Einwilligung zur Nutzung der personenbezogenen Daten für Werbezwecke abhängig zu machen.

Eine mögliche Lösung des Problems ist die Abkopplung der Einverständniserklärung zur Nutzung personenbezogener Daten zu Werbezwecken von dem eigentlichen Verwendungszweck. Dieses hat zur Folge, dass bei oben genannter Gewinnspielteilnahme zum einen die Einverständniserklärung zur Nutzung der personenbezogenen Daten zum Zwecke der Auslosung des Gewinnes und zum anderen eine weitere Einverständniserklärung zur Nutzung der personenbezogenen Daten zu Werbezwecken existieren muss. Hierbei ist zu beachten, dass die Teilnahme am Gewinnspiel auch ohne Einwilligung zur Nutzung der personenbezogenen Daten zu Werbezwecken möglich sein muss.

4.4 Datenschutz-Risikomanagement

Im Bereich des ISMS gibt es definierte Standards, wie eine Risikobewertung durchzuführen ist. Solch einen Standard gibt es für das Datenschutz-Risikomanagement bisher noch nicht. Dies bedeutet für die Unternehmen ein hohes Maß an Unsicherheit, da es noch kein einheitliches Verständnis dafür gibt, wie, in welchem Umfang und mit welchen Maßstäben die Risikobewertung durchzuführen ist. Hier kann durch die Black- und White-Lists der Datenschutzaufsichtsbehörden zumindest in Bezug auf die DSFA eine Rechtssicherheit geschaffen werden.

Durch die Ähnlichkeiten des DSMS und des ISMS kann, bis sich ein einheitlicher Standard für das Datenschutz-Risikomanagement etabliert hat, auf die ISO 27005 zurückgegriffen werden. Diese beschreibt das Risikomanagement in einem ISMS und kann aufgrund der ähnlichen Anforderungen des DSMS als Orientierung genutzt werden.

4.5 Privacy by Default & Privacy by Design

Um die Datenvermeidung und Datensparsamkeit weiter in den Fokus des Datenschutzes zu rücken, wurde mit der DSGVO die Anforderung an die Unternehmen gestellt, durch Technikgestaltung und datenschutzfreundliche Voreinstellungen die Sicherheit der Rechte der Betroffenen weiter zu schützen. In diesem Zusammenhang haben sich die Begriffe „Privacy by Design“ und „Privacy by Default“ etabliert. Die Unternehmen sollen hierbei durch die datenschutzfreundliche Planung, Gestaltung und Umsetzung von Anwendungen und Informations- und Kommunikationssystemen die obengenannten Datenschutzgrundsätze umsetzen. Dies lässt sich durch die proaktive Einbindung des Datenschutzes bereits in der Planungs- und Entwicklungsphase der Anwendungen erreichen. Es erfordert jedoch ein Umdenken bei der Entwicklung neuer Anwendungen, da sich bereits zu Beginn Gedanken über die Sicherstellung der Datenschutzgrundsätze gemacht werden müssen. Darüber hinaus muss sichergestellt werden, dass Anwendungen in den Standardeinstellungen nur personenbezogene Daten verarbeiten, die für den konkreten Zweck erforderlich sind (Voßhoff, 2017, S. 22).

Beispiele für die datenschutzfreundliche Gestaltung von Anwendungen sind die Implementierung sicherer Nutzer-Authentifizierungen, integrierter Verschlüsselungs-methoden und die sparsame Nutzung personenbezogener Daten (Kipker, 2015).

4.6 Unterschiedliche Sichtweisen von ISMS und DSMS

Das Problem bei der Integrierung eines DSMS in ein bestehendes ISMS, ist die unterschiedliche Sichtweise der beiden Managementsysteme. Das ISMS stellt das Unternehmen in den Mittelpunkt der Betrachtung, während das DSMS den Fokus auf die Rechte der Betroffenen legt. Hierdurch kann es potentiell zu Konflikten kommen.

