MASTERARBEIT

BEST PRACTICE VORGEHEN BEI DER UMSETZUNG DER EU-DATENSCHUTZ-GRUNDVERORDNUNGSVORSCHRIFTEN IN KLEIN- UND MITTELUNTERNEHMEN

ausgeführt am

Studiengang
Informationstechnologien und Wirtschaftsinformatik

Von: Markus Schmölzer, BSc
Personenkennzeichen: 1710320023

Graz, am 19. März 2019 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

An dieser Stelle danke ich allen Personen, die mich bei der Erstellung dieser Masterarbeit unterstützt und motiviert haben.

Zunächst möchte ich mich bei Herrn Dipl.-Ing. (FH) Christian Schmid, MSc für die Betreuung bei der Erstellung dieser Masterarbeit bedanken. Durch sein weitreichendes Fachwissen im Bereich der Datenschutz-Grundverordnung und anderen IT-Sicherheitsthemen, konnte er mir wertvolle Hinweise zur Strukturierung dieser Masterarbeit, dem Methodeneinsatz, der Datenerhebung und der daraus resultierenden Maßnahmengenerierung/-entwicklung bieten.

Ebenfalls möchte ich mich bei den Angestellten der Saubermacher Dienstleistungs AG, für die Unterstützung bei der Durchführung sämtlicher unternehmensrelevanter Erhebungen bedanken. Bei der Ausarbeitung dieser Masterarbeit stellten mir diverse Personen ihr breitgefächertes Fachwissen über Unternehmensprozesse und –abläufe zur Verfügung. Besonders möchte ich mich für die informationsreiche Diskussion zur DSGVO-Umsetzung im Unternehmen bedanken.

Abschließend möchte ich mich bei meiner Familie und meinen Freunden für die Unterstützung und insbesondere für das Korrekturlesen bedanken.

KURZFASSUNG

Besonders im Bereich der Informationstechnologie herrscht eine immerwährende Weiterentwicklung. Neue Technologien oder Vorgehensweisen bringen jedoch neben Verbesserungen jedoch meist auch neue Sicherheitsrisiken mit sich. Um ein einheitliches Sicherheitsniveau bei der Verarbeitung von personenbezogenen Daten im europäischen Raum zu schaffen, wurde die Datenschutz-Grundverordnung (DSGVO) erlassen. Am 25. Mai 2018 ist die DSGVO in Kraft getreten und ein Großteil der Unternehmen musste technische und organisatorische Maßnahmen zur DSGVO Konformität ergreifen. In dieser Masterarbeit wurde die Sammlung von Methoden und Vorgehensweisen zur bestmöglichen Umsetzung der durch die DSGVO vorgeschriebenen Anforderungen behandelt. Daher lautet die Forschungsfrage: „Wie können Klein- und Mittelunternehmen vorgehen um ihre IT-Infrastruktur an die notwendigen Voraussetzungen der Datenschutz-Grundverordnung anzupassen?“. Um die Forschungsfrage zu beantworten, wurde zunächst in der DSGVO bezüglich relevanten Aspekten und wichtigen Vorschriften recherchiert. In einer Zusammenfassung aller wichtigen Bereiche wird ein grundlegendes Wissen zur DSGVO vermittelt. Um Informationen aus der tatsächlichen Praxissituation zu erhalten, wurden fragebogengestützte Experteninterviews mit zehn Datenschutzexperten aus verschiedenen Unternehmen und Tätigkeitsbereichen durchgeführt. Anhand der Ergebnisse aus der Literaturrecherche und den Antworten aus den Experteninterviews wurde eine Best Practice Checklist zur Maßnahmenkontrolle erstellt. Mittels der in dieser Masterarbeit angeführten Informationen sowie der Unterstützung durch die erstellte Best Practice Checkliste werden Unternehmen bzw. Datenschutzverantwortliche bei der Umsetzung der DSGVO-Maßnahmen unterstützt.

ABSTRACT

Rapid and continuous development can be observed in many industries and in IT particularly. New technologies or services, however, usually bring new security risks. In order to create a consistent level of security in the processing of personal data in the European Union, the General Data Protection Regulation (GDPR) was enacted on May 25 2018. Most companies had to implement technical and organisational measures to ensure GDPR conformity. This master thesis deals with the methods and procedures for a best-practice implementation of the requirements prescribed by the GDPR. Therefore, the research question is: "How can small and medium-sized enterprises proceed to adapt their IT infrastructure to the requirements of the General Data Protection Regulation?". In order to answer the research question, first the GDPR itself was researched for relevant aspects and important regulations. A summary of all key areas provides basic knowledge of the GDPR. In order to obtain information from the current practice situation, questionnaire-based expert interviews were conducted with ten data protection experts from various companies and fields of activity. Based on the results of the literature research and the answers from the expert interviews, a best practice checklist was created. The information provided in this master's thesis and the best practice checklist can support companies and data protection officers in the implementation of the GDPR measures.

INHALTSVERZEICHNIS

1 EINLEITUNG

Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet.
(Kovacs, 2012)

Wie Gary Kovacs bereits in seinem TED Talk des Jahres 2012 sagte, ist die Datensicherheit bzw. die Privatsphäre ein wichtiges Gut und darf nicht durch etwaige Tätigkeiten von UserInnen im Internet einer permanenten Gefährdung ausgesetzt sein. Diese Aussage lässt sich auf sämtliche Tätigkeiten, in denen personenbezogene Daten verarbeitet werden, erweitern. Um den personen- bzw. unternehmensbezogenen Datenschutz zu gewährleisten wird fortwährend eine Vielzahl an Richtlinien, Verordnungen und Gesetzen erlassen. In der vorliegenden Masterarbeit wird daher das aktuelle Thema des Datenschutzes im Zusammenhang mit der neuen EU-Verordnung 2016/679 – EU Datenschutz-Grundverordnung (DSGVO) aufgegriffen und ausführlich behandelt. Der primäre Fokus liegt hierbei auf der neuen DSGVO, allerdings werden auch Verbindungen, Ähnlichkeiten sowie relevante Unterschiede zu dem zuvor geltenden Datenschutzgesetz (DSG) 2000 beschrieben und Änderungen des DSG im Laufe der Zeit betrachtet.

Die DSGVO trat mit 25. Mai 2018 in Kraft. Das oberste Ziel der DSGVO ist die Vereinheitlichung des europäischen Datenschutzes. Daher wurde eine Vielzahl neuer Regeln entwickelt und Anforderungen an Firmen gestellt um zukünftig den neuen Datenschutzkriterien zu entsprechen. Bei Verletzungen des Datenschutzes können hohe Bußgelder von den Unternehmen eingefordert werden. Dies ist besonders relevant für Betriebe, die auf sensible Benutzer- bzw. Kundeninformationen Zugriff haben (Wirtschaftskammer Österreich, 2018a).

1.1 Motivation

Da die Datensicherheit auch in meinem persönlichen Arbeitsumfeld ein relevantes Thema ist, möchte ich die DSGVO in meiner Masterarbeit aufgreifen und einer genaueren Betrachtung unterziehen. Aktuell sind die MitarbeiterInnen in meinem Unternehmen damit beschäftigt sämtliche notwendigen Maßnahmen zur DSGVO Konformität umzusetzen. Im Zuge dieser Arbeit wird ein Best Practice Vorgehensmodel, mit allen notwendigen Schritten für die Konformität zur DSGVO, beschrieben werden. Der Fokus wird hierbei primär auf IT-Infrastrukturthemen sowie die technischen und organisatorischen Maßnahmen in diesem Bereich gelegt.

1.2 Hypothesen und Forschungsfrage

Im Zuge dieser Masterarbeit wird eine Best Practice Leitfaden für Klein- und Mittelunternehmen erstellt. Dieser Leitfaden und die dazu gehörende Checklist werden alle Fragen zur Vorgehensweise, bei der sämtliche relevanten IT-Infrastrukturthemen betrachtet werden, beantworten. Die Ausgangsfrage lautet deshalb: „Welche Vorgehensweise soll im Best Practice Fall bei der Umsetzung der EU-Datenschutz-Grundverordnung in Klein- und Mittelunternehmen praktiziert werden?“

Ausgehend von der Ausgangsfrage werden Hypothesen gebildet und in Korrelation gesetzt. Diese befassen sich ebenfalls mit der DSGVO und dem bestmöglichen Vorgehen. So bietet sich beispielsweise als H1 die Hypothese an: „Die Umsetzung der durch die DSGVO vorgeschriebenen Anforderungen führt bei Klein- und Mittelbetrieben branchenübergreifend zu den gleichen grundlegenden Vorgehensweisen“ und als H0 die Hypothese: „Die Umsetzung der durch die DSGVO vorgeschriebenen Anforderungen führt bei Klein- und Mittelbetrieben branchenübergreifend zu unterschiedlichen Vorgehensweisen“.

Die für diese Arbeit behandelte Forschungsfrage lautet:

„Wie können Klein- und Mittelunternehmen vorgehen um ihre IT-Infrastruktur an die notwendigen Voraussetzungen der Datenschutz-Grundverordnung anzupassen?“

1.3 Methodik

Zur Beantwortung der Forschungsfrage werden zunächst alle Vorschreibungen der DSGVO betrachtet und analysiert. Um ein Best Practice Vorgehen beschreiben zu können, werden verschiedene literarische Werke im IT-Datenschutzbereich aufgegriffen. Im Anschluss an die Literaturrecherche werden qualitative Interviews mit IT-Fachleuten aus mehreren Unternehmen geführt. In den Interviews wird die unternehmensinterne Vorgehensweise bei der Umsetzung der DSGVO Richtlinien besprochen. Welche Tätigkeiten die einzelnen Unternehmen durchgeführt haben, um DSGVO konform zu sein, werden danach anhand festgelegter Kriterien verglichen und bewertet. Das Resultat dieser Masterarbeit ist ein branchenunabhängiges Dokument, mit allen notwendigen Schritten, zur Erfüllung der DSGVO.

Im Zuge dieser Arbeit wird eine qualitative empirische Umfrage mittels Experteninterviews durchgeführt. Die Interviews sind durch einen einheitlichen Interviewfragebogen (Leitfaden) gestützt. Dadurch wird die Vergleichbarkeit der in den Experteninterviews gewonnenen Ergebnisse gewährleistet. Insgesamt werden für die vorliegende Masterarbeit zehn Interviews mit IT-Fachleuten aus verschiedenen Branchen durchgeführt.

Zudem wird einschlägige Fachliteratur aus verschiedenen IT Bereichen gewählt. Neben der DSGVO Erläuterung lassen sich die folgenden Themenbereiche in dieser Masterarbeit finden: IT-Infrastruktur, Netzwerktechnik, Backupmethoden und Datenaufbewahrung.

Zur zeitgerechten Umsetzung aller notwendigen Tätigkeiten und Durchführung dieser Masterarbeit wurde folgender Arbeitsplan erstellt:

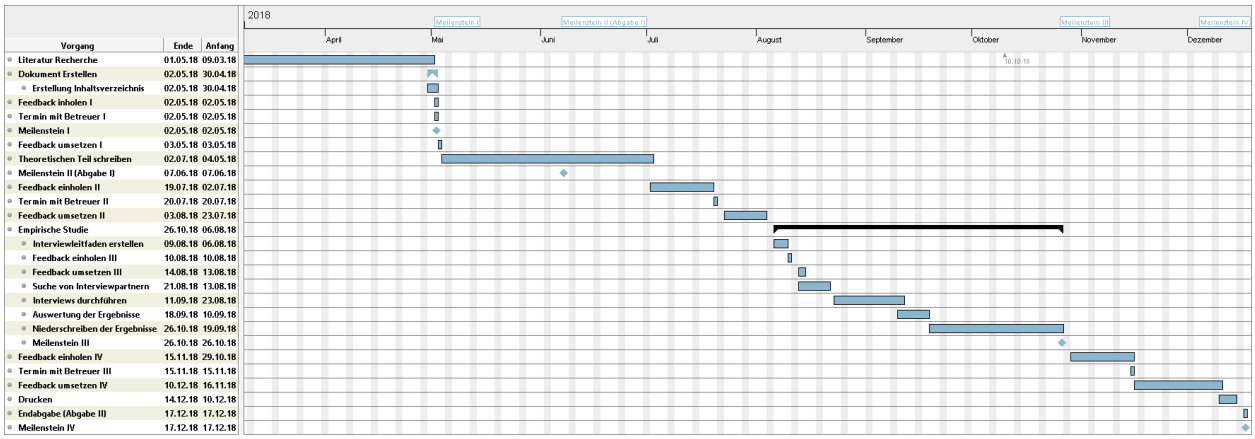

Abbildung 1: Arbeitsplan zur Masterarbeit (Eigene Darstellung)

1.4 Ziel dieser Masterarbeit

Das Ziel dieser Masterarbeit ist die Entwicklung eines Best Practice Leitfadens für die Anpassung der IT-Infrastruktur von klein- und mittelständigen Unternehmen an die DSGVO Vorgaben. Dieser Best Practice Leitfaden basiert auf Informationen aus literarischen Werken, Fachartikeln, Expertenwissen sowie auf Beobachtungen aus dem eigenen Arbeitsumfeld. Da die DSGVO mit 25. Mai 2018 in Kraft getreten ist und viele Unternehmen ihre IT-Infrastruktur für DSGVO-Compliance bis dato bereits überarbeitet haben, wird besonders auf das Expertenwissen und die „lessons learned“ der Experten gesetzt.

1.5 Verwendete Terminologie

Um eine leichtere Verständlichkeit der in der Datenschutz-Grundverordnung verwendeten Terminologie zu unterstützen, werden im Folgenden einige relevante grundliegende Begriffe erläutert.

EU Verordnungen

Wurde vom Rat eine Verordnung angenommen, so gilt diese als verbindlicher Rechtsakt für alle Mitgliedstaaten der EU. Sie müssen die Verordnung im vollen Umfang umsetzen (Europa.Eu, 2018, S. 1).

Richtlinien

Als Richtlinien werden Rechtsakte bezeichnet, die für alle EU-Mitgliedsstaaten zu erreichende Ziele festlegen. Wie diese Ziele erreicht bzw. welche Maßnahmen zur Verwirklichung eingesetzt werden, obliegt den Mitgliedsstaaten. Im Zuge einer EU-Richtlinie können die EU-Länder eigene Rechtsvorschriften erlassen (Europa.Eu, 2018).

Personenbezogene Daten

Als personenbezogene Daten, werden laut Definition alle Informationen verstanden, die sich auf eine identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person gesehen, wenn sie direkt oder indirekt mittels Zuordnung von einzelnen oder mehreren Merkmalen identifiziert werden kann. Zu diesen Merkmalen zählen Namen, Kennzeichen, Standortdaten oder sonstige Informationen zählen, die eine Person identifizierbar machen (Wirtschaftskammer Österreich, 2018b).

Anonyme Informationen

Anonyme Informationen sind solche, die sich nicht auf eine natürliche Person beziehen bzw. auf personenbezogene Daten, die anonymisiert wurden und somit keine Identifikation der betroffenen Person möglich machen (Wirtschaftskammer Österreich, 2018b).

Betroffene Person

Als betroffene Person wird diejenige natürliche Person bezeichnet, von der die personenbezogenen Daten stammen und die identifiziert werden kann (Wirtschaftskammer Österreich, 2018b).

Besondere Kategorien personenbezogener Daten

Alle Informationen über die ethnische Herkunft, politische Meinung, religiöse und weltanschauliche Überzeugung sowie die Gewerkschaftszugehörigkeit fallen neben genetischen und biometrischen Daten zur eindeutigen Identifikation einer natürlichen Person, Gesundheitsinformationen sowie Daten über die sexuelle Orientierung einer Person fallen in die Kategorie der besonderen personenbezogenen Daten (Wirtschaftskammer Österreich, 2018b).

Verantwortlicher

Als Verantwortlicher wird eine natürliche bzw. juristische Person, Behörde, Einrichtung oder eine andere Stelle bezeichnet, die über die Verarbeitungszwecke und Mittel von personenbezogenen Daten entscheidet (Wirtschaftskammer Österreich, 2018b).

Auftragsverarbeiter

Als Auftragsverarbeiter wird eine natürliche bzw. juristische Person, Behörde, Einrichtung oder eine andere Stelle bezeichnet, die vom Verantwortlichen beauftragt wurde um die personenbezogenen Daten zu verarbeiten (Wirtschaftskammer Österreich, 2018b).

Pseudonymisierung

Wurden personenbezogene Daten pseudonymisiert, so können diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden, sofern diese gesondert aufbewahrt und durch technische und organisatorische Maßnahmen geschützt sind. Durch Pseudonymisierung können Datenschutzmissbrauchsrisiken für die betroffene Person minimiert werden und den Verantwortlichen sowie die Auftragsverarbeiter bei deren Datenschutzpflichten unterstützen (Wirtschaftskammer Österreich, 2018b).

Gesundheitsdaten

Als Gesundheitsdaten werden Informationen über den körperlichen und geistigen Gesundheitszustand einer natürlichen Person bezeichnet. Informationen über erbrachte Gesundheitsdienstleistungen oder andere Daten, die über den Gesundheitszustand der Person Auskunft geben, fallen ebenfalls in diese Kategorie (Wirtschaftskammer Österreich, 2018b).

Genetische Daten

Als genetische Daten werden Informationen über geerbte oder erworbene genetische Eigenschaften einer natürlichen Person bezeichnet, welche Auskunft über die Physiologie oder Gesundheit geben. Auch Daten über biologische Proben einer natürlichen Person gehören in diese Kategorie (Wirtschaftskammer Österreich, 2018b)

Biometrische Daten

Durch spezielle technische Verfahren gewonnene personenbezogene Daten über physische, psychologische und verhaltenstypische Merkmale natürlicher Personen, die zur Identifikation herangezogen werden können, wie z.B. Gesichtsbilder, zählen zu der Kategorie der biometrischen Daten (Wirtschaftskammer Österreich, 2018b).

Profiling

Unter Profiling wird jede Art der automatisierten Verarbeitung von personenbezogenen Daten verstanden, durch die bestimmte persönliche Aspekte analysiert bzw. bewertet werden können. Aspekte wie Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Interessen, Verhalten, etc. werden hierbei analysiert und bewertet um Ereignisse oder Verhaltensweisen einer Person vorherzusagen (Wirtschaftskammer Österreich, 2018b).

Aufsichtsbehörde

Jeder Mitgliedsstaat der europäischen Union bestimmt mindestens eine Aufsichtsbehörde, die über die erforderlichen Qualifikationen zur Umsetzung der Verordnung verfügt. Befinden sich mehrere Aufsichtsbehörden in einem Mitgliedsstaat, so wird eine davon zur federführenden Aufsichtsbehörde ernannt (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 66–67).

Die Aufsichtsbehörde in Österreich ist die österreichische Datenschutzbehörde mit dem Hauptsitz in:

> Wickenburggasse 8
> 1080 Wien
> Tel: +43 1 52 152 0
> E-Mail: dsb@dsb.gv.at
>
> (Wirtschaftskammer Österreich, 2017)

Europäischer Datenschutzausschuss

Um eine einheitliche Anwendung der DSGVO innerhalb der europäischen Union zu gewährleisten wird der europäische Datenschutzausschuss (in dieser Masterarbeit „Ausschuss“ genannt) mit eigener Rechtspersönlichkeit eingerichtet. Der Ausschuss besteht aus dem Leiter einer

Aufsichtsbehörde jedes Mitgliedsstaates und dem europäischen Datenschutzbeauftragten oder ihren Vertretern. Existieren mehrere Aufsichtsbehörden innerhalb eines Mitgliedsstaates, so wird ein gemeinsamer Vertreter dieses Mitgliedsstaates ernannt. Darüber hinaus kann die Kommission, jedoch ohne Stimmrecht, an den Tätigkeiten und Sitzungen des Ausschusses teilnehmen. Der Ausschuss dient zur Sicherstellung der einheitlichen Anwendung der DSGVO. Zu dessen Aufgaben zählen unter anderem die Förderung der Zusammenarbeit zwischen den Aufsichtsbehörden, die Abgabe von Stellungsnahmen für die Kommission, die Leitlinienbereitstellung, die Empfehlung von speziellen Verfahren oder die Streitbeilegung (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 76–78).

2 ENTSTEHUNG DER DSGVO

Die Datenschutz-Grundverordnung (DSGVO) wurde am 27. April 2016 in Brüssel beschlossen. Im Amtsblatt der Europäischen Union wird die EU Verordnung 2016/679 wie folgt betitelt:

> *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016*
>
> *zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*
>
> *(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 1)*

Neben der Ablösung der Datenschutz Richtlinie 95/46/EG wurden auch Anpassungen, am weiterhin in Österreich geltenden Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999 idgF vorgenommen. Die wichtigsten datenschutzrelevanten Vorschriften werden in den folgenden Punkten behandelt.

2.1 EU-Datenschutz-Richtlinie 95/46/EG

Wie zuvor erwähnt, wurde am 27. April 2016 mit dem Beschluss der neuen Datenschutz-Grundverordnung, die Aufhebung der Richtlinie 95/46/EG beschlossen. Seit dem Inkrafttreten der DSGVO 2016/679 am 25. Mai 2018 ist diese Richtlinie somit ungültig. Die nun obsolete EU-Datenschutz-Richtlinie wurde wie folgt zusammengefasst.

> *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 [Amtsblatt L 281 vom 23.11.1995]*
>
> *Auf europäischer Ebene ist die Richtlinie 95/46/EG der Bezugstext im Zusammenhang mit dem Schutz personenbezogener Daten. Mit dieser Richtlinie wird ein Regelungsrahmen eingeführt, der darauf abzielt, ein Gleichgewicht zwischen einem hohen Schutz der Privatsphäre und dem freien Verkehr personenbezogener Daten innerhalb der Europäischen Union (EU) zu schaffen. Zu diesem Zweck sieht die Richtlinie strenge Beschränkungen für die Erhebung und Verwertung personenbezogener Daten vor und fordert, in den einzelnen Mitgliedstaaten eine unabhängige nationale Stelle einzurichten, deren Aufgabe die Überwachung jeglicher Tätigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten ist.*
>
> *(Europäisches Parlament und Rat der Europäischen Union, 2014, S. 1)*

2.2 Datenschutzgesetz DSG 2000

Die Datenschutz-Grundverordnung wird durch das in Österreich geltende Datenschutzgesetz ergänzt. Das bis zur Einführung der DSGVO geltende Datenschutzgesetz (DSG), BGBl. I NR. 165/1999, idgF wird in diesem Kapitel behandelt (Datenschutzbehörde Republik Österreich, o.D.a).

Seit der Ursprungsversion von 1999 wurde das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (kurz DSG) mehrfach angepasst bzw. erweitert. Die Anpassungen im BGBl. I Nr. 120/2017 werden später noch näher betrachtet. In der aktuellen Version des DSG), also in der Fassung vom 07.03.2019 ist das folgende Änderungsverzeichnis vermerkt:

- BGBl. I Nr. 136/2001 - 2. Euro-Umstellungsgesetz;
- BGBl. I Nr. 13/2005 - Änderung des Datenschutzgesetzes 2000 - DSG 2000;
- BGBl. I Nr. 2/2008 - Änderung des Bundes-Verfassungsgesetzes und Erlassung eines Ersten Bundesverfassungsrechtsbereinigungsgesetzes;
- BGBl. I Nr. 133/2009 - Bundesgesetz, mit dem das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010);
- BGBl. I Nr. 135/2009 - Eingetragene Partnerschaft-Gesetz - EPG und Änderung des Allgemeinen Bürgerlichen Gesetzbuches, des Ehegesetzes, des Fortpflanzungs-medizingesetzes, des IPR-Gesetzes, der Jurisdiktionsnorm, des Strafgesetzbuches, der Strafprozessordnung;
- BGBl. I Nr. 112/2011 - Budgetbegleitgesetz 2012;
- BGBl. I Nr. 51/2012 – Verwaltungsgerichtsbarkeits-Novelle 2012;
- BGBl. I Nr. 57/2013 - DSG-Novelle 2013;
- BGBl. I Nr. 83/2013 - DSG-Novelle 2014;
- BGBl. I Nr. 132/2015 - Aufhebung des § 28 Abs. zwei Datenschutzgesetz 2000 durch den Verfassungsgerichtshof;
- BGBl. I Nr. 120/2017 - Datenschutz-Anpassungsgesetz 2018;
- BGBl. I Nr. 23/2018 - Änderung des Datenschutzgesetzes – DSG;
- BGBl. I Nr. 24/2018 - Datenschutz-Deregulierungs-Gesetz 2018;
- BGBl. I Nr. 14/2019 - Änderung des Bundes-Verfassungsgesetzes, des Übergangs-gesetzes vom 1. Oktober 1920, in der Fassung des B. G. Bl. Nr. 368 vom Jahre 1925, des Bundesverfassungsgesetzes betreffend Grundsätze für die Einrichtung und Geschäftsführung der Ämter der Landesregierungen außer Wien, des Bundesforstegesetzes 1996, des Datenschutzgesetzes, des Bundesgesetzblattgesetzes, des Niederlassungs- und Aufenthaltsgesetzes und des Bundesgesetzes über die Europäische Ermittlungsanordnung in Verwaltungsstrafsachen.

(Bundesministerium für Digitalisierung und Wirtschaftsstandort, 2019)

Die einzelnen Anpassungen am Datenschutzgesetz im Laufe der Jahre verfügen über unterschiedlichen Umfang. In der Anpassung des Jahres 2001 wurde beispielsweise primär die Euroumstellung behandelt und somit die Währungsdaten getauscht. Hingegen wurden im Bundesgesetzblatt 120/2017 umfassende Änderungen des Datenschutzgesetzes wegen der kommenden DSGVO durchgeführt.

2.3 Datenschutz-Anpassungsgesetz 2018

Durch das Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017 wurde das Datenschutzgesetz 2000 stark verändert um den Vorgaben der DSGVO zu entsprechen. Neben umfangreichen Änderungen wurde auch der Titel von „Datenschutzgesetz 2000“ auf nur noch „Datenschutzgesetz“ gekürzt (Datenschutzbehörde Republik Österreich, o.D.a).

2.4 Änderungen am Datenschutzgesetz nach Inkrafttreten der DSGVO

Seit dem Datenschutz-Anpassungsgesetz 2018 wurden weitere Änderungen am DSG durchgeführt. Im Folgenden werden alle Änderungen bis März 2019 (Abschlusstermin dieser Masterarbeit) betrachtet.

2.4.1 Änderung des Datenschutzgesetzes

Im 23. Bundesgesetz BGBl. I Nr. 23/2018 wurden nur kleine Änderungen in Form von zwei Verfassungsbestimmungen am Datenschutzgesetz vorgenommen. Nach dem neuen Gesetzt übt die Datenschutzbehörde auch ihre Befugnisse bei der Vollziehung gegenüber den obersten Organen aus (Österreichisches Parlament, 2018a, S. 1).

2.4.2 Datenschutz-Deregulierungsgesetz 2018

Das Datenschutz-Deregulierungsgesetz 2018 wurde am 15. Mai 2018 veröffentlicht und nimmt einige Veränderungen am Datenschutzgesetz vor. Die folgenden Punkte gehören zu den wichtigsten Änderungen:

- Das Auskunftsrecht von Verantwortlichen kann jetzt verweigert werden, wenn der Verantwortliche dadurch Betriebsgeheimnisse offenlegen würde;
- Um das Redaktionsgeheimnis und das Recht auf freie Meinungsäußerung zu wahren gelten für Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Unternehmensintern eigene Datenschutzregeln als für Unternehmen mit anderen Tätigkeitsbereichen;
- Kommt es zu einem Verstoß, so wird von der Datenschutzbehörde zunächst eine Verwarnung ausgesprochen und nicht gleich eine Strafe verhängt;

- Gegen Behörden und öffentliche Stellen, die im gesetzlichen Auftrag handeln kann keine Geldstrafe verhängt werden;
- Es wurden einige schriftliche Anpassungen am DSG vorgenommen.

  (Österreichisches Parlament, 2018b, S. 1–4)

2.4.3 BGBl. I Nr. 14/2019

Im 14. Bundesgesetz des Jahres 2019 BGBl. I Nr. 14/2019 werden in vielen Bereichen Änderungen eingeführt. Der Titel des Bundesgesetzes lautet wie folgt:

> *Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Übergangsgesetz vom 1. Oktober 1920, in der Fassung des B. G. Bl. Nr. 368 vom Jahre 1925, das Bundesverfassungsgesetz betreffend Grundsätze für die Einrichtung und Geschäftsführung der Ämter der Landesregierungen außer Wien, das Bundesforstegesetz 1996, das Datenschutzgesetz, das Bundesgesetzblattgesetz, das Niederlassungs- und Aufenthaltsgesetz und das Bundesgesetz über die Europäische Ermittlungsanordnung in Verwaltungsstrafsachen geändert werden.*
>
> *(Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz, 2019, S. 1)*

In Artikel fünf werden die Änderungen des Datenschutzgesetzes behandelt. Die Paragraphen 60 und 61 treten mit sofortiger Wirksamkeit außer Kraft und die Paragraphen zwei und drei mit 1. Jänner 2020. Somit sind die Zuständigkeiten (§ 2) und der räumliche Anwendungsbereich (§ 3) mit 2020 Bundesmaterie (Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz, 2019, S. 5–6).

2.5 Datenschutzgesetz 1978

Das Bundesgesetz BGBl. Nr. 565/1978 befasst sich als erstes Gesetz mit dem Schutz personenbezogene Daten und war bis zu dem Inkrafttreten des DSG 2000 gültig. Auf den 14 Seiten des am 28. November 2018 veröffentlichen Dokuments werden viele Datenschutzthemen bereits behandelt (Österreichischer Nationalrat, 1978, S. 1–14).

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 1978 Ausgegeben am 28. November 1978 193. Stück

565. Bundesgesetz: Datenschutzgesetz – DSG
(NR: GP XIV RV 72 AB 1024 S. 104. BR: 1893 AB 1895 S. 380.)

Abbildung 2: Überschrift BGBl. Nr. 565/1978 (Österreichischer Nationalrat, 1978)

Zunächst werden die Grundrechte bei der Verarbeitung und die Zuständigkeit zur Gesetzgebung behandelt. Hier werden bereits Themen wie Geheimhaltungsrecht der personenbezogenen

Daten, Auskunftsrecht über verarbeitete Daten und die Beschränkung von Rechten bei automatisierter Verarbeitung angeführt. Bestimmungen für den öffentlichen Bereich, den privaten Bereich sowie der internationale Datenverkehr werden voneinander getrennt und mit unterschiedlichen Vorschriften behandelt. Das Auskunftsrecht, die Richtigstellungspflicht und die Löschungspflicht sind bereits ein Teil der Verordnung und wurden mit Fristen belegt. Strafbestimmungen des Geheimnisbruchs sind ebenfalls ein Teil der Verordnung. Es wurden Beträge von 150.000 Schilling und Freiheitsstrafen angeführt. Mit erstem Jänner 1980 ist die Verordnung in Kraft getreten (Österreichischer Nationalrat, 1978, S. 1–13).

3 INHALT DER DSGVO

Das primäre Ziel der DSGVO ist der Schutz der personenbezogenen Daten natürlicher Personen und die Vereinheitlichung des Datenschutzrechts aller europäischen Mitgliedsstaaten. Es wurden in der Verordnung 2016/679 insgesamt 173 Gründe dafür angeführt. Die Verordnung umfasst elf Kapitel mit insgesamt 99 Artikeln. Die wichtigsten Gründe und Artikel werden im folgenden Teil dieser Masterarbeit beschrieben. Der Fokus wird dabei auf alle sicherheitsrelevanten Themen, sowie den Umgang mit personenbezogenen Daten und die technischen und organisatorischen Maßnahmen gelegt.

Die DSGVO besteht aus elf Kapiteln mit insgesamt 99 Artikeln. Im folgenden Teil dieser Masterarbeit werden die einzelnen Kapitel zusammengefasst um die relevanten Aspekte der Verordnung darzustellen.

3.1 Kapitel 1: Allgemeine Bestimmungen

Im ersten Kapitel der DSGVO werden die allgemeinen Ziele, Anwendungsbereiche und Begriffsbestimmungen erläutert. Es wird bereits in Artikel eins erklärt, dass sich die Verordnung dem Schutz der personenbezogenen Daten und den Grundrechten bzw. Grundfreiheiten natürlicher Personen widmet.

Der Anwendungsbereich wird in sachliche und räumliche Themen unterteilt. Zu den sachlichen Anwendungsbereichen zählen automatisierte und nicht-automatisierte Verarbeitungstätigkeiten der personenbezogenen Daten. Außerdem werden Ausnahmen, unter denen die Datenverarbeitung erlaubt ist, angeführt. Die räumlichen Themen beschreiben, in welchem territorialen Gebiet die Verordnung Anwendung findet in Bezug auf die Niederlassung der Verantwortlichen bzw. Auftragsgeber und deren Tätigkeiten (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 32–33).

> *Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.*
>
> *(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 32)*

Des Weiteren werden in Kapitel eins insgesamt 26 Fachbegriffe erläutert, die in der Verordnung Anwendung finden. Ein Teil dieser Fachausdrücke wurde in dieser Masterarbeit bereits in Kapitel 1.5 beschrieben.

3.2 Kapitel 2: Grundsätze

Kapitel zwei der DSGVO befasst sich mit den Grundsätzen der personenbezogenen Datenverarbeitung. Im ersten Artikel des Kapitels (Artikel 5) ist definiert wie mit personenbezogenen Daten umgegangen werden muss (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 35–36).

(1) personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 35–36)

Artikel sechs der DSGVO erläutert die Rechtmäßigkeit der Datenverarbeitung. Zunächst werden die Bedingungen für eine rechtmäßige Verarbeitung in der Verordnung 2016/679 wie folgt erläutert.

> *(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:*
>
> *a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;*
>
> *b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;*
>
> *c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;*
>
> *d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;*
>
> *e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;*
>
> *f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.*
>
> *(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 36)*

Des Weiteren wird in Artikel sechs den Mitgliedstaaten zugestanden, die unter den Buchstaben c und e ausgeführten Bedingungen präziser zu gestalten. Zudem sind in Artikel sechs die dafür geltenden Rechtsgrundlagen beschrieben (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 36).

Artikel sieben der DSGVO befasst sich mit den Bedingungen bezüglich der Einwilligung zur Verarbeitung persönlicher Daten. Hierbei wird die Freiwilligkeit der Zustimmung, Nachweispflicht der Einwilligung durch den Verantwortlichen (Datenverarbeiter) sowie das jederzeit gültige Widerrufsrecht der betroffenen Personen, näher ausgeführt. Außerdem wird eine leicht verständliche und zugängliche Form der Einwilligungserklärung gefordert (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 37).

Die Einwilligungsbedingungen für Kinder und deren Bezug von Diensten der Informationsgesellschaft wird in Artikel acht der DSGVO näher ausgeführt. Hier wird den Mitgliedsstaaten ebenfalls ein Mitgestaltungsrecht hinsichtlich der Auferlegung einer Altersgrenze eingeräumt, wobei die Altersgrenze jedoch die Vollendung des dreizehnten Lebensjahres nicht unterschreiten darf (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 37–38).

Im neunten Artikel der DSGVO wird die Verarbeitung von besonderen Kategorien der personenbezogenen Daten beschrieben. Diese persönlichen Daten werden im Artikel wie folgt definiert.

> *(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder das Gewerkschafszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.*
>
> *(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 38)*

Des Weiteren wird in Artikel neun erklärt unter welchen Bedingungen die Verarbeitung der zuvor beschriebenen besonderen personenbezogenen Daten erlaubt ist. Unter den folgenden Punkten ist eine Verarbeitung zulässig.

- Wenn die betroffene Person der Verarbeitung der besonderen personenbezogenen Daten für einen oder mehrere Zwecke ausdrücklich zugestimmt hat;
- Wenn die Verarbeitung erforderlich ist um das Recht auf Arbeit, das Recht auf soziale Sicherheit und des Sozialschutzes wahrnehmen zu können und seinen Pflichten nachzukommen;
- Wenn es um den Schutz von lebenswichtigen Interessen der betroffenen oder einer anderen natürlichen Person geht und die betroffene Person aus körperlichen oder rechtlichen Gründen nicht im Stande sein sollte der Verarbeitung zuzustimmen;
- Wenn die Garantie einer politischen, weltanschaulichen, religiösen oder gewerkschaftlichen Stiftung, Vereinigung oder Organisation ohne Gewinnerziehungsabsicht sowie deren ausschließliche bzw. ehemalige Mitglieder oder Personen die im Zusammenhang mit der Organisation regelmäßigen Kontakt unterhalten, betroffen sind;
- Wenn die personenbezogenen Daten bereits durch die betroffene Person öffentlich zugänglich gemacht wurden;
- Wenn die Handlungsfähigkeit der Gerichte bei der Ausübung oder Verteidigung von Rechtsansprüchen zu unterstützen ist;
- Aus Gründen eines erheblichen öffentlichen Interesses unter Berücksichtigung der Wahrung der Grundrechte und Interessen der betroffenen Person;
- Für Zwecke der Gesundheitsvorsorge, Arbeitsmedizin, Beurteilung der Arbeitsfähigkeit eines Beschäftigten wie auch für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- bzw. Sozialbereich oder für Systeme sowie Dienste im Gesundheits- und Sozialbereich;

- Aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsmaßnahmen oder zur Gewährleistung der Gesundheitsvorsorge sowie bei Arzneimitteln bzw. Medizinprodukten;
- Für im öffentlichen Interesse liegende Archivzwecke und wissenschaftliche oder historische Forschungszwecke unter Berücksichtigung der Wahrung der Grundrechte und Interessen der betroffenen Person.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 39)

Den Mitgliedsstaaten wird zugestanden zusätzliche Bedingungen oder Einschränkungen bei der Verarbeitung biometrischer und genetischer Daten sowie Gesundheitsdaten einzuführen bzw. aufrechtzuerhalten (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 39).