Das ISMS ist bei der LieferUs GmbH zum Schutze der Unternehmensinformationen und zur Minimierung von Unternehmensrisiken implementiert worden. Das DSMS hingegen hat die Aufgabe, die Interessen Dritter zu schützen. Auf den ersten Blick bringt ein DSMS dem Unternehmen daher nicht mehr als die Umsetzung rechtlicher Forderungen, und scheint sogar eine zusätzliche Last darzustellen.

Bei genauerer Betrachtung wird jedoch deutlich, dass Unternehmensabläufe durch die Nutzung eines DSMS effizienter und damit kostengünstiger durchgeführt werden können, sodass die Implementierung eines DSMS durchaus auch einen Vorteil für das Unternehmen schafft (Loomans et al., 2014, S. 25).

5 Diskussion und Fazit

Mit einem DSMS lassen sich die Anforderungen, die die DSGVO an Unternehmen stellt, erfüllen. Der prozessorientierte Ansatz mit KVP und PDCA-Zyklus scheint hierfür sogar so gut geeignet, dass die Vermutung naheliegt, der Gesetzgeber habe bereits bei der Formulierung der Verordnung die Nutzung eines DSMS zur Umsetzung dieser im Sinn gehabt. Die Einbeziehung von informationssicherheitstechnischen Maßnahmen in die erforderlichen TOMs zur Sicherstellung der Rechte der betroffenen Personen in Art. 32 DSGVO lässt zudem darauf schließen, dass der Gesetzgeber zur Sicherstellung des Datenschutzes auch die Informationssicherheit als notwendig erachtet, und somit die Nutzung eines ISMS als Ausgangspunkt für das DSMS bereits im Vorwege bedacht haben könnte. Dennoch gibt es bei der Umsetzung einiger Anforderungen der DSGVO noch Unsicherheiten. Dies hängt zum einen mit den in der DSGVO vorhandenen Öffnungsklauseln zusammen, zum anderen aber auch mit dem Inhalt der DSGVO selbst. So ergeben sich bezüglich Art. 7 Abs. 4 erhebliche rechtliche Inkongruenzen, wie das Kopplungsverbot auszulegen ist, da sich der Artikel und der Erwägungsgrund diesbezüglich widersprechen. Es bleibt abzuwarten, welche Auslegung des Kopplungsverbotes sich durchsetzen wird. Durch die Vielzahl an Öffnungsklauseln kann zudem der Eindruck entstehen, dass die Verordnung gar keine Verordnung sein soll, sondern vielmehr ein Hybrid aus Verordnung und Datenschutzrichtlinie. Dieses kann einerseits so aufgefasst werden, dass auf europäischer Ebene nicht mehr als ein Nebeneinander von europäischem und nationalen Datenschutzrecht gewollt ist (Roßnagel und Barlag, 2017). Andererseits kann der Eindruck entstehen, dass um jeden einzelnen Punkt der Verordnung lange gerungen wurde, und nur durch die Öffnungsklauseln ein Konsens gefunden werden konnte (Albrecht und Jotzo, 2017). Unabhängig davon, welche Annahme zutrifft, wird die Zukunft zeigen, ob die DSGVO zur gewünschten Harmonisierung des Datenschutzes innerhalb der EU führen wird.

Der Zeitrahmen, der durch die DSGVO zur Umsetzung der Anforderungen vorgegeben wurde, stellt die Unternehmen ebenfalls vor Herausforderungen. Der Zeitplan sieht zwar eine Umsetzungsfrist von zwei Jahren vor, aufgrund der rechtlichen Unsicherheiten in der DSGVO und bei der Erstellung des DSAnpUG-EU haben viele Unternehmen mit der Implementierung eines DSMS jedoch gezögert, sodass ihnen für die Umsetzung nun nur noch einige Monate bleiben. So scheint es schwer möglich zu sein, ein vollständig funktionierendes DSMS bis zum Stichtag einzuführen. Aufgrund des KVP ist dies allerdings nicht zwingend erforderlich. Das DSMS muss zwar bis zum 25.05.2018 vollständig eingeführt sein, aber noch keinen allumfassenden Schutz der Rechte der betroffenen Personen gewährleisten, denn durch die regelmäßige Überprüfung und die kontinuierliche Verbesserung des Systems ist sichergestellt, dass Abweichungen zu den Anforderungen identifiziert und behoben werden.