Artikel zehn der DSGVO befasst sich mit der Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten. Ein umfassendes Register der strafrechtlichen Verurteilungen und die Verarbeitung dieser Daten, darf nur unter behördlicher Aufsicht geführt werden (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 39).

Ist die Identifikation der personenbezogenen Daten zur Verarbeitung dieser Daten nicht notwendig, so ist der Verantwortliche nicht dazu verpflichtet diese Informationen aufzubewahren oder einzuholen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 39).

3.3 Kapitel 3: Rechte der betroffenen Personen

In Kapitel drei der DSGVO sind die Rechte der betroffenen Person sowie die notwendigen Tätigkeiten des Verantwortlichen zur Gewährleistung dieser Rechte beschrieben. Der erste Abschnitt bezieht sich auf die Transparenz und die Modalitäten der Datenverarbeitung sowie die Rechte der betroffenen Person.

Die Informationen zur Verarbeitung der personenbezogenen Daten der Betroffenen sind vom Verantwortlichen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln. Dies gilt besonders für Informationen, die sich an Kinder richten. Die Übermittlung der Daten muss schriftlich bzw. in elektronischer Form erfolgen. Wenn die betroffene Person es verlangen, kann die Information auch mündlich erfolgen, sofern die Identität der betroffenen Person nachgewiesen wurde. Der Verantwortliche darf eine Informationsausgabe verweigern falls er glaubhaft machen kann, nicht in der Lage zu sein, die betroffene Person zu identifizieren (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 39–40).

Die Anfrage über die Auskunft der Verarbeitung von personenbezogenen Daten der betroffenen Person muss vom Verantwortlichen innerhalb eines Monats beantwortet werden. Aufgrund von hohen Anfragemengen bzw. einem hohen Komplexitätsgrad der Anfragen, kann die Frist um weitere zwei Monate verlängert werden. In diesem Fall ist die betroffene Person innerhalb des ersten Monats über die Fristverlängerung zu informieren. Wird der Verantwortliche nach Antragsstellung der betroffenen Person nicht tätig, so muss er die Person ohne Verzögerung, spätestens innerhalb eines Monats nach Antragsstellung über die Gründe informieren und über

die Möglichkeiten einer Beschwerde Auskunft erteilen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 40).

Alle Informationen zur personenbezogenen Datenverarbeitung werden unentgeltlich zur Verfügung gestellt, es sei denn die betroffene Person stellt Anträge in hoher Frequenz. Bei exzessiver Antragsstellung kann der Verantwortliche ein angemessenes Entgelt für die Bereitstellung der Informationen (Verwaltungskosten) einfordern oder sich weigern die Informationen bereitzustellen. Wenn Zweifel hinsichtlich der Identität der betroffenen Person bestehen, kann der Verantwortliche zusätzliche Informationen über die Person anfordern um diese eindeutig zu identifizieren (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 40).

3.3.1 Informationspflicht zur Datenerhebung

Im zweiten Abschnitt des dritten Kapitels der DSGVO wird die Informationspflicht über die Erhebung der Daten beschrieben. Der Verantwortliche muss der betroffenen Person folgende Informationen zum Zeitpunkt der Datenerhebung mitteilen:

- Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des Vertreters bzw. Kontaktdaten des Datenschutzbeauftragten;
- Die Zwecke der Verarbeitung der personenbezogenen Daten und deren Rechtsgrundlage;
- Ob die Verarbeitung aus Interesse des Verantwortlichen oder eines Dritten durchgeführt wird;
- Die Empfänger der personenbezogenen Daten bzw. die Kategorie der Empfänger;
- Ob die Übermittlungsabsicht der personenbezogenen Daten gegenüber einem Drittland oder einer internationalen Organisation besteht.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 40–41)

Um eine transparente Verarbeitung zu ermöglichen, müssen zum Zeitpunkt der Erhebung des Weiteren folgende Informationen vom Verantwortlichen an die betroffene Person übermittelt werden:

- Wie lange die personenbezogenen Daten aufbewahrt werden und falls möglich die Kriterien für die Festlegung der Aufbewahrungsdauer;
- Die Informationen zum Widerspruchsrecht bezüglich der Verarbeitung sowie das Auskunftsrecht über die Berichtigung, Löschung oder Einschränkung der Verarbeitung;
- Informationen über das Beschwerderecht bei einer Aufsichtsbehörde;
- Inwieweit die Daten zur Erfüllung eines Vertragsabschlusses erforderlich sind und ob die Person dazu verpflichtet ist diese Daten bereitzustellen bzw. welche Folgen eine Nichterfüllung nach sich zieht;

- Werden die personenbezogenen Daten für einen anderen Zweck verarbeitet, als den für den die Daten erhoben wurden, so muss der Verantwortliche die betroffene Person darüber informieren.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 40–41)

Wenn die Daten nicht von der betroffenen Person direkt erhoben werden, sondern aus anderen Quellen stammen, muss der Verantwortliche die betroffene Person über die Verarbeitung informieren. Hierfür muss zusätzlich die Quelle der personenbezogenen Daten angeführt werden. Die Informationspflicht entfällt, wenn die betroffene Person bereits informiert wurde, die Informationserteilung sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert. Dies gilt besonders für die Verarbeitung von Daten im öffentlichen Interesse liegender Archivzwecke bzw. für wissenschaftliche oder historische Forschungszwecke/Statistikzwecke (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 40–41).

3.3.2 Berichtigung und Löschung personenbezogener Daten

Abschnitt drei des dritten Kapitells befasst sich mit der Berichtigung und Löschung personenbezogener Daten. Zunächst wird das Recht auf Berichtigung beschrieben. Die betroffene Person hat das Recht auf die unverzügliche Richtigstellung der sie betreffenden personenbezogenen Daten durch den Verantwortlichen. Unter Berücksichtigung der Verarbeitungszwecke kann die betroffene Person die Vervollständigung der personenbezogenen Daten auch mittels einer ergänzenden Erklärung verlangen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 43).

Aus den folgenden Gründen kann die betroffene Person vom Verantwortlichen verlangen die personenbezogenen Daten zu löschen.

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 43–44)

Wurden die personenbezogenen Daten öffentlich gemacht, d.h. wurde anderen Teilnehmern der Zugriff auf die personenbezogenen Daten gewährt, muss der Verantwortliche unter Zuhilfenahme angemessener technischer Mittel, die für die Datenverarbeitung Verantwortlichen darüber informieren. Sämtliche Links, Kopien oder Replikationen der personenbezogenen Daten müssen gelöscht werden (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 44).

Unter gewissen Umständen können die zuvor erwähnten Ansprüche nicht gültig gemacht werden. Darunter fallen z.B. die Ausübung des Rechts auf Meinungsäußerung, die Geltendmachung bzw. Ausübung von Rechtsansprüchen oder Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 44).

Das Recht auf Verarbeitungseinschränkung wird in Artikel 18 der DSGVO behandelt. Unter gewissen Voraussetzungen kann eine Verarbeitung eingeschränkt anstatt zurückgezogen bzw. als ungültig erklärt zu werden.

Der Verantwortliche ist verpflichtet alle Berichtigungen, Löschungen oder Einschränkungen der Verarbeitung von personenbezogenen Daten den Empfängern mitzuteilen. Erweist sich dies als unmöglich oder ist nur mit außerordentlichem Aufwand möglich, so kann der Verantwortliche davon absehen. Der Verantwortliche muss der betroffenen Person von den Empfängern berichten, sollte die betroffene Person dies verlangen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 44).

Die betroffene Person hat das Recht, die von ihr zur Verfügung gestellten personenbezogenen Daten vom Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Diese Daten dürfen an eine andere verantwortliche Person, ohne den ehemals Verantwortlichen zu benachrichtigen, übergeben werden (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 44–45).

Die in der DSGVO angeführten Beschränkungen können in Form von Gesetzgebungsmaßnahmen die Rechtsschriften der Mitgliedsstaaten, sofern diese im Wesensgehalt die Grundrechte und Grundfreiheiten einer demokratischen Gesellschaft sicherstellen, einschränken. Jede Gesetzgebungsmaßnahme muss spezifische Vorschriften enthalten zumindest in Bezug auf:

a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,

b) die Kategorien personenbezogener Daten,

c) den Umfang der vorgenommenen Beschränkungen,

d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung;

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,

f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 46–47)

3.4 Kapitel 4: Verantwortlicher und Auftragsverarbeiter

Im ersten Abschnitt des vierten Kapitels der DSGVO werden die allgemeinen Pflichten des Verantwortlichen bzw. des Auftragsverarbeiters behandelt. Es werden hier erstmals die sogenannten technischen und organisatorischen Maßnahmen (TOMs) erwähnt. Der Verantwortliche führt unter Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte der Person geeignete TOMs durch. Die TOMs müssen im erforderlichen Fall überprüft und aktualisiert werden. Um die Erfüllung der Pflichten des Verantwortlichen nachweisen zu können, müssen Verhaltensregeln bzw. geeignete Zertifizierungsverfahren herangezogen werden.

Die notwendigen TOMs sind vom Verantwortlichen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und dem Zweck bzw. den Umständen der Datenverarbeitung, zu wählen. Maßnahmen wie z.B.: die Pseudonymisierung können dabei helfen Datenschutzgrundsätze wie die Datenminimierung wirksam umzusetzen. Der Verantwortliche muss die notwendigen Garantien übernehmen um den Anforderungen der DSGVO zu genügen und um die Rechte der betroffenen Person zu schützen. Die verwendeten Maßnahmen müssen sicherstellen, dass nur Daten, die für den Verarbeitungszweck notwendig sind, herangezogen werden. Dies inkludiert

- die Menge der erhobenen personenbezogenen Daten,
- den Umfang der Verarbeitungstätigkeiten,
- die Speicherfrist der Daten,
- die Zugänglichkeit der Daten.

(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 47-48)

Diese Maßnahmen müssen darüber hinaus sicherstellen, dass die personenbezogenen Daten bereits durch Voreinstellung (ohne Eingreifen) nicht von jeder natürlichen Person, ohne Verarbeitungsnutzen, eingesehen werden können. Erstellen bzw. erarbeiten mehrere Verantwortliche gemeinsam die Mittel und Zwecke der Verarbeitung, so legen sie die Vereinbarung in transparenter Form fest und geben bekannt wer von ihnen welche Verpflichtungen zu übernehmen hat (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 48).

Befindet sich der Verantwortliche außerhalb der Europäischen Union bzw. hat keine Niederlassung in einem der Mitgliedsstaaten, so kann dieser einen Vertreter innerhalb der Europäischen Union schriftlich ernennen. Der Verantwortliche beauftragt den Vertreter dazu, als Anlaufstelle für Fragen, im Zusammenhang mit der Verarbeitung der personenbezogenen Daten

und der Einhaltung der Verordnung, der betroffenen Person zur Verfügung zu stehen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 48-49).

Der Verantwortliche kann einen Auftragsverarbeiter beauftragen die personenbezogene Datenverarbeitung durchzuführen. Der Auftragsverarbeiter hat hierbei die TOMs durchzuführen, sodass diese im Einklang mit der Verordnung erfolgen und den Schutz der Rechte der betroffenen Person gewährleisten. Der Auftragsverarbeiter darf keinen weiteren Verarbeiter ohne schriftliche Abklärung bzw. Beauftragung durch den Verantwortlichen hinzuziehen. Dieser Verarbeitung muss ein Vertrag zugrunde liegen, welcher die relevanten Eckpunkte, wie Verarbeitungsdauer, -art und -zweck der personenbezogenen Daten, aufführt. Zertifizierungen oder Verhaltensregeln können als Garantie vom Auftragsverarbeiter als Sicherheit herangezogen werden (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 49-50).

Die Verantwortlichen und gegebenenfalls deren Vertreter müssen ein Verzeichnis über sämtliche Verarbeitungstätigkeiten in ihrem Zuständigkeitsbereich führen. Die folgenden Punkte müssen in diesem Verzeichnis enthalten sein:

- Namen und Kontaktdaten des Verantwortlichen, des Vertreters und gegebenenfalls die eines etwaigen Datenschutzbeauftragten;
- Der Verarbeitungszweck;
- Die Kategorie der personenbezogenen Daten;
- Alle Empfänger der personenbezogenen Daten zu Verarbeitungszwecken, einschließlich Empfänger aus Drittländern bzw. Ländern außerhalb der Europäischen Union;
- Gegebenenfalls die Informationen von Organisationen bzw. Verarbeitern in Drittländern inkl. Datenübermittlung und Dokumentation der Garantien;
- Die Löschungsfristen der Datenkategorien - falls dies möglich ist;
- Falls möglich eine Beschreibung der angewendeten bzw. anzuwendenden TOMs.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 50-51)

Die vom Verantwortlichen beauftragten Auftragsverarbeiter und gegebenenfalls deren Vertreter führen ebenfalls ein Verzeichnis, mit den von ihnen durchgeführten Tätigkeiten der Verarbeitungen. Dieses Verzeichnis enthält:

- Namen und Kontaktdaten des Auftragsverarbeiters sowie jenes Verantwortlichen, der den Auftrag zur Datenverarbeitung gegeben hat, gegebenenfalls die Vertreter des Auftragsverarbeiters sowie des Verantwortlichen und etwaige Datenschutzbeauftragte;
- Die Verarbeitungskategorie, welche vom Verantwortlichen beauftragt wurde;
- Gegebenenfalls die Informationen von Organisationen/Verarbeitern in Drittländern inkl. Datenübermittlung und Dokumentation der Garantien;
- Falls möglich eine Beschreibung der angewendeten bzw. anzuwendenden TOMs.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 51)

Alle diese Punkte sind schriftlich bzw. in einem elektronischen Format zu dokumentieren (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 51).

3.4.1 Sicherheit der personenbezogenen Daten

In Abschnitt zwei des vierten Kapitels der DSGVO wird die Sicherheit der personenbezogenen Daten behandelt. Der Verantwortliche bzw. der Auftragsverarbeiter muss unter Berücksichtigung mehrerer Merkmale wie Eintrittswahrscheinlichkeit, Stand der Technik oder dem Zweck der Verarbeitung, geeignete TOMs setzen um ein angemessenes Schutzniveau zu gewährleisten. Zu diesen TOMs werden unter anderem die folgenden Punkte gezählt:

- Verschlüsselung und Pseudonymisierung der Daten - Daten können nicht mehr bzw. nicht ohne erheblichen Aufwand einer natürlichen Person zugeordnet werden;
- Vertraulichkeit - personenbezogene Daten, Systeme und Dienste können im Zusammenhang mit deren Verarbeitung nur von den befugten Personen bzw. Verarbeitern eingesehen werden;
- Integrität - Die verarbeiteten Daten, Systeme und Dienste sind vor unautorisierter Veränderung geschützt;
- Verfügbarkeit - Es muss sichergestellt sein, dass Daten, Systeme und Dienste zum benötigten Zeitpunkt für die Datenverarbeitung oder andere Tätigkeiten wie beispielsweise die Auskunftspflicht, verfügbar sind;
- Belastbarkeit - Die verwendeten Systeme und Dienste müssen unter Berücksichtigung des Standes der Technik ausreichend belastbar sein. D.h. die Systeme müssen widerstandsfähig im Fall eines Fehlers, einer Störung oder bei hoher Last sein;
- Daten, Systeme, Dienste und deren Zugang müssen bei einem physischen oder technischen Zwischenfall rasch wiederherstellbar sein;
- Die Einführung eines Verfahrens zur regelmäßigen Prüfung, Bewertung und Evaluierung der TOM-Wirksamkeit.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 51-52)

Zur Beurteilung eines angemessenen Schutzniveaus und der jeweiligen TOMs müssen insbesondere die Risiken bzw. Auswirkungen, die mit einer Verarbeitung einhergehen, beachtet werden. Dazu gehören: unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder Offenlegung der personenbezogenen Daten. Um die Erfüllung der Anforderungen durch die verwendeten TOMs nachweisen zu können, werden Zertifizierungsverfahren herangezogen. Des Weiteren müssen der Verantwortliche und der Auftragsverarbeiter die notwendigen Schritte zur Sicherstellung vornehmen, sodass ihnen unterstellte Personen, die Zugang zu den personenbezogenen Daten haben, diese nur auf Anweisung bearbeiten (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 52).

Im Fall einer Datenschutzverletzung der personenbezogenen Daten muss der Verantwortliche eine Meldung innerhalb von 72 Stunden nach dem Zeitpunkt der Verletzung der zuständigen

Aufsichtsbehörde übermitteln. Erfolgt die Meldung nicht binnen 72 Stunden, muss eine Begründung für die Verzögerung angefügt werden. Hat die Verletzung keine Auswirkung auf die Rechte und Freiheiten der betroffenen Person, so muss keine Meldung erbracht werden. Wird dem Auftragsverarbeiter eine Verletzung des Datenschutzes bekannt, so meldet er diese dem Verantwortlichen unverzüglich (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 52).

Eine Datenschutzverletzungsmeldung enthält zumindest die folgenden Informationen:

- Eine Beschreibung über die Art der Verletzung, soweit möglich mit Angabe über die Anzahl der betroffenen Personen, der betroffenen Kategorien und die Zahl der betroffenen Datensätze;
- Namen und Kontaktinformationen des Datenschutzbeauftragten bzw. der Anlaufstelle für zusätzliche Informationen;
- Eine Beschreibung der Auswirkungen bzw. wahrscheinlichen Folgen der Datenschutzverletzung für die betroffenen Personen;
- Eine Beschreibung der vom Verantwortlichen durchgeführten oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung der durch die Datenschutzverletzung entstandenen Auswirkungen.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 52)

Sollten dem Verantwortlichen nicht sämtliche Informationen zur Verfügung stehen, so müssen diese ohne weitere Verzögerung schrittweise zur Verfügung gestellt werden, sobald sie verfügbar sind. Der Verantwortliche muss alle Fakten der Verletzungen des Datenschutzes, sowie die ergriffenen Abhilfemaßnahmen dokumentieren. Diese Dokumentation muss der zuständigen Aufsichtsbehörde zur Verfügung gestellt werden, damit diese eine Überprüfung der Einhaltung durchführen kann (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 52).

Neben der Aufsichtsbehörde muss die jeweilige betroffene natürliche Person von der Datenschutzverletzung informiert werden. Birgt die Verletzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person, so muss der Verantwortliche die Person unverzüglich von der Verletzung informieren. Hat der Verantwortliche dafür gesorgt, dass geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und auf die personenbezogenen Daten angewandt wurden (z.B. Verschlüsselung/Pseudonymisierung) oder hat der Verantwortliche nachfolgende Maßnahmen ergriffen um die Risiken zu minimieren bzw. die Rechte sowie Freiheiten zu schützen und besteht diesbezüglich keine Gefahr mehr, so kann von einer Informierungspflicht abgesehen werden. Falls eine Informierung der betroffenen Personen mit einem unverhältnismäßigen Aufwand verbunden ist, kann eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme, durch die die betroffenen Personen benachrichtigt werden, erfolgen. Die Aufsichtsbehörde kann vom Verantwortlichen verlangen eine Benachrichtigung der betroffenen Person nachzuholen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 52–53).

3.4.2 Datenschutz-Folgenabschätzung

In Abschnitt drei der DSGVO werden die Datenschutz-Folgenabschätzung und die vorherige Konsultation behandelt. Birgt die Verarbeitung, insbesondere bei der Verwendung neuer Technologien bzw. aufgrund der Art, des Umfangs, der Umstände oder des Zwecks der Verarbeitung ein hohes Risiko für die Datensicherheit der personenbezogenen Daten, so muss vom Verantwortlichen eine Abschätzung der potentiellen Auswirkungen eines Datenschutzvergehens durchgeführt werden. Für ähnliche Verarbeitungsvorgänge mit annähernd gleichem Risiko genügt eine einzelne Abschätzung. Um eine aussagekräftige Datenschutz-Folgenabschätzung durchführen zu können, ist das hinzuziehen des Datenschutzbeauftragten (sofern ein solcher ernannt wurde) erforderlich. Besonders bei der systematischen bzw. umfangreichen Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen, Überwachung öffentlicher Bereiche oder bei Datenverarbeitungsvorgängen zur Bewertung von Aspekten natürlicher Personen zur Entscheidungsfindung muss eine Folgenabschätzung durchgeführt werden (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 53–54).

Von der österreichischen Aufsichtsbehörde wurde eine Liste der Verarbeitungszwecke, für die eine Datenschutz-Folgenabschätzung notwendig ist, veröffentlicht. Jene „Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung“ (DSFA-AV) trat am 25. Mai 2018 in Kraft. In der Verordnung werden anhand eines „Whitelist“ Verfahrens, alle Bereiche aufgezählt, bei denen keine Datenschutz-Folgenabschätzung notwendig ist. Das Inhaltsverzeichnis der DSFA-AV umfasst die jeweiligen Kategorien:

- A01: Kundenverwaltung, Rechnungswesen, Logistik, Buchführung
- A02: Personalverwaltung
- A03: Mitgliederverwaltung
- A04: Kundenbetreuung und Marketing für eigene Zwecke
- A05: Sach- und Inventarverwaltung
- A06: Register, Evidenzen, Bücher
- A07: Zugriffsverwaltung für EDV-Systeme
- A08: Zutrittskontrollsysteme
- A09: Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)
- A10: Bild- und Akustikdatenverarbeitung in Echtzeit
- A11: Bild- und Akustikdatenverarbeitungen zu Dokumentationszwecken
- A12: Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdienste, Anbieter und Apotheken
- A13: Rechts- und Beratungsberufe

- A14: Archivierung, wissenschaftliche Forschung und Statistik
- A15: Unterstützungsbekundungen
- A16: Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts
- A17: Öffentliche Abgabenverwaltung
- A18: Förderverwaltung
- A19: Öffentlichkeitsarbeit und Informationstätigkeit durch öffentliche Funktionsträger und deren Geschäftsapparate
- A20: Aktenverwaltung (Büroautomation) und Verfahrensführung
- A21: Organisation von Veranstaltungen
- A22: Preise und Ehrungen

  (Bundesministerium für Digitalisierung und Wirtschaftsstandort, 2018, S. 1–2)

Stellt sich durch die Datenschutz-Folgenabschätzung heraus, dass die Verarbeitung ein hohes Risiko zur Folge hätte, so muss der Verantwortliche vor der Verarbeitung die zuständige Aufsichtsbehörde informieren, sofern der Verantwortliche keine Maßnahmen zur Minimierung des Risikos trifft. Ist die Aufsichtsbehörde der Auffassung, dass die geplante Verarbeitung nicht verordnungskonform ist, insbesondere wenn das durch eine Verarbeitung entstehende Risiko vom Verantwortlichen nicht ausreichend ermittelt oder reduziert wurde, so unterbreitet sie dem Verantwortlichen bzw. dem Auftragsverarbeiter eine entsprechende schriftliche Empfehlung. Der Verantwortliche stellt hierfür der zuständigen Aufsichtsbehörde alle notwendigen Informationen zur Verfügung (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 54–55).

3.4.3 Datenschutzbeauftragte, Zertifizierungen und Verhaltensregeln

Abschnitt vier des dritten Kapitels der DSGVO befasst sich mit den Datenschutzbeauftragten. Die Ernennung eines Datenschutzbeauftragten ist zwingend notwendig, wenn eine Behörde oder öffentliche Stelle (Gerichte ausgenommen) die Verarbeitung durchführt, eine systematische bzw. umfangreiche regelmäßige Überwachung der betroffenen Person notwendig ist oder wenn die personenbezogenen Daten strafrechtliche Verurteilungen und Straftaten beinhalten. Der Datenschutzbeauftragte wird aufgrund seiner Fähigkeiten, seines Fachwissens im Bereich des Datenschutzrechts und anhand der Datenschutzpraxis, die er vorweisen kann, benannt. Der Datenschutzbeauftragte kann seine Tätigkeiten durch einen Dienstleistungsvertrag erfüllen oder ein Angestellter des Verantwortlichen bzw. des Auftragsverarbeiters sein. Die Kontaktdaten des Datenschutzbeauftragten werden veröffentlicht und der zuständigen Aufsichtsbehörde mitgeteilt (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 55).

Die folgenden Aufgaben sind vom Datenschutzbeauftragten nach Artikel 39 der DSGVO zu erfüllen:

- Erfüllung der Beratungsfunktion gegenüber dem Verantwortlichen, dem Auftragsverarbeiter und den Beschäftigten, die eine Verarbeitung von personenbezogenen Daten durchführen;
- Die Überwachung der Einhaltung der DSGVO und anderen Datenschutzvorschriften der Europäischen Union bzw. der Mitgliedsstaaten;
- Die Überwachung der Strategien des Verantwortlichen und des Auftragsverarbeiters im Bezug auf die Sicherstellung des Schutzes der personenbezogenen Daten;
- Schulung, Sensibilisierung und die Zuweisung von Zuständigkeiten der an der Datenverarbeitung beteiligten Personen;
- Beratung zur Datenschutz-Folgenabschätzung auf Anfrage;
- Die Zusammenarbeit mit der jeweiligen Aufsichtsbehörde;
- Der Datenschutzverantwortliche dient als Anlaufstelle für die Auftragsbehörde bei allen Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte frühzeitig in alle Fragen zum Schutz der personenbezogenen Daten eingebunden und von ihnen bei seinen Tätigkeiten unterstützt wird. Die betroffenen Personen können vom Datenschutzbeauftragten Informationen zur Verarbeitung ihrer personenbezogenen Daten erfragen. Der Datenschutzbeauftragte ist zur Geheimhaltung bzw. Vertraulichkeit nach dem Recht der Europäischen Union verpflichtet. Von dem Verantwortlichen und dem Auftragsverarbeiter wird sichergestellt, dass die anderen Aufgaben und Pflichten nicht zu einem Interessenskonflikt für den Datenschutzbeauftragten führen können (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 55–56).

Des Weiteren werden im vierten Kapitel der DSGVO die Verhaltensregeln und die Zertifizierungen erläutert. Speziell für die Bedürfnisse der Klein- und Mittelunternehmen werden Verhaltensregeln, die eine ordnungsgemäße Anwendung der DSGVO erleichtern, gefordert. Verhaltensregeln können von Vereinigungen oder Verbänden für eine Sammlung von Verantwortlichen oder Auftragsverarbeitern erstellt werden, wenn diese in eine ähnliche Kategorie fallen. Im Artikel 40 der DSGVO wird folgendes Beispiel für eine präzise Angabe von möglichen Verhaltensregeln angeführt:

- Eine transparente und faire Verarbeitung;
- Die Interessen des Verantwortlichen wahren;
- Die Erhebung der personenbezogenen Daten;
- Die Pseudonymisierung der Daten;
- Die Informierung der betroffenen Person und der Öffentlichkeit;
- Die Ausübung der Rechte der betroffenen Personen;

- Der Schutz von Kindern und die Informierung über die Einwilligung der Erziehungsberechtigten;
- Die Maßnahmen und Verfahren zur Sicherheit der Datenverarbeitung;
- Die Meldung von Datenschutzverletzungen an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Person;
- Die Übermittlung der personenbezogenen Daten an internationale Unternehmen oder Länder außerhalb der Europäischen Union;
- Außergerichtliche Verfahren oder Streitbeilegungsverfahren zwischen Verantwortlichen und betroffenen Personen, im Zusammenhang mit der Verarbeitung von personenbezogenen Informationen.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 56–57)

Die Verhaltensregeln müssen Verfahren vorsehen, die es den Verantwortlichen und den Auftragsverarbeitern ermöglichen die Datenverarbeitungsvorgänge zu überwachen. Insbesondere muss es möglich sein die Einhaltung der DSGVO zu überprüfen. Werden Verhaltensregeln genehmigt, doch gelten diese nicht in allen Mitgliedsstaaten, so muss die zuständige Aufsichtsbehörde ein Verzeichnis über die Verhaltensregeln führen und dieses veröffentlichen. Ist ein Entwurf der Verhaltensregeln, deren Anpassung oder Änderung formuliert und ist er mit der DSGVO vereinbar, so wird dieser der Kommission vorgelegt. Die Kommission kann sodann über die Gültigkeit dieser Verhaltensregeln bestimmen und trägt Sorge dafür, dass die Verhaltensregeln in geeigneter Weise veröffentlicht werden. Die genehmigten Verhaltensregeln werden vom Ausschuss in ein Register aufgenommen und veröffentlicht (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 57–58).

Zur Überwachung der Einhaltung der Verhaltensregeln kann eine andere Stelle, die über das nötige Fachwissen in Bezug auf die Verhaltensregeln verfügt von der Aufsichtsbehörde bevollmächtigt werden. Die gewählte Stelle muss neben dem Fachwissen über die Punkte der Verhaltensregeln noch Verfahren festlegen, mit denen sie sicherstellt, dass Verantwortliche und Auftragsverarbeiter diese Regeln umsetzen bzw. einhalten, sodass Beschwerden hinsichtlich der Regelverletzungen nachgegangen werden kann. Des Weiteren muss nachgewiesen werden, dass die Aufgaben und Pflichten der Stelle nicht zu einem Interessenkonflikt führen können. Die zuständige Aufsichtsbehörde kann die Vollmacht der jeweiligen Stelle erteilen, und bei Nichterfüllung auch widerrufen. Dies betrifft jedoch nicht die Verarbeitung durch Behörden oder andere öffentliche Stellen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 58).

Um eine DSGVO Konformität der Verantwortlichen und Auftragsverarbeiter zu beweisen werden Zertifizierungen in der Verordnung erwähnt. Derartige datenschutzspezifische Zertifizierungen, Prüfzeichen oder Siegel können freiwillig durchgeführt werden. Für die Umsetzung eines Zertifizierungsverfahrens benötigt die jeweilige Zertifizierungsstelle oder die zuständige Aufsichtsbehörde den Zugriff auf alle notwendigen Informationen bzw. den Zugang zu allen relevanten Verarbeitungstätigkeiten. Wird eine Zertifizierung erfolgreich durchgeführt, so mindert sie nicht die Verantwortung des Verantwortlichen und des Auftragsverarbeiters die

DSGVO Richtlinien umzusetzen. Eine Zertifizierung ist nur für einen bestimmten Zeitraum gültig, und kann durch die zuständige Aufsichtsbehörde widerrufen werden, sollten die Anforderungen nicht oder nicht mehr erfüllt sein. Die maximale Gültigkeitsdauer einer Zertifizierung beträgt drei Jahre (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 58-59).

Eine Zertifizierungsstelle muss von der zuständigen Aufsichtsbehörde oder einer nationalen Akkreditierungsstelle berechtigt werden um Zertifizierungen durchführen zu können. Die Zertifizierungsstelle muss neben der Zufriedenheit der Aufsichtsbehörde und dem Beweis, dass die Aufgaben und Pflichten zu keinem Interessenkonflikt führen können, zudem sicherstellen, dass sie folgende Verfahren bzw. Methoden definiert hat:

- Verfahren zur Erteilung und Widerrufung von Zertifizierungen;
- Methoden zur Erfassung von Datenschutzverletzungen oder Beschwerden zu Datenschutzthemen;
- Verfahren zur Kontrolle der Zertifizierungsumsetzung des Verantwortlichen und des Auftragsverarbeiters;
- Methoden zur Kontrolle der Verarbeitungstransparenz gegenüber der Öffentlichkeit und der betroffenen Person.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 59-60).

Eine Zertifizierungsstelle kann die Zertifizierungserlaubnis für eine maximale Laufzeit von fünf Jahren erhalten und von der Aufsichtsbehörde unter begründetem Vorwand jederzeit widerrufen werden. Eine Verlängerung ist unter den gleichen Voraussetzungen wie für die ursprüngliche Akkreditierung, möglich. Die genauen Kriterien für die Erhaltung einer Zertifizierungserlaubnis werden von der zuständigen Aufsichtsbehörde in leicht zugänglicher Form veröffentlicht (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 60).

3.5 Kapitel 5: Übermittlungen personenbezogener Daten an Drittländer oder an Organisationen

Im fünften Kapitel der DSGVO wird die Weitergabe personenbezogener Daten an internationale Organisationen und an Drittländer behandelt. In Artikel 44, dem ersten Artikel dieses Kapitels wird angeführt, dass die in Kapitel fünf enthaltenen Vorschreibungen von dem Verantwortlichen und dem Auftragsverarbeiter eingehalten werden müssen damit die Datenverarbeitung zulässig ist. Dies gilt auch falls die personenbezogenen Daten von Drittländern oder internationalen Organisationen an weitere Drittländer bzw. internationale Organisationen weitergegeben werden. Darüber hinaus wird festgelegt, dass sämtliche Bestimmungen dieses Kapitels anzuwenden sind damit das durch die DSGVO definierte Schutzniveau nicht untergraben wird (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 60).

3.5.1 Angemessenheitsbeschluss der Kommission

In Artikel 45 wird die Datenübermittlung aufgrund eines Angemessenheitsbeschlusses erklärt. Entscheidet die Kommission, dass ein Drittland, ein Gebiet oder ein Sektor über ein ausreichendes Schutzniveau verfügt, so wird keine weitere Genehmigung benötigt (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 61).

Mit dem Stand vom 20.07.2018 sind bezogen auf alle Mitgliedsstaaten der EU und die EWR-Staaten (Europäischen Wirtschaftsraum) Liechtenstein, Norwegen und Island abgesehen von den allgemeinen Rechtspflichten keine weiteren Rechtsgrundlagen zu prüfen. Des Weiteren hat die Kommission eine Angemessenheitsentscheidung bezüglich der Staaten Andorra, Argentinien, Färöer-Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay und Japan (seit 23.01.2019) getroffen. Für diese Staaten gelten die gleichen Bestimmungen wie für EU-Mitgliedsstaaten und die EWR Staaten. Für die Vereinigten Staaten von Amerika wurde ein „Selbstzertifizierungsmechanismus“ für Unternehmen eingeführt. Die vom US-amerikanischen Handelsministerium verwaltete „Privacy-Shield“ Liste führt Unternehmen auf, die über ein ausreichendes Sicherheitsniveau verfügen und somit keine weiteren Voraussetzungen für eine Datenübermittlung erfüllen müssen. Die aktuelle „Privacy-Shield“ Liste kann im Internet unter der Webseite https://www.privacyshield.gov/welcome gefunden werden (Wirtschaftskammer Österreich, 2019e).

Die Kommission achtet insbesondere auf die folgenden Punkte bei der Angemessenheitsprüfung des gebotenen Schutzniveaus:

- Die Rechtsstaatlichkeit des betreffenden Landes bzw. der internationalen Organisation;
- Die Achtung der Menschenrechte und der Grundfreiheiten des betreffenden Landes bzw. der internationalen Organisation;
- Rechtsvorschriften in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht;
- Behördenzugang zu personenbezogenen Daten;
- Anwendung der Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften;
- Geltende Vorschriften über die Weiterübermittlung der personenbezogenen Daten an Drittländer bzw. internationale Organisationen;
- Durchsetzbare und wirksame Rechte der betroffenen Personen;
- Verwaltungsrechtliche und gerichtliche Rechtsbeihilfe für betroffene Personen;
- Eine oder mehrere Aufsichtsbehörden sind im Drittland vorhanden bzw. die internationale Organisation untersteht diesen Aufsichtsbehörden;
- Die Aufsichtsbehörden haben angemessene Durchsetzungsbefugnisse hinsichtlich der Beratung und Unterstützung der betroffenen Person zur Ausübung ihrer Rechte;

- Verpflichtungen, die Einfluss auf den Schutz der personenbezogenen Daten haben können und vom Drittland oder der internationalen Organisation eingegangen worden sind.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 61)

Sollte die Kommission aufgrund nach einer Beurteilung entscheiden, dass ein Drittland, ein Gebiet, Sektoren eines Drittlands oder eine internationale Organisation über ein geeignetes Schutzniveau verfügen, muss dieser Schutz fortlaufend gewährleistet sein. Dieser Durchführungsakt muss mindestens alle vier Jahre wiederholt werden. Alle Entwicklungen des Drittstaates bzw. der internationalen Organisation werden hierbei betrachtet. Die Kommission kann den Angemessenheitsbeschluss widerrufen, sollte sich das Schutzniveau verschlechtern oder andere Änderungen vorliegen, die Auswirkungen auf die Sicherheit der personenbezogenen Daten haben können. In diesem Fall nimmt die Kommission eine Beratungsfunktion ein um Abhilfe mit der Situation zu schaffen, die zu dem Beschluss geführt hat (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 61–62).

3.5.2 Garantien und verbindliche interne Datenschutzvorschriften

In Artikel 46 wird die Datenübermittlung an Drittländer oder internationale Organisationen unter der Voraussetzung das kein Beschluss gegen die Verarbeitung vorliegt, behandelt. Der Verantwortliche oder der Auftragsverarbeiter darf Daten nur übermitteln sofern geeignete Garantien vorgesehen sind und den betroffenen Personen durchsetzbare Rechte und Rechtsbehelfe zur Verfügung stehen. Die folgenden Punkte können als geeignete Garantien angesehen werden, sodass keine weitere Genehmigung einer Aufsichtsbehörde zur Datenverarbeitung notwendig ist:

- Ein rechtlich bindendes Dokument zwischen den öffentlichen Stellen oder Behörden;
- Verbindliche interne Datenschutzvorschriften (erläutert in Artikel 47);
- Von der Kommission erlassene Standarddatenschutzklauseln (erläutert in Artikel 93 Absatz 2);
- Standarddatenschutzklauseln von einer Aufsichtsbehörde, sofern diese von der Kommission in einem Prüfverfahren genehmigt wurden (erläutert in Artikel 93 Absatz 2);
- Genehmigte Verhaltensregeln zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in Bezug auf die Rechte der betroffenen Person;
- Ein genehmigter und anerkannter Zertifizierungsmechanismus zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in Bezug auf die Rechte der betroffenen Person.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 62)

Geeignete Garantien, sofern von der zuständigen Aufsichtsbehörde genehmigt, können auch aus Vertragsklauseln zwischen dem Verantwortlichen bzw. dem Auftragsverarbeiter und dem

Empfänger der personenbezogenen Daten einer internationalen Organisation bzw. einem Drittland bestehen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 62).