Selbst wenn das DSMS sämtliche Anforderungen erfüllt, kann dennoch keine vollständige Sicherheit der Rechte der betroffenen Personen garantiert werden, da ein DSMS nur die Methoden zur Sicherstellung des Datenschutzes stellt, und diese von Mitarbeitern genutzt werden müssen. Um Datenschutzverletzungen durch Mitarbeiter nach Möglichkeit zu verhindern, sollten diese im Umgang mit den Methoden geschult und für die Thematik Datenschutz sensibilisiert werden. Doch selbst, wenn sich die Mitarbeiter des eigenen Unternehmens vollkommen datenschutzkonform verhalten, ist auch dies keine Garantie für die Sicherstellung des Datenschutzes. Auch Geschäftspartner und Auftragsdatenverarbeiter nutzen personenbezogene Daten, die durch das Unternehmen erhoben wurden, und können dadurch Datenschutz-verletzungen verursachen. Um dieses Risiko zu minimieren, muss sichergestellt werden, dass diese ebenfalls ein wirksames DSMS besitzen. Zum Nachweis der Wirksamkeit ist die Zertifizierung des DSMS sinnvoll und für die Erhöhung des Datenschutzniveaus innerhalb der EU unerlässlich. Hierfür sollten geeignete Zertifikate etabliert werden.

Abschließend lässt sich sagen, dass es möglich ist, bei der Einführung und dem Betrieb eines DSMS auf vorhandene Managementsysteme zurückzugreifen. Besonders der Aufbau auf einem ISMS nach ISO 27001 macht Synergieeffekte auf Grund der sehr ähnlichen Anforderungen sehr gut nutzbar. Beide Managementsysteme sind nach der ISO-„High-Level-Struktur“ aufgebaut und nutzen den KVP zur kontinuierlichen Verbesserung. Zudem wird in beiden Managementsystemen zum Konformitätsnachweis ein Dokumentenmanagement-system eingesetzt. Darüber hinaus verfolgen beide Systeme einen risikobasierten Ansatz bei der Bewertung und Umsetzungen von Maßnahmen. Zwar haben beide Systeme unterschiedliche Zielsetzungen, da jedoch im ISMS auch Maßnahmen zum Datenschutz und im DSMS Maßnahmen der Informationssicherheit zum Schutze personenbezogener Daten gefordert werden, ist eine Kombinierung dieser Beiden nicht nur möglich, sondern überaus empfehlenswert. Alles umfassend stellt das Vorhandensein eines ISMS nach ISO 27001 eine erhebliche Erleichterung bei der Implementierung eines DSMS im Unternehmen dar.

Literaturverzeichnis

Albrecht, J.P., Jotzo, F., 2017. Das neue Datenschutzrecht der EU: Grundlagen, Gesetzgebungsverfahren, Synopse, 1. Auflage. ed, NomosPraxis. Nomos, Baden-Baden.

Artikel-29-Datenschutzgruppe, 2007. Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ (No. WP 136).

Artikel-29-Datenschutzgruppe, 2013. Opinion 03/2013 on purpose limitation (No. WP 203).

Artikel-29-Datenschutzgruppe, 2016a. Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“) (No. WP 243).

Artikel-29-Datenschutzgruppe, 2016b. Leitlinien zum Recht auf Datenübertragbarkeit (No. WP 242).