Eine von einem Mitgliedsstaat oder einer Aufsichtsbehörde erteilte Genehmigung bleibt so lange gültig bis diese von der Aufsichtsbehörde geändert, ersetzt oder aufgehoben wird (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 62).

Das Thema verbindliche interne Datenschutzvorschriften wird in Artikel 47 aufgegriffen. Verbindliche interne Datenschutzvorschriften können von der zuständigen Aufsichtsbehörde genehmigt werden. Diese müssen für alle Mitglieder einer Unternehmensgruppe bzw. einer Gruppe von Unternehmen, welche in einem gemeinsamen Wirtschaftsfeld tätig sind, rechtlich bindend sein und von diesen Mitgliedern und deren Beschäftigten umgesetzt werden. Die verbindlichen internen Datenschutzvorschriften müssen den betroffenen Personen durchsetzbare Rechte für die Verarbeitung der personenbezogenen Daten bieten und die folgenden Anforderungen erfüllen:

- Angaben zur Struktur und die Kontaktdaten der Unternehmensgruppe bzw. der Gruppe von Unternehmen und jedem ihrer Mitglieder;
- Informationen zur Datenübermittlung oder der Reihe von Datenübermittlungen;
- Welche Art der personenbezogenen Daten verarbeitet wird;
- Die Art und der Zweck der Verarbeitung dieser personenbezogenen Daten;
- Die Art der betroffenen Personen;
- Das betreffende Drittland bzw. die betreffenden Drittländer;
- Auflistung der internen und externen Rechtsverbindlichkeiten der jeweiligen internen Datenschutzvorschrift;
- Die Anwendung der grundlegenden Datenschutzgrundsätze, dazu gehören: Zweckbindung, Datenminimierung, Speicherfristbegrenzung, Datenqualität, Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen, Verarbeitung der besonderen Kategorien von personenbezogenen Daten, Rechtsgrundlage zur Verarbeitung alle Maßnahmen zur Sicherstellung der Datensicherheit für die Weiterübermittlung an nicht durch diese Datenschutzvorschriften gebundene Stellen;
- Die Rechte der betroffenen Person in Bezug zur Verarbeitung und die offenstehenden Mittel diese Rechte umzusetzen um einer automatischen Verarbeitung (wie etwa Profiling) nicht unterworfen zu werden;
- Die Möglichkeit für die betroffene Person rechtliche Schritte bei den zuständigen Gerichten der Mitgliedsstaaten im Falle einer Verletzung einzuleiten und gegebenenfalls eine Wiedergutmachung bzw. Schadenersatz zu erhalten;
- Die vom jeweiligen zuständigen Mitgliedsstaat definierte Haftung für den Verantwortlichen oder Auftragsverarbeiter im Falle eines etwaigen Verstoßes eines nicht in der Europäischen Union niedergelassenen Mitglieds der Unternehmensgruppe. Der Verantwortliche bzw. der Auftragsverarbeiter wird teilweise oder vollständig von dieser

Haftung befreit, falls dieser nachweisen kann, dass der Schadensauslöser nicht dem betreffenden Mitglied zur Last gelegt werden kann;

- Auf welche Art und Weise die betroffenen Personen über die Bestimmungen und Aspekte der verbindlichen internen Datenschutzvorschriften informiert werden;
- Die Aufgaben der benannten Datenschutzbeauftragten und jeder anderen Person bzw. Einrichtung die sich mit der Überwachung und Einhaltung der verbindlichen internen Datenschutzvorschriften sowie mit der Überwachung von Schulungsmaßnahmen befasst
- die Beschwerdeverfahren;
- Die Verfahren zur Überprüfung der verpflichtenden internen Datenschutzvorschriften. Diese Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Maßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse der Überprüfung werden dem Datenschutzbeauftragten mitgeteilt und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt;
- Verfahren zur Meldung und Erfassung von Vorschriftsänderungen und die Information an die Aufsichtsbehörde;
- Verfahren zur Zusammenarbeit mit der Aufsichtsbehörde und die Mitteilung über die Ergebnisse der Überprüfung von Maßnahmen zur Gewährleistung der verpflichtenden internen Datenschutzvorschriften;
- Das Mitteilungsverfahren zur Informierung der zuständigen Aufsichtsbehörde über Änderungen von rechtlich geltenden Bestimmungen in einem Drittland, die sich nachteilig auf die verbindlichen internen Datenvorschriften auswirken können;
- Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugriff auf personenbezogene Daten.

(Europäisches Parlament und Rat der Europäischen Union, 2016, S. 62–64)

Das Format und die Verfahren zum Informationsaustausch zwischen Verantwortlichen, Auftragsverarbeitern und der Aufsichtsbehörde kann durch die Kommission festgelegt werden (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 64).

Urteile durch ein Gericht eines Drittlandes und Entscheidungen einer Verwaltungsbehörde eines Drittlandes, die eine Offenlegung oder Übermittlung von personenbezogenen Daten durch seinen Verantwortlichen bzw. Auftragsverarbeiter verlangen, dürfen nur dann anerkannt oder vollstreckt werden, wenn sie sich auf eine geltende internationale Übereinkunft wie z.B. ein Rechtshilfeabkommen zwischen Drittland und der Europäischen Union oder einem ihrer Mitgliedsstaaten stützen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 64).

3.5.3 Rechtmäßige Verarbeitung ohne Angemessenheitsbeschluss und Garantien

In Kapitel fünf werden auch die Ausnahmen für besondere Fälle beschrieben. Besteht kein Angemessenheitsbeschluss oder keine geeigneten Garantien einschließlich verbindlicher interner Datenschutzvorschriften, so ist eine Übermittlung von personenbezogenen Daten an ein Drittland bzw. eine internationale Organisation nur unter den folgenden Punkten zulässig:

- Die betroffene Person hat die Datenübermittlung ausdrücklich bewilligt nachdem sie über die möglichen Risiken dieser Datenübermittlung ohne das Vorliegen eines Angemessenheitsbeschlusses und ohne Garantien informiert wurde;
- Die Datenübermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich;
- Die Datenübermittlung ist zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich;
- Die Datenübermittlung ist für den Verantwortlichen zum Abschluss bzw. der Erfüllung eines im Interesse der betroffenen Person und einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich;
- Die Datenübermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig;
- Die Datenübermittlung ist zur Ausübung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich;
- Die Datenübermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage ist eine Einwilligung zu erteilen;
- Die Datenübermittlung erfolgt aus einem Register, das von der Europäischen Union oder den Mitgliedsstaaten zur Information der Öffentlichkeit bestimmt ist. Es ist entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können zur Einsichtnahme zugängig. Dies gilt nur soweit die von der Europäischen Union oder den Mitgliedsstaaten festgelegten Voraussetzungen für die Einsichtnahme gegeben sind.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 64)

Sollte die Übermittlung ohne Angemessenheitsbeschluss, ohne Garantien oder ohne die zuvor genannten Punkte erfolgen, darf eine Übermittlung an ein Drittland nur stattfinden, wenn diese nicht wiederholt erfolgt, eine begrenzte Anzahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist oder die Interessen, Rechte und Freiheiten der betroffenen Person nicht überwiegen. Der Verantwortliche hat alle Umstände der Datenübermittlung zu beurteilen und muss auf der Bewertungsgrundlage geeignete Garantien in Bezug auf den Schutz der personenbezogenen Daten festlegen. Die Aufsichtsbehörde wird über die Übermittlung durch den Verantwortlichen in Kenntnis gesetzt und

informiert die betroffene Person über die zwingenden berechtigten Interessen für die Übermittlung (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 64).

Die Kommission und die Aufsichtsbehörden arbeiten zusammen und treffen geeignete Maßnahmen zum Schutz der personenbezogenen Daten in Bezug auf Drittländer und internationale Organisationen. Die folgenden Maßnahmen werden in Artikel 50 aufgeführt:

- Die Entwicklung von Mechanismen zur internationalen Zusammenarbeit um eine wirksame Durchsetzung von Rechtsvorschriften zum Schutz der personenbezogenen Daten zu erleichtern;
- Gegenseitige internationale Amtshilfe bei der Durchsetzung von Rechtsschriften zum Schutz der personenbezogenen Daten, wozu vor allem Meldungen, Beschwerdeverweise, Amtshilfe bei Untersuchungen und Informationsaustausch zählen;
- Die Einbindung maßgeblicher Interessenträger in Maßnahmen zur Verbesserung der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsschriften zum Schutz der personenbezogenen Daten;
- Die Verbesserung des Austausches und der Dokumentation von Praktiken und Rechtsschriften zum Schutz der personenbezogenen Daten einschließlich der Zuständigkeitskonflikte in Drittländern.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 65)

3.6 Kapitel 6: Unabhängige Aufsichtsbehörde

In Artikel sechs der DSGVO werden die unabhängigen Aufsichtsbehörden der Mitgliedsstaaten behandelt. Eine oder mehrere Aufsichtsbehörden werden von jedem Mitgliedsstaat mit der Überwachung der Anwendung der Datenschutz-Grundverordnung beauftragt. Die Wahrung der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung und die Erleichterung des freien Verkehrs von personenbezogenen Daten werden durch diese Behörden sichergestellt (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 65).

Sollte ein Mitgliedsstaat mehr als eine Aufsichtsbehörde beauftragen, so wird eine Aufsichtsbehörde vom Staat bestimmt um diese Behörden im Ausschuss zu vertreten. Jede Aufsichtsbehörde handelt völlig unabhängig bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse. Jeder Mitgliedsstaat muss die folgenden Punkte in Bezug auf die Aufsichtsbehörden sicherstellen:

- Die Aufsichtsbehörde hat genügend personelle, technische und finanzielle Ressourcen sowie Räumlichkeiten und Infrastrukturen um ihre Aufgaben und Befugnisse auszuüben;
- Die Aufsichtsbehörden wählen ihr eigenes Personal aus, und alle Mitglieder unterstehen lediglich der Leitung oder anderen Mitgliedern der Aufsichtsbehörde selbst;
- Die Aufsichtsbehörden werden einer Finanzkontrolle unterzogen, die keine Auswirkung auf die Unabhängigkeit der Behörde hat und sicherstellt, dass die Behörde über ihre

eigenen jährlichen Haushaltspläne verfügt, die ein Teil des Staatshaushaltes oder des nationalen Haushaltes sein können.

(Europäisches Parlament und Rat der Europäischen Union, 2016, 65–66)

Bei der Auswahl der Mitglieder der jeweiligen Aufsichtsbehörde ist darauf zu achten, dass die Interessen und Tätigkeiten der spezifischen Person nicht im Konflikt mit dem Amt stehen. Die Mitglieder der Aufsichtsbehörde müssen über die erforderliche Qualifikation, Erfahrung und Sachkunde im Bereich des Schutzes von personenbezogenen Daten verfügen um die Aufgaben bewältigen zu können. Das Amt eines Mitglieds endet mit dem Ablauf der Amtszeit, dem Pensionsantritt, Rücktritt oder wenn jenes Mitglied aufgrund einer schweren Verfehlung der Aufgaben dem Amt enthoben wird (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 66).

Bei Verantwortlichen mit mehreren Niederlassungen ist die Aufsichtsbehörde desjenigen Mitgliedsstaates zuständig, in dem sich die Hauptniederlassung des Verantwortlichen befindet. Verstoßt nur eine Niederlassung in einem Mitgliedsstaat gegen die Verordnung oder sollte der Verstoß nur Personen eines Mitgliedsstaats betreffen, so ist die jeweilige Aufsichtsbehörde des betroffenen Mitgliedsstaates hierfür heranzuziehen. In Abstimmung mit der federführenden Aufsichtsbehörde (die Behörde des Mitgliedsstaats, in dem sich die Hauptniederlassung des Verantwortlichen befindet) wird entschieden welche Aufsichtsbehörde sich mit dem Fall befasst (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 67-68).

Zu den Aufgaben der Aufsichtsbehörde gehören unter anderem die folgenden Tätigkeiten:

- Überwachung der Anwendung dieser Verordnung;
- Sensibilisierung bezüglich Risiken, Vorschriften, Garantien und Rechten;
- Anfragen der betroffenen Person in Bezug auf Informationen beantworten und ihre Rechte wahren;
- Sich mit Beschwerden befassen und diese in angemessenem Umfang untersuchen.
- Zusammenarbeit mit anderen Aufsichtsbehörden;
- Verfolgung von Entwicklungen, die sich auf den Schutz personenbezogener Daten beziehen können, insbesondere Entwicklungen in der Informations- und Kommunikationstechnologie;
- Einführung von Datenschutzzertifizierungsverfahren und Datenschutzsiegel/-prüfzeichen;
- Regelmäßige Überprüfung der Zertifizierungen;
- Vertragsklauseln zur Datenverarbeitung von internationalen Organisationen oder Drittländern definieren;
- Führen von Verzeichnissen über Verstöße gegen die Verordnung und ergriffene Maßnahmen;
- Erstellung eines Jahresberichts über ihre Tätigkeiten.

(Europäisches Parlament und Rat der Europäischen Union, 2016, 68–69)

Jede Aufsichtsbehörde verfügt über die nötigen Befugnisse um ihren Tätigkeiten nachzugehen. Darunter fallen Datenschutzüberprüfungen oder die Anweisung von Vertretern des Verantwortlichen bzw. des Auftragsverarbeiters Informationen zur Erfüllung der Verordnung bereitzustellen. Die Aufsichtsbehörde kann unter anderem Warnungen und Verwarnungen des Verantwortlichen bzw. des Auftragsverarbeiters aussprechen, Verarbeitungsbeschränkungen/-verbote verhängen, Zertifizierungen widerrufen, Geldbußen verhängen oder die Übermittlung von Daten an ein Drittland unterbinden (Europäisches Parlament und Rat der Europäischen Union, 2016, 69–70).

3.7 Kapitel 7: Zusammenarbeit und Kohärenz

Das siebente Kapitel der DSGVO trägt den Titel „Zusammenarbeit und Kohärenz“. Zunächst werden die Punkte Zusammenarbeit, gegenseitige Amtshilfe und die gemeinsamen Maßnahmen der Aufsichtsbehörden behandelt. Die federführende Aufsichtsbehörde arbeitet mit anderen Aufsichtsbehörden zusammen und strebt hinsichtlich der soeben genannten Punkte einen Konsens an. Hierbei werden auch zweckdienliche Informationen zwischen den Aufsichtsbehörden ausgetauscht. Die federführende Aufsichtsbehörde kann andere betroffene Aufsichtsbehörden darum ersuchen gemeinsame Tätigkeiten zur Durchführung von Untersuchungen oder Überwachungen durchzuführen und übermittelt etwaige nützliche Informationen. Betroffenen Aufsichtsbehörden steht die Möglichkeit offen Einspruch gegen Beschlüsse der federführenden Aufsichtsbehörde zu erheben.

Sollte ein Beschluss von der federführenden Aufsichtsbehörde erlassen werden, so teilt sie diesen der Hauptniederlassung des Verantwortlichen oder des Auftragsverarbeiters mit und setzt andere betroffene Aufsichtsbehörden und den Ausschuss über den Beschluss in Kenntnis. Hierbei wird neben dem Beschluss auch eine Zusammenfassung über Fakten und Gründe übermittelt. Sollte eine Beschwerde abgelehnt werden, so informiert die zuständige Aufsichtsbehörde den Beschwerdeführer und den Verantwortlichen. Wird eine Beschwerde nur teilweise abgelehnt oder abgewiesen, so muss für jeden Teil ein eigener Beschluss getroffen werden. Auch hier werden der Beschwerdeführer sowie der Verantwortliche bzw. der Auftragsverarbeiter darüber informiert (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 71).

Nachdem ein Beschluss getroffen wurde und der Verantwortliche bzw. Auftragsverarbeiter informiert wurde, ergreift der betroffene Verantwortliche bzw. Auftragsverarbeiter die nötigen Maßnahmen um die Verarbeitung der personenbezogenen Daten mit dem Beschluss in Einklang zu bringen. Die federführende Aufsichtsbehörde unterrichtet die anderen Aufsichtsbehörden davon sobald sie vom Verantwortlichen oder dem Auftragsverarbeiter über die ergriffenen Maßnahmen unterrichtet wurde. Informationen zwischen den Aufsichtsbehörden werden hierbei auf einem elektronischen Weg in einem standardisierten Format übermittelt (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 71–72).

Um die DSGVO einheitlich durchführen und anwenden zu können, unterstützen sich die Aufsichtsbehörden gegenseitig, insbesondere in Bezug auf Auskunftsersuchen und

aufsichtsbezogene Maßnahmen. Die Aufsichtsbehörden ergreifen alle geeigneten Maßnahmen um den Ansuchen von anderen Aufsichtsbehörden zeitgerecht nachzukommen. Durch eine Anforderung übermittelte Informationen werden nur zu dem Zweck verwendet, für den sie ursprünglich angefordert wurden. Unter gewissen Voraussetzungen können derartige Ansuchen auch abgelehnt werden, z.B. falls diese den Zuständigkeitsbereich der Aufsichtsbehörde überschreiten oder wenn das Ansuchen gegen das Unionsrecht verstößt (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 72).

Durchsetzungsmaßnahmen und Untersuchungen können von Aufsichtsbehörden ebenfalls mithilfe gemeinsamer Maßnahmen durchgeführt werden. Gibt es Niederlassungen vom Verantwortlichen oder dem Auftragsverarbeiter in mehreren Mitgliedsstaaten oder betrifft die Datenverarbeitung betroffene Personen aus mehreren Mitgliedsstaaten, so ist jede betroffene Aufsichtsbehörde berechtigt an den Maßnahmen teilzunehmen. Eine Aufsichtsbehörde kann hierzu Befugnisse und Berechtigungen auf eine andere Aufsichtsbehörde oder deren Mitglieder übertragen soweit dies nach dem Recht des betroffenen Mitgliedsstaates zulässig ist. Sind Bedienstete einer unterstützenden Aufsichtsbehörde in einem anderen Mitgliedsstaat tätig und verursachen bei ihrem Einsatz etwaige Schäden, so übernimmt der einladende Mitgliedsstaat die Verantwortung für ihr Handeln. Etwaige entstandene Schäden durch das Handeln der Bediensteten werden hierbei durch den Mitgliedsstaat ersetzt in dessen Hoheitsgebiet der Schaden entstanden ist (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 72–73).

Um eine einheitliche Umsetzung der Verordnung innerhalb der Europäischen Union zu gewährleisten, arbeiten die Aufsichtsbehörden innerhalb des Kohärenzverfahrens untereinander und mit der Kommission zusammen. Wenn eine zuständige Aufsichtsbehörde eine neue Maßnahme erlässt, so wird vom Ausschuss eine Stellungnahme dazu verfasst. Die Aufsichtsbehörde hat hierfür dem Ausschuss einen Entwurf des Beschlusses zu übermitteln. Zu den Maßnahmen zählen unter anderem die Änderung der Verhaltensregeln, die Ernennung einer Zertifizierungsstelle, die Festlegung von Standard-Datenschutzklauseln, die Genehmigung von Vertragsklauseln oder die Annahme verbindlicher interner Vorschriften (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 73–74).