Artikel-29-Datenschutzgruppe, 2017. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248) (No. WP 248). EU-Kommission.

BGH, 2017. Urteil vom 16. 5. 2017 – VI ZR 135/13.

Borchers, D., 2006. Datenschutzmanagement als Wettbewerbsfaktor. Datenschutz Datensicherheit-DuD 30, 721–724.

Brauweiler, J., Will, M., Zenker-Hoffmann, A., 2015. Auditierung und Zertifizierung von Managementsystemen, essentials. Springer Fachmedien Wiesbaden, Wiesbaden.

BSI, 2012. Leitfaden Informationssicherheit, Bundesamt für Sicherheit in der Informationstechnik. Bonn.

Buchholz, L., 2013. Strategisches Controlling. Springer Fachmedien Wiesbaden, Wiesbaden.

Bundesrat, 2017. Bundesrat Drucksache 332/17.

Bundestag, 2017. Bundestag novelliert das Datenschutzrecht (Pressemitteilung). Deutscher Bundestag.

Datenschutzkanzlei, 2017. Datenschutz-Folgenabschätzung: Erste Kriterien veröffentlicht. Datenschutzkanzlei.

Daum, A., Greife, W., Przywara, R., 2010. BWL für Ingenieure und Ingenieurinnen: was man über Betriebswirtschaft wissen sollte, 1. Aufl. ed, Studium Grundlagen Maschinenbau. Vieweg + Teubner, Wiesbaden.

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 2017. Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017 (No. ISO / IEC 27002:2017).

DIN-Normenausschuss Qualitätsmanagement, Statistik und Zertifizierungsgrundlagen (NQSZ), Quality Management, Statistics and Certification Standards Committee, 2017. Leitfaden zur Auditierung von Managementsystemen (ISO/DIS 19011:2017); Deutsche und Englische Fassung prEN ISO 19011:2017 (Norm No. ISO / DIS 19011:2017).

Düwell, F., 2017. Das Datenschutz-Anpassungs- und -Umsetzungsgesetz | juris Das Rechtsportal. juris.

EuGH, 2013. Urteil vom 30. 5. 2013 – C-342/12.

EU-Kommission, 2015. Einigung über die EU-Datenschutzreform der Kommission wird digitalen Binnenmarkt voranbringen (Pressemitteilung). EU-Kommission.

Europäische Union, 2011. Interinstitutionelle Regeln für Veröffentlichungen, 2011, 2011th ed. Amt für Veröff. der Europ. Union, Luxemburg.

Europäische Union, 2015. Benutzerleitfaden zur Definition von KMU.

Europäisches Parlament, 1995. 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.

Europäisches Parlament, 2016. Parlament verabschiedet EU-Datenschutzreform – EU fit fürs digitale Zeitalter (Pressemitteilung). EU-Parlament.

Feil, T., 2017. Umsetzung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO, Rechtstipp vom 28.02.2017. anwalt.de.

Friedewald, M., Obersteller, H., Nebel, M., Bieker, F., Rost, M., 2016. Datenschutz-Folgeabschätzung (White Paper). forum <privatheit>.

Gadatsch, A., 2017. Grundkurs Geschäftsprozess-Management. Springer Fachmedien Wiesbaden, Wiesbaden.

Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.), 2017. GDD-Praxishilfe DS-GVO IV Vertragsmuster zur Auftragsverarbeitung. Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.), Bonn.

Härting, N., 2016. Kopplungsverbot – der Einwilligungskiller nach der DSGVO. CR-Onlinede Blog.

ISO/IEC JTC 1/SC 27 IT Sicherheitsverfahren, 2011. Information technology — Security techniques — Privacy framework (No. ISO / IEC 29100:2011).

ISO/IEC JTC 1/SC 27 IT Sicherheitsverfahren, 2017. Information technology — Security techniques — Code of practice for personally identifiable information protection (No. ISO / IEC 29151).