Die Aufsichtsbehörden, die Kommission oder der Vorsitz des Ausschusses können beantragen, dass Angelegenheiten geprüft werden, die Auswirkungen für mehrere Mitgliedsstaaten oder eine generelle Gültigkeit haben. Dies trifft insbesondere zu, wenn eine zuständige Aufsichtsbehörde den auferlegten Maßnahmen nicht nachkommt (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 74).

Zum Zweck der Streitbeilegung kann der Ausschuss in speziellen Einzelfällen einen verbindlichen Beschluss erlassen. Darunter fällt beispielsweise die Entscheidung welche Aufsichtsbehörde für eine Hauptniederlassung zuständig ist oder der Fall, dass ein maßgeblicher und begründeter Einspruch einer betroffenen Aufsichtsbehörde durch die federführende Aufsichtsbehörde nicht ausreichend begründet abgelehnt wurde. Ein Beschluss wird innerhalb eines Monats von einer Zweidrittelmehrheit des Ausschlusses angenommen. Dieser Beschluss ist für alle betroffenen Aufsichtsbehörden verbindlich und die Kommission wird davon in Kenntnis gesetzt. Wenn

dringlicher Handlungsbedarf besteht, so kann die betroffene Aufsichtsbehörde sofort eine einstweilige Maßnahme mit festgelegter Geltungsdauer von maximal drei Monaten beschließen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 75–76).

3.8 Kapitel 8: Rechtsbehelfe, Haftung und Sanktionen

Das achte Kapitel der DSGVO befasst sich mit Rechtsbehelfen, Haftung und Sanktionen. Jede betroffene Person hat das Recht auf Beschwerde bei der Aufsichtsbehörde, wenn die betroffene Person die Auffassung vertritt, dass ihre personenbezogenen Daten bzw. der Umgang mit diesen Daten gegen die DSGVO verstoßen. Die zuständige Aufsichtsbehörde benachrichtigt den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 80).

Jede natürliche oder juristische Person kann einen gerichtlichen Rechtsbehelf gegen einen sie betreffenden Beschluss einer Aufsichtsbehörde erheben. In diesem Fall sind die Gerichte des Mitgliedsstaates zuständig, in dem sich die betreffende Aufsichtsbehörde befindet (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 80).

Jede natürliche Person hat ebenfalls das Recht eine Klage gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter zu erheben, wenn sie der Ansicht ist, dass eine Datenschutzverletzung im Zusammenhang mit ihren personenbezogenen Daten vorliegt. Zuständig hierfür sind die Gerichte des Mitgliedsstaates, in dem das Vergehen aufgetreten ist oder wahlweise die Gerichte des Mitgliedsstaates, in dem die betroffene Person ihren ständigen Aufenthaltsort hat (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 81).

Eine betroffene Person hat das Recht eine Einrichtung, Organisation oder Vereinigung ohne gewinnbringende Absichten, die im Zusammenhang mit dem Schutz der personenbezogenen Daten tätig ist, damit zu beauftragen eine Beschwerde im Namen der Person einzureichen (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 81).

Erleidet eine Person durch einen Verstoß gegen die DSGVO einen materiellen oder immateriellen Schaden, so hat sie einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder den Auftragsverarbeiter. Alle an der Verarbeitung beteiligten Verantwortlichen haften für den entstandenen Schaden, sofern dieser durch eine nicht verordnungsgemäße Datenverarbeitung entstanden ist. Auftragsverarbeiter haften nur wenn sie den speziell Auftragsverarbeitern auferlegten Verordnungspflichten nicht nachkommen oder wenn sie die rechtmäßig erteilten Datenverarbeitungsanweisungen des Verantwortlichen nicht beachten (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 80).

Sind mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter an demselben Schaden beteiligt, so haftet jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden und trägt den Schadensersatz. Der Verantwortliche oder der Auftragsverarbeiter können von der Haftung befreit werden sofern sie eindeutig nachweisen können, dass sie für keinerlei Umstände, die zu dem Schaden geführt haben verantwortlich sind (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 80–81).

Die Aufsichtsbehörden stellen sicher, dass die verhängten Geldstrafen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sind. Die folgenden Kriterien können unter anderem herangezogen werden, um über die Verhängung einer Geldbuße zu entscheiden und um die Höhe des Betrags der Geldbuße festzulegen:

- Schwere, Art und Dauer des Verstoßes in Zusammenhang mit der Verarbeitungsart, dem Verarbeitungsumfang, dem Verarbeitungszweck, der Anzahl der betroffenen Personen und dem Schadensausmaß;
- Fahrlässige oder vorsätzliche Handlungen, die zu dem Verstoß führten;
- Durchgeführte Maßnahmen vom Verantwortlichen oder dem Auftragsverarbeiter zur Verminderung des entstandenen Schadens;
- Bereits eingetretene Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
- Verantwortungsgrad des Verantwortlichen oder des Auftragsverarbeiters anhand der getroffenen technischen und organisatorischen Maßnahmen;
- Der Zusammenarbeitsumfang mit einer Aufsichtsbehörde um den negativen Auswirkungen des Verstoßes abzuhelfen;
- Wie der Verstoß bekannt wurde und den Umfang der Verstoßmeldung durch den Verantwortlichen oder den Auftragsverarbeiter;
- Welche Kategorien von personenbezogenen Daten durch den Verstoß betroffen sind;
- Wurden Verhaltensregeln eingehalten und gab es Zertifizierungen.

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 82)

Je nach Art des Verstoßes können Geldstrafen von bis zu 20 Millionen Euro oder bei Unternehmen bis zu 4% des weltweit erzielten Jahresumsatzes verhängt werden, je nachdem welcher Betrag höher ist. Den Mitgliedsstaaten steht offen, ob und in welchem Umfang sie Strafen für Behörden und öffentliche Stellen in dem jeweiligen Mitgliedsstaat verhängen. Die Mitgliedsstaaten können Sanktionen für Verstöße gegen diejenigen Verordnungen festlegen, die keinen Geldbußen unterliegen und Maßnahmen zur Anwendung dieser Sanktionen treffen. Die definierten Sanktionen müssen verhältnismäßig, wirksam und abschreckend sein (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 82–83).

3.9 Kapitel 9: Vorschriften für besondere Verarbeitungssituationen

Die Vorschriften für besondere Verarbeitungssituationen werden im neunten Kapitel der DSGVO ausgeführt. Die Mitgliedsstaaten müssen dafür sorgen, dass das Recht auf freie Meinungsäußerung und Informationsfreiheit im Einklang mit der Verordnung stehen. Dies betrifft auch die Verarbeitung von Informationen bzw. Daten für journalistische, wissenschaftliche, künstlerische und literarische Zwecke. Die damit im Zusammenhang stehenden Rechtsvorschriften der Mitgliedsstaaten werden der Kommission mitgeteilt (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 83–84).

Durch Rechtsvorschriften oder Kollektivvereinbarungen können spezifischere Vorschriften, zur Gewährleistung des Schutzes, der Rechte und der Freiheiten bei der personenbezogenen Datenverarbeitung von Beschäftigtendaten im Beschäftigungskontext verfasst werden. Dies gilt insbesondere für die folgenden Zwecke:

- Einstellung
- Arbeitsauftragserfüllung
- Management
- Arbeitsplanung und Arbeitsorganisation
- Gleichheit und Diversität am Arbeitsplatz
- Gesundheit und Sicherheit am Arbeitsplatz
- Schutz des Arbeitgebereigentums
- Schutz des Kundeneigentums
- Inanspruchnahme für individuelle und kollektive Rechte und Leistungen
- Beendigung des Beschäftigungsverhältnisses

  (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 84)

Die Vorschriften der Mitgliedsstaaten enthalten besondere Maßnahmen zur Wahrung der Menschenwürde, der Grundrechte und der berechtigten Interessen der betroffenen Person. Dies gilt besonders im Zusammenhang mit der Verarbeitungstransparenz der personenbezogenen Datenübermittlung innerhalb von Unternehmensgruppen oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben und für Überwachungssysteme am Arbeitsplatz (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 84).

Die Verarbeitung von wissenschaftlichen oder historischen Forschungszwecken, statistischen Zwecken oder und im öffentlichen Interesse liegenden Archivzwecken muss geeigneten Garantien unterliegen. Diese Garantien stellen sicher, dass technische und organisatorische Maßnahmen gesetzt wurden um insbesondere die Datenminimierung zu gewährleisten. Die Pseudonymisierung kann zu diesen Maßnahmen gehören (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 84–85).

3.10 Kapitel 10: Delegierte Rechtsakte und Durchführungsrechtsakte

In Kapitel zehn werden delegierte Rechtsakte und Durchführungsrechtsakte behandelt. Der Kommission wurde bis auf unbestimmte Zeit ab Mai 2016 die Befugnis übertragen delegierte Rechtsakte zu erlassen. Diese Befugnis kann vom Europäischen Parlament oder dem Rat jederzeit widerrufen werden. Wird ein delegierter Rechtsakt von der Kommission erlassen, so übermittelt sie diesen dem Europäischen Parlament und dem Rat. Ein delegierter Rechtsakt tritt drei Monate nach der Übermittlung in Kraft oder wenn das Europäische Parlament und der Rat der Kommission mitteilen, dass sie keinen Einspruch dagegen erheben werden (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 85–86).

3.11 Kapitel 11: Schlussbestimmungen

Das letzte Kapitel der DSGVO trägt den Titel Schlussbestimmungen. Zunächst wird die Aufhebung der Richtlinie 95/46/EG mit 25. Mai 2018 ausgeführt und sodann erläutert, dass die in der Richtlinie 95/46/EG eingesetzte Gruppe zum Schutz von Personen bei der personenbezogenen Datenverarbeitung in der DSGVO der eigens dafür errichtete Europäische Datenschutzausschuss sein wird (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 86).

Im Zusammenhang mit der Richtlinie 2002/58/EG wird erwähnt, dass die DSGVO natürlichen oder juristischen Personen keine weiteren Pflichten bei der Verarbeitung von Daten in Verbindung mit der Bereitstellung von elektronischen Kommunikationsdiensten in öffentlichen Kommunikationsnetzen auferlegt. Beschlossene internationale Übereinkünfte die vor dem 24. Mai 2016 im Zusammenhang mit der Übermittlung von personenbezogenen Daten an Drittländer oder internationale Organisationen und im Einklang mit dem vor diesem Tag geltenden Unionsrecht stehen, bleiben in Kraft bis sie geändert, ersetzt oder gekündigt werden (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 86–87).

Die Kommission legt dem Europäischen Parlament sowie dem Rat bis zum 25. Mai 2020 und danach alle vier Jahre einen Bericht über die Überprüfung der DSGVO vor. Zur Berichterstellung kann die Kommission Hilfe von den Mitgliedsstaaten anfordern. Diese Berichte werden ebenfalls öffentlich zugänglich gemacht. Besonders relevant bezüglich jener Berichte sind das Kapitel fünf über die Übermittlung der personenbezogenen Daten an Drittländer oder internationale Organisationen und das Kapitel sieben über die Zusammenarbeit und Kohärenz. Um einen einheitlichen und kohärenten Schutz von natürlichen Personen und der Verarbeitung personenbezogener Daten zu gewährleisten, legt die Kommission gegebenenfalls Gesetzgebungsvorschläge zur Änderung anderer Rechtsaktie der Europäischen Union im Zusammenhang mit der Datenverarbeitung vor (Europäisches Parlament und Rat der Europäischen Union, 2016, S. 87).

3.12 Zusammenfassung

Die Datenschutzverordnung umfasst mit ihren 173 angeführten Gründen und den 99 Artikeln in elf Kapiteln zahlreiche Aspekte, um den Schutz von personenbezogenen Daten bei der Datenverarbeitung zu verbessern. Im Vordergrund steht die Vereinheitlichung des Datenschutzes aller Mitgliedsstaaten der Europäischen Union. Den Mitgliedsstaaten wird jedoch genug Spielraum gelassen um die Vorschriften selbst umzusetzen bzw. anzupassen. Unternehmen wird bei der Datenverarbeitung auferlegt, dass die geeigneten technischen und organisatorischen Maßnahmen getroffen werden um die Rechte der betroffenen Person bei der Verarbeitung von personenbezogenen Daten zu gewährleisten. Darüber hinaus wird dem Verantwortlichen und dem Auftragsverarbeiter aufgetragen die Rechtmäßigkeit und die Transparenz bei der Verarbeitung sicherzustellen. Die Daten der Personen müssen dem Zweck der Verarbeitung dienen und dürfen nicht für andere illegitime Zwecke missbraucht werden.

Betroffenen Personen werden mehrere Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten zugeschrieben. Darunter fallen das Recht zur Informationsanfrage über die Art und Menge der personenbezogenen Daten, das Recht der Verarbeitung zu widersprechen sowie das Recht zur Berichtigung bzw. Löschung und Übertragung der personenbezogenen Daten. Zur rechtmäßigen Verarbeitung von personenbezogenen Daten holt das Unternehmen von der betroffenen Person eine eindeutige Einwilligung ein. Diese Einwilligung kann von der betroffenen Person jederzeit widerrufen werden. Werden personenbezogene Daten in einer hohen Menge oder in großem Umfang innerhalb einer Organisation verarbeitet, so macht die Ernennung eines Datenschutzbeauftragten Sinn. Die Hauptaufgabe eines Datenschutzbeauftragten ist die Sicherstellung aller Vorkehrungen zur sicheren Verarbeitung von personenbezogenen Daten. Neben der Einführung von Sicherheitsmaßnahmen zum Datenschutz gehören die Bewusstseinsschaffung bzw. Schulung der Mitarbeiter und allen anderen Personen mit Zugriff auf personenbezogene Daten zu den Aufgaben des Datenschutzbeauftragten.

Sollte eine Verletzung des Schutzes der personenbezogenen Daten vorliegen, so werden Fristen und Vorgehensweisen zur Information der betroffenen Personen sowie der zuständigen Aufsichtsbehörde angeführt. Bei Verstößen können monetäre Strafen von bis zu 20 Millionen Euro oder 4% des Jahresumsatzes eines Unternehmens verhängt werden. Wird eine wesentliche Änderung der Verarbeitung von personenbezogenen Daten oder ein neues Produkt oder Projekt geplant, so ist eine Datenschutzfolgeabschätzung durchzuführen um sicherzustellen, dass keine gravierenden Änderungen bei dem Datenverarbeitungsverfahren notwendig sind. Besonders bei der Datenweitergabe an Drittländer und internationale Organisationen wird ein hoher Wert auf die ordnungsgemäße Vereinbarung bei der Verarbeitung gelegt.

4 DATENERHEBUNG ZUR UMSETZUNG DER DSGVO KONFORMITÄT

Im Zuge der Datenerhebung werden Erfahrungswerte, sowie das einschlägige Fachwissen von Experten im Bereich der DSGVO erhoben. Der für die Fragebogengestützten Experteninterviews gewählte Personenkreis setzt sich aus technischen Fachpersonen, organisatorisch Verantwortlichen und Fachexperten für die DSGVO zusammen. Die erhaltenen Informationen über die Vorgehensweise bei der Umsetzung, die dafür benötigten Ressourcen sowie etwaige auftretende Problemstellungen werden danach ausgewertet und miteinander verglichen. Neben Experteninterviews werden auch bereits verfügbare literarische Werke zur DSGVO Compliance betrachtet um eine Best Practice Vorgehensweise zur DSGVO Konformität zu erstellen.

4.1 Experteninterviews

Um spezifische Informationen zur DSGVO Compliance zu erhalten wird eine empirische, qualitative Umfrage in Form von Experteninterviews durchgeführt. Experteninterviews sind ein systematisches und theoriengeleitetes Verfahren zur Datenerhebung. Im Unterschied zur quantitativen Befragung ist bei qualitativen Experteninterviews die Auswertbarkeit aufgrund mangelnder Standardisierung erschwert (Robert Kaiser, 2014, S. 6).

Damit eine Aussage über die erhaltenen Ergebnisse getroffen werden kann, stützt zusätzlich ein Fragebogen bzw. Gesprächsleitungsbogen die geführten Interviews. Der Fragebogen umfasst wichtige Aspekte der DSGVO und der DSG Konformität. Das Ziel der Datenerhebung ist eine vergleichbare Informations- und Wissenssammlung durch die gesammelten Erfahrungen von verschiedenen Experten aus dem angewandten Bereich des Datenschutzes, zu erhalten.

4.2 Identifikation relevanter Themenbereiche

Um alle wichtigen Themenbereiche für die DSGVO Compliance abzudecken, werden neben der Verordnung zusätzliche Quellen zu diesem Thema herangezogen. Die folgenden Themenbereiche werden in den Experteninterviews behandelt:

- Vorgehen bei der Informationssammlung zur DSGVO/DSG Compliance
- Datenschutzverantwortung
- Erhebung und Analyse aller verwendeten personenbezogenen Daten
- Relevanz der personenbezogenen Daten für den Geschäftsprozess
- Technische und organisatorische Maßnahmen
- Zertifizierungen und Prüfung der Datenschutzmaßnahmen
- Vorkehrungen zur Informations- und Auskunftspflicht

- Sensibilisierungsmaßnahmen und Schulung der Angestellten
- Fortlaufende Verbesserung und Aktualisierung der Datenschutzmaßnahmen
- Wissen aus der DSGVO Compliance-Umsetzung

4.3 Erstellung eines unterstützenden Fragebogens

Damit ein Vergleich der unterschiedlichen durch die Experten erhaltenen Informationen möglich ist, werden die Experteninterviews mit Unterstützung eines Fragebogens durchgeführt. Um spezifische Antworten zu den einzelnen Themenbereichen zu erhalten, werden diese Berichte anhand von detaillierten Fragen genauer erforscht. Die folgenden Themen sind im Fragebogen enthalten.

4.3.1 Vorgehen bei der Informationssammlung zur DSGVO/DSG Compliance

Zunächst wird erhoben wie sich die befragten Personen, Abteilungen bzw. Unternehmen fachlich auf die DSGVO vorbereitet haben. Man kann hier beispielsweise erfragen ob auf externe Ressourcen wie juristische Beratung, Veranstaltungen oder Schulungen zurückgegriffen wurde oder ob die befragten Personen spezielle literarische Quellen zur Verbesserung des Fachwissens über die DSGVO herangezogen haben und empfehlen können. Derartige Informationen sind für eine bestmögliche Vorbereitung von Vorteil.

Vorbereitete Fragen:

- Wie haben Sie bzw. Ihre Kollegen sich fachlich auf die Umsetzung der DSGVO vorbereitet?
- Auf welche Ressourcen haben Sie zurückgegriffen um Fachwissen zu erlangen?
- Können Sie Literatur oder andere Quellen empfehlen um Datenschutzfachwissen zu erwerben?

4.3.2 Datenschutzverantwortung

Der zweite Themenbereich, der in den Experteninterviews abgedeckt wird, bezieht sich auf den Umgang mit der Verantwortung im Bereich der Verarbeitung von personenbezogenen Daten und den dazu gehörenden Datenschutzmaßnahmen. Ob ein Datenschutzbeauftragter im Unternehmen ernannt wird, hängt von der Unternehmensgröße und der Art der Datenverarbeitung bzw. der Datenmenge/-art ab. Es wird erfragt wie die jeweilige mit dem Datenschutz betraute Person ausgewählt, eingestellt bzw. geschult wurde und welche Qualitäten/Qualifikationen die Person für die Ernennung zum Datenschutzbeauftragten bereits vorweisen muss. Eventuell wurde die Verantwortung aber auch an einen externen Partner weitergeben. Falls dies so ist, stellen sich weitere Fragen, nämlich welche Gründe für diese Entscheidung ausschlaggebend waren und wie bei der Auswahl des Partners vorgegangen

wurde. Auch die Identifikation und Informierung etwaiger Auftragsverarbeiter ist ein wichtiger Punkt der Datenschutzverantwortung.

Vorbereitete Fragen:

- Wurde in Ihrem Unternehmen ein Datenschutzverantwortlicher bzw. ein Datenschutzbeauftragter ernannt?
- Falls vorhanden: Wie haben Sie etwaige Auftragsverarbeiter über ihre Pflichten informiert?
- Wurden Schulungen/Weiterbildungen für den Datenschutzverantwortlichen durchgeführt?
- Haben Sie auf externe Ressourcen (Fachpersonal) zugegriffen?
- Waren die Qualifikationen und das Fachwissen eine Hürde hinsichtlich der Personenwahl?

4.3.3 Erhebung und Analyse aller verwendeten personenbezogenen Daten

Bevor Maßnahmen zur Datensicherheit ausgewählt oder umgesetzt werden, sollte zunächst eine umfangreiche Analyse, der zum gegenwärtigen Zeitpunkt vorhandenen und verarbeiteten personenbezogenen Daten durchgeführt werden. Dieser Themenbereich dient der Erfragung, welche Techniken und Vorgehensweisen zur Erhebung der bereits vorhandenen bzw. verarbeiteten Daten von den Fachexperten angewandt wurden.

Vorbereitete Fragen:

- Wie sind Sie bei der Datenerhebung der personenbezogenen Daten vorgegangen?
- Welche Techniken und Vorgehensweisen haben Sie hierfür verwendet?

4.3.4 Relevanz der personenbezogenen Daten für den Geschäftsprozess

Jener Themenbereich befasst sich mit der Relevanz von gespeicherten personenbezogenen Daten zur Erfüllung des Geschäftsprozesses. Hier soll festgestellt werden, ob Daten als unnötig, veraltet oder unbrauchbar identifiziert wurden und wie mit ihnen umgegangen wurde. Ebenfalls soll festgestellt werden, ob Maßnahmen zur Löschung und Bereinigung getroffen wurden um nicht benötigte Daten zu entfernen oder ob Maßnahmen wie Anonymisierung durchgeführt wurden um einen besseren Datenschutz zu gewährleisten.

Vorbereitete Fragen:

- Waren sämtliche verfügbare personenbezogene Daten notwendig um den Geschäftsprozess zu gewährleisten?
- Konnten Sie auch „nicht notwendige“ personenbezogene Daten identifizieren?
- Wurden Maßnahmen zur Löschung nicht benötigter Daten getroffen?
- Wurden Daten anonymisiert?

4.3.5 Technische und organisatorische Maßnahmen

Der Themenbereich technische und organisatorische Maßnahmen ist für die Erstellung eines Best Practice Leitfadens von entscheidender Bedeutung. Deshalb wird den Experten zu diesem Themenblock die größte Anzahl an Interviewfragen gestellt. Zunächst wird in Erfahrung gebracht, inwieweit sich die Personen, Abteilungen sowie Unternehmen über mögliche oder notwendige technische und organisatorische Maßnahmen erkundigt haben bzw. wie sie bei der Informationsbeschaffung vorgegangen sind. Falls auf Werkzeuge oder externe Ressourcen zurückgegriffen wurde, wäre eine Bewertung oder mögliche Weiterempfehlung dieser Werkzeuge bzw. Ressourcen wünschenswert.

Ebenfalls wird erfragt, ob das Unternehmen Abnahme- und Prüfverfahren der jeweiligen TOMs verwendet und ob wiederkehrende Verfahren zur Kontrolle der Maßnahmenaktualität eingeplant werden. Besonders für den Katastrophenfall sollten Unternehmen gerüstet sein, also bereits Pläne wie in der Situation eines data breach zu reagieren ist und einen Notfalls- bzw. Wiederanlaufplan speziell für den IT-Infrastrukturbereich vorliegen haben. Es wird auch versucht in Erfahrung zu bringen, welche Maßnahmen für die Fachexperten persönlich, besonders interessant bzw. einprägsam waren.

Vorbereitete Fragen:

- Wie haben Sie sich über die TOMs informiert?
- Wie sind Sie bei der Umsetzung der TOMs vorgegangen?
- Haben Sie Werkzeuge oder externe Ressourcen verwendet?
- Gab es für die notwendigen TOMs eine Abnahme bzw. eine Überprüfung?
- Gibt es eine laufende Kontrolle für die TOMs?
- Wurden Maßnahmen im Fall eines data breach getroffen?
- Gibt es ein Betriebshandbuch, einen Notfall- und Wiederanlaufplan?
- Wurden bauliche Änderungen durchgeführt?
- Welche TOMs waren für Sie besonders interessant/relevant/einprägsam?

4.3.6 Zertifizierungen und Prüfung der Datenschutzmaßnahmen

In diesem Themenbereich wird erfragt, ob das jeweilige Unternehmen bereits eine Zertifizierung der Datenschutzmaßnahmen, einer Fachperson/-abteilung, eines Unternehmensbereiches oder des gesamten Unternehmens durchgeführt hat bzw. ob es Pläne für eine Zertifizierung in näherer Zukunft gibt.

Vorbereitete Fragen:

- Wurde eine Datenschutzzertifizierung oder Prüfung von einer externen Stelle durchgeführt?

- Haben Sie darüber nachgedacht Ihr Unternehmen bzgl. des Datenschutzes zu zertifizieren z.B. ISO 27001?
- Wurden Personen in Ihrem Unternehmen geschult oder zertifiziert?

4.3.7 Vorkehrungen zur Informations- und Auskunftspflicht

Unternehmen müssen auf Anfragen von betroffenen Personen im Zusammenhang mit der vorgeschriebenen Informations- und Auskunftspflicht in fristgerechter Zeit reagieren. Es soll in Erfahrung gebracht werden, ob das jeweilige Unternehmen auf derartige Anfragen vorbereitet ist, sie fristgerecht beantworten kann und Personen mit ausreichenden Berechtigungen und adäquatem Fachwissen dafür zuständig sind. Auch die Löschung sowie Richtigstellung von personenbezogenen Daten kann von betroffenen Personen gefordert werden. Hierauf sollten Unternehmen ebenfalls vorbereitet sein.

Vorbereitete Fragen:

- Wurden in Ihrem Unternehmen Vorkehrungen zur Auskunftspflicht getroffen?
- Wurden Personen/Abteilungen definiert, die für derartige Anfragen zuständig sind?
- Können Anfragen zu personenbezogenen Daten und deren etwaige Richtigstellung bzw. Löschung innerhalb des vorgeschriebenen Zeitrahmens beantwortet oder durchgeführt werden?

4.3.8 Sensibilisierungsmaßnahmen und Schulung der Angestellten

Im Umgang mit personenbezogenen Daten spielt die Security Awareness der Mitarbeiter eines Unternehmens eine entscheidende Rolle. Im Rahmen der Interviews soll festgestellt werden inwieweit die Mitarbeiter hinsichtlich dieses wichtigen Bereichs sensibilisiert und welche Maßnahmen durchgeführt wurden. Die Einschätzung des Fachexperten bezüglich des derzeitigen Standes des Sicherheitswissens der Unternehmensangestellten soll auch erfragt werden um festzustellen wie erfolgreich die gegenwärtig eingesetzten Maßnahmen sind. Ob und welche Tätigkeiten durchgeführt werden um Mitarbeiter über aktuelle Sicherheitsthemen und neue Gefahren zu informieren ist ein weiterer relevanter Punkt.

Vorbereitete Fragen:

- Wurden die Angestellten in Ihrem Unternehmen hinsichtlich des Datenschutzes sensibilisiert bzw. geschult?
- Welche Maßnahmen wurden zur Steigerung der Security Awareness durchgeführt?
- Wie schätzen Sie den aktuellen Status des Sicherheitswissen der Angestellten ein?
- Sind fortlaufende bzw. wiederkehrende Maßnahmen zur Verbesserung des Sicherheitswissens der Angestellten geplant?

4.3.9 Fortlaufende Verbesserung und Aktualisierung der Datenschutzmaßnahmen

Ein weiterer wichtiger Teil des Sicherheitskonzepts ist die fortlaufende Verbesserung und Aktualisierung aller Datenschutzmaßnahmen. Es wird versucht zu erfragen wie die zuständige Abteilung des jeweiligen Unternehmens den Datenschutz aufrechterhält, aktualisiert und auf mögliche neue Gefahren innerhalb und außerhalb des Unternehmens reagiert. Falls wiederkehrende Verbesserungsmaßnahmen bereits geplant sind, wird erfragt welche Informationsquellen zur Recherche herangezogen und wie die Maßnahmenaktualisierungen terminisiert werden (z.B. Wartungstage oder Reaktion auf Ereignisse).

Vorbereitete Fragen:

- Sind in Ihrem Unternehmen fortlaufende Maßnahmen zur Verbesserung des Datenschutzes geplant?
- Wie wird auf aktuelle Gefahren und Bedrohungen des Datenschutzes reagiert?

4.3.10 Wissen aus der DSGVO Compliance-Umsetzung

Am Ende der Interviews soll noch die persönliche Erfahrung der Fachexperten bezüglich der Umsetzung der DSGVO Maßnahmen erhoben werden. Besonders die begangenen Fehler bzw. gelernten Lektionen bei der Durchführung wie auch Tipps/Empfehlungen für Unternehmen oder Mitarbeiter, die sich demnächst mit dem Thema DSGVO Compliance beschäftigen, werden in diesem Kontext erfragt.

Vorbereitete Fragen:

- Welche der im Interview besprochenen Punkte, Maßnahmen oder Themenbereiche würden Sie mit ihrem jetzigen Wissen anders durchführen bzw. umsetzen?
- Wenn Sie noch einmal die Compliance Maßnahmen umsetzen müssten, was würden Sie anders machen?
- Welche Tipps können Sie einer Person geben, die gerade damit beginnt die DSGVO Compliance umzusetzen?

4.4 Interviewdurchführung - Datenerhebung

Die fragebogengestützten Interviews werden mittels der Sprachmemo App eines Apple iPhone aufgenommen damit eine spätere Auswertung leichter durchgeführt werden kann. Es wurde so weit wie möglich versucht eine ruhige Räumlichkeit und entspannte Atmosphäre zu schaffen um Ablenkungen während der Interviews zu vermeiden. Alle Interviews wurden anonym durchgeführt, das heißt es werden keine Personen- oder Unternehmensnamen genannt.

Die zehn ausgewählten Datenschutzexperten mit denen Experteninterviews geführt wurden, haben zum größten Teil unterschiedliche Aufgabengebiete bzw. Positionen in ihrem

Unternehmen. Darunter fallen z.B. Datenschutzberater, Infrastrukturleiter Datenschutzbeauftragte und technische Umsetzer. Deshalb ist davon auszugehen, dass nicht jede Person zu allen Themenbereichen Informationen liefern kann. Dies gilt besonders für diejenigen Personen, die in Großunternehmen angestellt sind.

Wenn die Experten von sich aus mehrere Fragen auf einmal beantworten oder einen Themenbereich mit einer Antwort bereits ausreichend abgedeckt haben, so wurden die bereits beantworteten Fragen oder Themenbereiche nicht erneut erfragt. Der Interviewfokus liegt primär auf den technischen und organisatorischen Maßnahmen sowie deren Umsetzung. Deshalb variiert die Interviewlänge der einzelnen Gespräche. Es wurde dennoch eine Interviewzeit zwischen mindestens 15 und maximal 45 Minuten angestrebt.

4.5 Datenaufbereitung und Auswertung

Die aufgenommenen Interviews wurden mehrfach überprüft und auf besonders relevante Aussagen hin untersucht. Neue Einsichten, Empfehlungen oder Warnungen der Fachexperten ergänzen die gesammelten Literaturinformationen. Die bereits verfügbaren Informationen werden somit durch das Expertenwissen im tatsächlichen Anwendungsfall ergänzt und dadurch aussagekräftiger.

5 IST-ANALYSE DER AKTUELLEN VERARBEITUNGS-SITUATION VON PERSONENBEZOGENEN DATEN

Für die Best Practice Umsetzung der Ist-Analyse der personenbezogenen Datenverarbeitung werden verschiedene Fachartikel, Formulare, Vorlagen und das zuvor durch die Experteninterviews erhobene Fachwissen verwendet. Eine primäre Quelle für Fachwissen stellt die Website der Wirtschaftskammer Österreich (WKO) dar. Hier sind zahlreiche Fachartikel mit zusätzlichen Informationen zur DSGVO Compliance zu finden. Die WKO Website zur DSGVO Umsetzungsunterstützung ist unter folgendem Link zu finden:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Unterstuetzung-zur-Umsetzung-der-DSGVO.html

Dies wurde auch in den durchgeführten Experteninterviews bestätigt. In jedem Interview wurde auf die WKO Seite, als ausgezeichnete Quelle für Informationen zur DSGVO verwiesen.

Zusätzlich wurde die Website bzw. der abonnierbare Newsletter der österreichischen Datenschutzbehörde genannt. Diese Website ist unter folgendem Link zu finden:

https://www.dsb.gv.at/

Die verschiedenen Tätigkeiten werden zunächst in einzelne Bereiche unterteilt. Die angeführten Themenbereiche müssen nicht nacheinander abgeschlossen werden, sondern können parallel bearbeitet werden. Besonders bei der Identifikation von vorhandenen personenbezogenen Daten wird meist eine bereichsübergreifende Bearbeitung notwendig und kann daher einen längeren Zeitraum in Anspruch nehmen.

Nachdem die Vorbereitungen abgeschlossen sind, wird mit der Ist-Analyse, also der Erhebung der aktuellen Situation begonnen. Die folgenden Teilbereiche können sich teilweise inhaltlich überschneiden. Die daraus resultierenden Maßnahmen und Tätigkeiten werden in den darauffolgenden Kapiteln näher erläutert.

5.1 Vorbereitung

Bevor mit der Analyse begonnen wird, sollten einige Vorbereitungen getroffen werden. Die hier angeführten Vorbereitungsmaßnahmen haben nicht direkt mit der Ist-Analyse zu tun, sollten jedoch vor der Durchführung der Analyse geklärt sein (Wirtschaftskammer Österreich, 2018e). Im Besonderen kann die Ernennung einer spezifischen Ansprechperson für die DSGVO Anpassungen Wege verkürzen und Abläufe beschleunigen.

5.1.1 Nominierung einer zuständigen Person

Zunächst sollte eine zuständige Person bzw. sollten mehrere zuständige Personen für die DSGVO Anpassung nominiert werden. Die etwaige Person kann aus dem eigenen Unternehmen

kommen oder auch von einer externen Einrichtung hinzugezogen werden (Wirtschaftskammer Österreich, 2018e). Für größere Unternehmen eignet sich oftmals eine Kombination aus beiden Optionen. Die interne Rechtsabteilung könnte beispielsweise Informationen bei einem externen Rechtsberater mit Fokus auf personenbezogenen Datenschutz einholen oder die IT-Abteilung könnte ein Audit oder penetration testing durch externe Firmen durchführen lassen.

Aus den Experteninterviews ging hervor, dass in nahezu jedem Unternehmen auf externe Fachpersonen bei der DSGVO- Umstellungsvorbereitung zurückgegriffen wurde. Die externen Fachpersonen wurden eingesetzt um interne Fachpersonen bei den DSGVO Umsetzungsmaßnahmen zu unterstützen bzw. um etwaige Fragen zu beantworten. Schulungen und Weiterbildungsmaßnahmen sind meist mit hohem Ressourceneinsatz verbunden. Deshalb macht es bei kleineren Unternehmen oder Unternehmen mit geringem Risikopotential durchaus Sinn auf externe Ressourcen zuzugreifen. Die meisten Experten erwähnten, dass vor allem auf Rechtsanwählte, die sich mit dem Fachgebiet des Datenschutzes beschäftigen, zurückgegriffen wurde.

5.1.2 Wird ein Datenschutzbeauftragter benötigt?

Laut DSGVO ist eine Verpflichtung zur Ernennung eines Datenschutzbeauftragten nur in folgenden Fällen notwendig:

- Die Kerntätigkeit des Unternehmens besteht in der Verarbeitung von personenbezogenen Daten mit hohem Umfang oder einer speziellen Art und benötigt daher eine regelmäßige und systematische Überwachung (Beispiele: Banken, Versicherungen);
- Zur Erfüllung der Kerntätigkeit des Unternehmens ist die Verarbeitung von sensiblen personenbezogenen Daten oder Daten über strafrechtliche Verurteilungen bzw. Straftaten notwendig (Beispiel: Krankenanstalten).

  (Wirtschaftskammer Österreich, 2019a)

Unter regelmäßig wird eine fortlaufende, wiederkehrende, an bestimmten Zeitpunkten stattfindende oder ständige Tätigkeit verstanden. Mit systematisch ist eine vereinbarte, organisierte, methodische oder im Rahmen eines Datenerfassungsplans erfolgende Tätigkeit gemeint. Es können sowohl Verantwortliche als auch Auftragsverarbeiter dieser Verpflichtung unterliegen. Ein Datenschutzbeauftragter kann von Unternehmen auch auf freiwilliger Basis jederzeit ernannt werden (Wirtschaftskammer Österreich, 2019a).

Der Datenschutzbeauftragte sollte einige Qualifikationen auf dem Gebiet des Datenschutzes aufweisen. Darunter fällt einschlägiges Fachwissen bezüglich Datenschutzrecht und der Datenschutzpraxis. Der Datenschutzbeauftragte muss ebenfalls in der Lage sein die an ihn gestellten Anforderungen und Aufgaben zu erfüllen. Bei Rechtsfragen können auch externe Berater herangezogen werden um den Datenschutzbeauftragten zu unterstützen (Wirtschaftskammer Österreich, 2019a).

5.1.3 Budgetierung, Zeitplanung und Ressourcenbereitstellung

Die Budgetierung, Zeitplanung und Ressourcenbereitstellung sollte ebenfalls vorab durchgeführt werden um Ressourcenengpässe oder Personalmangel während der Umsetzung zu vermeiden. Hierbei ist darauf zu achten, dass alle notwendigen Mitarbeiter oder Abteilungen über den Ressourcen- und Zeiteinsatz rechtzeitig informiert werden (Wirtschaftskammer Österreich, 2018e).

Die Auswertung der Experteninterviews zeigte, dass bei größeren Unternehmen die Vermittlung der Wichtigkeit der DSGVO-Umsetzungsthemen ein entscheidender Faktor ist. Diesbezüglich wurden Zeitpunkte von mehreren Monaten vor 25.Mai 2018 genannt um die Unterstützung und die nötigen Ressourcen vom Vorstand bzw. der Unternehmensführung zu erhalten.