Jacob, M., 2013. Management und Informationstechnik. Springer Fachmedien Wiesbaden, Wiesbaden.

Kersten, H., Klett, G., Reuter, J., Schröder, K.-W., 2016. IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, Edition <kes>. Springer Vieweg, Wiesbaden.

Kipker, D.-K., 2015. Privacy by Default und Privacy by Design. Datenschutz Datensicherheit-DuD 39, 410–410.

Klug, C., 2016. Der Datenschutzbeauftragte in der EU - Maßgaben der Datenschutzgrundverordnung. ZD 2016, 315–318.

Kranig, T., Sachs, A., Gierschmann, M., 2017. Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüfleitfaden für Aufsichtsbehörden. Bundesanzeiger Verlag, Köln.

Kühling, J., Buchner, B., Bäcker, M., 2017. Datenschutz-Grundverordnung: Kommentar. C.H. Beck, München.

Kühling, J., Martini, M., Heberlein, J., Kühl, B., Nink, D., Weinzierl, Q., Wenzel, M., 2016. Die Datenschutz-Grundverordnung und das nationale Recht: erste Überlegungen zum innerstaatlichen Regelungsbedarf, MV-Wissenschaft. Verlagshaus Monsenstein und Vannerdat, Münster.

Lachner, T.M., 2007. Das Artikelgesetz, Beiträge zum Parlamentsrecht. Duncker & Humblot, Berlin.

Lambertz, P., 2016. DSGVO: Anforderungen Datenschutz-Management-System. Datenschutz Praxis.

Loomans, D., Matz, M., Wiedemann, M., 2014. Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems: ein risikobasierter Ansatz für alle Unternehmensgrößen. Springer Vieweg, Wiesbaden.

Loomans, D., Wichtermann, M., Matz, M., 2010. Anforderungen an ein Datenschutz-Managementsystem. Loomans & Matz AG, Mainz.

Marschall, K., Müller, P., 2016. Der Datenschutzbeauftragte im Unternehmen zwischen BDSG und DS-GVO. Bestellung, Rolle, Aufgaben und Anforderungen im Fokus europäischer Veränderungen. ZD 2016, 415–421.

Roßnagel, A., Barlag, C., 2017. Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts, 1. Auflage. ed, NomosPraxis. Nomos, Baden-Baden.

Rost, M., 2013. Datenschutzmanagementsystem. Datenschutz Datensicherheit - DuD 37, 295–300.

Schneider, V., 2004. Organizational Governance — Governance in Organisationen. In: Governance — Regieren in komplexen Regelsystemen, Governance. VS Verlag für Sozialwissenschaften, pp. 173–192.

Sowa, A., 2017. Management der Informationssicherheit. Springer Fachmedien Wiesbaden, Wiesbaden.

Staska, H., 2015. Normenwissen kompakt: High Level Structure (HLS). C.O.M.E.S.

Völker, J., 2004. BS 7799–Von „Best Practice “zum Standard. DuD 2, 102–108.

Voßhoff, A., 2017. Datenschutz-Grundverordnung BfDI – Info 6.

Westerkamp, C., 2017. Gespräch über den Zeitlichen Aufwand der Implementierung eines DSMS.

Wybitul, T., 2016. EU-Datenschutz-Grundverordnung in der Praxis – Was ändert sich durch das neue Datenschutzrecht? BB 2016, 1077–1081.

Wybitul, T., Ströbel, L., 2016. Checklisten zur DSGVO – Teil 1: Datenschutz-Folgenabschätzung in der Praxis. BB 2016, 2307–2311.

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit eigenständig und ohne fremde Hilfe angefertigt habe. Textpassagen, die wörtlich oder dem Sinn nach auf Publikationen oder Vorträgen anderer Autoren beruhen, sind als solche kenntlich gemacht. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Hamburg, 27.09.2017

Tobias Malte Kretzmann