Einige der Fachexperten gaben zu Protokoll, dass in ihren Unternehmen kurz vor Inkrafttreten der DSGVO noch bestimmte Themen bzw. Fragen zur DSGVO-Umsetzung offen waren. Dadurch herrschte Zeitdruck in den Abteilungen und meist brachte dieser Druck Probleme, Fehlentscheidungen bzw. halb fertige Lösungen mit sich. Deshalb sollten bei der Zeit- und Ressourcenplanung genügend Reserven eingeplant werden.

5.2 Welche personenbezogenen Daten derzeit werden verarbeitet?

Der erste Schritt der Ist-Analyse ist die Beantwortung der Frage: Welche personenbezogenen Daten bzw. Datenarten werden derzeit verarbeitet (Wirtschaftskammer Österreich, 2018e)? Hierbei werden die folgenden Kategorien voneinander unterschieden:

Allgemeine personenbezogene Daten

Beispiele: Namen, Kennnummer, Standortdaten, Bankdaten, Geburtsdatum

(Wirtschaftskammer Österreich, 2018b)

Besondere Kategorien personenbezogener Daten

Gesundheitsdaten
Beispiele: Krankengeschichte, Gesundheitsdienstleistungen

Genetische Daten
Beispiele: Fingerabdruck, Iris Scan

Biometrische Daten
Beispiele: Unterschriften, Gesichtsbilder

Andere sensible personenbezogene Daten
Beispiele: sexuelle Orientierung, ethnische Herkunft, politische Meinung, Religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeiten

(Wirtschaftskammer Österreich, 2018b)

Die Fachexperten bezeichneten in den Interviews als optimale Vorgehensweise zur DSGVO-Umsetzung eine bereichsweite Datenerhebung. Diesbezüglich wurden je nach Fachbereich eine

oder mehrere zuständige Personen ernannt, meist Führungspersonen, die für die Datenerhebung in dem jeweiligen Bereich zuständig waren. Durch diese Vorgehensweise wurde das Fachwissen der einzelnen Personen optimal genutzt um alle verarbeiteten Daten zu identifizieren und die Verarbeitungsvorgänge bestmöglich zu gestalten.

5.3 Welche Datenverarbeitungsvorgänge bestehen?

Im nächsten Schritt sollte der derzeitige Stand der laufenden Datenverarbeitung betrachtet werden. Nach der alten Rechtslage (DSG 2000) mussten Unternehmen Datenverarbeitungsvorgänge im Datenverarbeitungsregister (DVR) registrieren (Wirtschaftskammer Österreich, 2018b).

Mit dem Inkrafttreten der DSGVO entfiel die Verpflichtung eine DRV-Meldung an die Datenschutzbehörde zu übermitteln. Seither muss der Verantwortliche unter den in Artikel 30 erwähnten Voraussetzungen ein eigenes Datenverarbeitungsverzeichnis anlegen. Ebenfalls besteht unter bestimmten Voraussetzungen die Verpflichtung eine Datenschutz-Folgenabschätzung durchzuführen. Alle DVR-Meldungen an die Datenschutzbehörde vor Eintritt der DSGVO entbinden den Datenschutzverantwortlichen nicht von den künftigen Verpflichtungen zur Führung eines Datenverarbeitungsregisters. Bis zum 31. Dezember 2019 steht das Datenverarbeitungsregister für Archivzwecke weiterhin zur Verfügung. Bis zu diesem Datum können vom Auftraggeber die bereits bereitgestellten DVR-Meldungen als PDF oder XML Dokument exportiert werden (Datenschutzbehörde Republik Österreich, o.D.b).

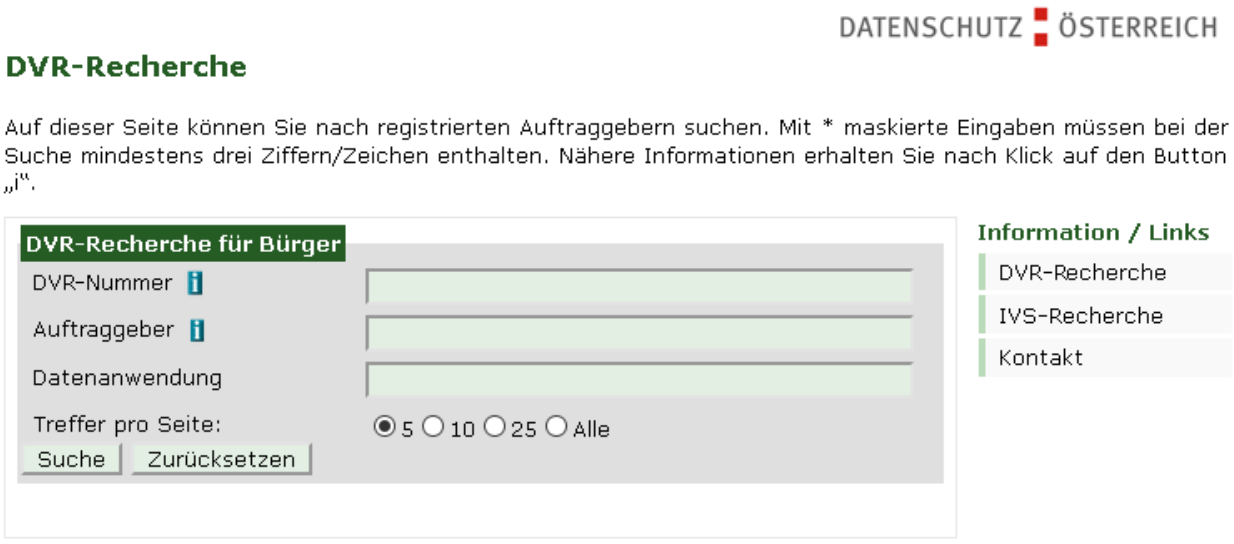

Abbildung 3: Übersicht der DVR-Recherche Website (Datenschutzbehörde Republik Österreich, 2019)

Eine Vorlage für ein Verarbeitungsverzeichnis wird in den nächsten Kapiteln dargelegt und näher behandelt.

5.3.1 Wird eine Bildverarbeitung durchgeführt?

Das Datenschutzanpassungsgesetz 2018 enthält einen eigenen Abschnitt zum Thema Bildverarbeitung. Das DSG definiert jegliche Bildverarbeitung wie folgt:

> *Eine Bildaufnahme [...] bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen.*
>
> *(Österreichisches Parlament, 2017, S. 15)*

Alle Bild- und Tonaufnahmen in Verbindung mit Videoaufzeichnungen des privaten Bereichs fallen unter diese Regelung. Die Bildaufnahme ist unter den folgenden Voraussetzungen zulässig:

- Sie ist für ein lebenswichtiges Interesse der betroffenen Person notwendig;
- Die betroffene Person hat die Verarbeitung ihrer personenbezogenen Daten ausdrücklich bewilligt;
- Die Bildaufnahme wurde durch gesetzliche Bestimmungen erlaubt oder angeordnet;
- Die Bildaufnahme dient dem vorbeugenden Schutz von Personen oder Sachen, die sich auf Liegenschaften befinden, die nur vom Verantwortlichen verwendet werden und die Aufnahme reicht räumlich nicht über die Grenzen der Liegenschaft hinaus;
- Die Bildaufnahme dient dem vorbeugenden Schutz von Personen oder Sachen an einem für die Öffentlichkeit zugänglichen Ort, an dem bereits eine Rechtsverletzung vorlag oder ein erhöhtes Gefahrenpotential durch die Natur des Ortes vorliegt;
- Es besteht ein privates Dokumentationsinteresse, dass nicht auf die Erfassung unbeteiligter Personen oder Objekte, die eine solche Person identifizierbar machen, abzielt.

  (Wirtschaftskammer Österreich, 2018d)

Wird eine Bildaufnahme durchgeführt, so müssen geeignete Datensicherheitsmaßnahmen ergriffen werden. Eine nachträgliche Veränderung der Bildaufnahme durch Unbefugte muss ausgeschlossen werden. Jeder Verarbeitungsvorgang unterliegt einer Protokollierungspflicht (außer bei Echtzeitüberwachungen). Personenbezogene Daten, die nicht für den Zweck benötigt werden, für den sie erhoben wurden und die keiner gesetzlichen Aufbewahrungspflicht unterliegen, sollten gelöscht werden. Für Bildaufnahmen gilt die Kennzeichnungspflicht, es sei denn sie dienen der verdeckten Ermittlung oder die betroffene Person wurde bereits über die Umstände informiert (Wirtschaftskammer Österreich, 2018d).

5.3.2 Wird Profiling angewendet?

Profiling ist jede Art der automatisierten Verarbeitung von personenbezogenen Daten, die dazu genutzt wird bestimmte Eigenschaften einer natürlichen Person zu bewerten um die folgenden

Aspekte im Zusammenhang mit Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren oder vorherzusagen. Für Profiling gelten besondere Regeln, wenn damit die automatische Generierung von Einzelentscheidungen verbunden ist (Wirtschaftskammer Österreich, 2018b).

5.4 Überprüfung von Bestimmungen und Verträgen

Im Zuge der Ist-Analyse sollten auch bestehende Bedingungen und Verträge auf deren Inhalt hin überprüft werden. Wurde beispielsweise in den AGBs die Verarbeitung von personenbezogenen Daten behandelt, so müssen diese gegebenenfalls angepasst werden oder separat erfolgen. Darunter fallen unter anderem die Folgenden:

- Die Allgemeinen Geschäftsbedingungen (AGB)
- Datenschutzerklärungen
- Impressum
- Laufende Verträge
- Website-Einstellungen

(Wirtschaftskammer Österreich, 2018e)

5.4.1 Werden Dienste an Kinder angeboten?

In der DSGVO wird die Altersgrenze von 16 Jahren für die Rechtmäßigkeit einer Einwilligungsbestätigung bei der Nutzung von Informationsdiensten festgelegt. Den Mitgliedsstaaten steht jedoch offen eine niedrigere Altersgrenze anzusetzen, solange diese nicht das vollendete 13. Lebensjahr unterschreitet. Im österreichischen DSG wird die Altersgrenze mit vollendetem 14. Lebensjahr festgesetzt (Wirtschaftskammer Österreich, 2018b).

5.4.2 Arbeitnehmerschutz

Die aktuellen Dienstverträge, Betriebsvereinbarungen, Dienstordnungen oder ähnliche mitarbeiterbezogene Verträge sollten ebenfalls überprüft werden. Falls vorhanden, wäre eine rechtzeitige Kommunikation bzw. Abstimmung mit dem Betriebsrat des Unternehmens durchzuführen (Wirtschaftskammer Österreich, 2018e).

Im Rahmen der Experteninterviews wurde deutlich, dass die personenbezogenen Daten der Angestellten ein wichtiges Thema im Bereich des Datenschutzes sind, jedoch der Fokus primär auf die personenbezogenen Daten der Kunden bzw. der verarbeiteten Daten des Geschäftsprozesses gelegt werden sollte.

5.4.3 Datenverarbeitungszweck und Beschreibung

Es sollte ebenfalls angeführt werden, welchen Zweck die eigentliche Datenverarbeitung verfolgt und welche personenbezogenen Daten notwendig sind um diesen Zweck zu erfüllen. Eine kurze Beschreibung des Datenverarbeitungszwecks und die Begründung, weshalb die Daten für die Erfüllung dieses Zwecks notwendig sind, sollte also ebenfalls für das Verarbeitungsverzeichnis vorbereitet werden.

5.4.4 Datenverkehr mit dem EU-Ausland

Innerhalb der Europäischen Union wird durch die DSGVO ein einheitliches Datenschutzniveau sichergestellt. Die Datenübermittlung an Drittländer oder internationale Organisationen ist nur unter bestimmten Voraussetzungen rechtlich zulässig.

Zunächst sollte überprüft werden, ob gegenwärtig personenbezogene Daten an Drittländer oder an internationale Organisationen übertragen werden. Falls Daten übertragen werden oder demnächst eine Datenübermittlung geplant ist, muss eine der folgenden Voraussetzungen gegeben sein, damit die Übermittlung rechtmäßig ist:

- Für das Drittland liegt ein Angemessenheitsbeschluss der Kommission vor. Dies betrifft derzeit Andorra, Argentinien, Färöer-Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay, Japan sowie USA durch das Privacy Shield;
- Es liegen geeignete Garantien vor. Dazu gehören verbindliche Datenschutzvorschriften durch die zuständige Aufsichtsbehörde, Standarddatenschutzklauseln von der Kommission oder von einer Aufsichtsbehörde oder genehmigte Verhaltensregeln bzw. genehmigte Zertifizierungsmechanismen zusammen mit geeigneten Garantien des Verantwortlichen oder des Auftragsverarbeiters in dem jeweiligen Drittland;
- Vertragsklauseln mit geeigneten Garantien zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Empfänger bzw. Verantwortlichen oder Auftragsverarbeiter in dem Drittland.

  (Wirtschaftskammer Österreich, 2019d)

In der DSGVO werden einige Ausnahmen für spezielle Fälle, in denen die Datenübermittlung dennoch gültig ist, angeführt. Darunter fällt beispielsweise eine ausdrückliche Einwilligung des Betroffenen (nach Informierung über die Risiken der Übermittlung) oder wenn die Übermittlung notwendig ist zur Geltendmachung, Ausübung oder Verteilung von Rechtsansprüchen (Wirtschaftskammer Österreich, 2019d).

5.5 Auftragsverarbeiter

Mit der DSGVO Einführung wurde der Begriff „datenschutzrechtlicher Dienstleister“ in „Auftragsverarbeiter“ umbenannt. Als Auftragsverarbeiter gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die im Auftrag des Verantwortlichen

personenbezogene Daten verarbeitet. Hierunter fallen unter anderem Cloud-Dienstanbieter und IT-Datenwartungsanbieter (Wirtschaftskammer Österreich, 2018l).

Das Auftragsverarbeitungsverhältnis ist nicht mit einem zivilrechtlichen Auftrag gleichzusetzen. Werden Daten weitergegeben um einen eigentlichen Auftrag durchzuführen, ist dies nicht als Auftragsverarbeitung zu werten (Wirtschaftskammer Österreich, 2018l).

Beispiel: Es wird Name und Anschrift benötigt um eine Reparatur von einer Handwerksfirma durchführen zu lassen (Wirtschaftskammer Österreich, 2018l).

5.6 Die Auftragsverarbeitungsvereinbarung

Der Verantwortliche wählt nur Auftragsverarbeiter aus, welche garantieren können, dass geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten vorhanden sind. Der Datenverarbeitung durch einen Auftragsverarbeiter liegt ein Vertrag zu Grunde. Der Vertrag wird schriftlich bzw. elektronisch abgeschlossen und kann auf Standardklauseln beruhen (Wirtschaftskammer Österreich, 2018l).

Eine Auftragsverarbeitung umfasst die folgenden Punkte:

- Kontaktinformationen des Verantwortlichen
- Kontaktinformationen des Auftragsverarbeiters
- Der Gegenstand der Vereinbarung, besteht aus:
    - Einer möglichst detaillierten Beschreibung des Auftrags inklusive der Art und des Zwecks der Verarbeitung
    - Falls vorhanden einem Rahmenvertrag, einem Werkvertrag oder einer Leistungsvereinbarung
    - Einer Auflistung der verarbeiteten Datenkategorien
    - Einer Auflistung der betroffenen Personenkategorien
- Die Angabe der Dauer der Vereinbarung (einmalig, befristet oder unbefristet)
- Die Angabe der Pflichten des Auftragsnehmers. Insgesamt werden hier neun Pflichten des Auftragsnehmers aufgelistet und erläutert
- Die Angabe des Durchführungsort der Datenverarbeitung
- Der Zulässigkeit der Hinzuziehung von Sub-Auftragsverarbeitern (Verbot, Zulässig für bestimmte Sub-Auftragsverarbeiter oder generell Zulässig)
- Der Unterschrift des Auftraggebers inkl. dem aktuellen Datum
- Der Unterschrift des Auftragnehmers inkl. dem aktuellen Datum

  (Wirtschaftskammer Österreich, 2018k)

Des Weiteren werden Anlagen über getroffene technische und organisatorische Maßnahmen angefügt. Diese umfassen die Datenschutzkategorien Vertraulichkeit, Datenintegrität,

Verfügbarkeit, Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Wirtschaftskammer Österreich, 2018k).

Den Meinungen in den Experteninterviews entsprechend, sollte eine Standardisierung der Auftragsverarbeitungsvereinbarungen angestrebt werden. Mittels Standardvorlagen können solche Auftragsverarbeitungsvereinbarungen schnell eingefordert und überprüft werden.

5.7 Identifikation technischer und organisatorischer Maßnahmen

Um die Sicherheit bei der Verarbeitung von personenbezogenen Daten zu gewährleisten, müssen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen bieten. Diese Maßnahmen müssen unter Berücksichtigung verschiedener Aspekte angemessen sein.

Bevor Maßnahmen geplant oder umgesetzt werden, sollte zunächst die Ist-Situation erhoben werden. Im Verarbeitungsverzeichnis werden ebenfalls die technischen und organisatorischen Maßnahmen für den Verarbeitungszweck angeführt. Es bietet sich jedoch an, diese und alle weiteren Maßnahmen in einer eigenen Liste vorab festzuhalten. Welche Maßnahmen für ein dem Risiko angemessenes Schutzniveau benötigt werden, ergibt sich sodann aus der Datenschutz-Folgenabschätzung. In Kapitel sechs werden die technischen und organisatorischen Maßnahmen detaillierter betrachtet (Wirtschaftskammer Österreich, 2018f).

Die Experteninterviews führten zu dem Ergebnis, dass in den meisten Unternehmen auf externe Ressourcen bzw. externes Fachwissen zur optimalen Auswahl bzw. Umsetzung der DSGVO TOMs zurückgegriffen wurde. Gründe für die Heranziehung externer Quellen stellen vor allem die anfallenden Kosten für die interne Weiterbildung bzw. Schulung der Angestellten wie auch das von den externen Experten eingebrachte angewandte Fachwissen aus abgeschlossenen Projekten anderer Unternehmen dar.

5.8 Pflichten und Betroffenenrechte

Die DSGVO bringt einige Pflichten für den Verantwortlichen bzw. den Auftragsverarbeiter und Rechte für die betroffenen Personen mit sich. Die folgenden rechtlichen Aspekte sollten daraufhin geprüft werden, inwieweit sie bereits teilweise oder vollständig erfüllt sind.

5.8.1 Die Rechtmäßigkeit und Transparenz

Zu prüfen ist, ob die Verarbeitung von personenbezogenen Daten auf rechtmäßige Weise und in einer für die betroffenen Personen leicht nachvollziehbaren Art und Weise durchgeführt wird. Informationen und Mitteilungen müssen für die betroffenen Personen leicht zugänglich und in einer einfachen Sprache verfasst sein. Dies gilt besonders für die Identität des Verantwortlichen, die Zwecke der Datenverarbeitung und die Art der Daten, welche von der betroffenen Person

verarbeitet werden. Die Transparenz während des Verarbeitungsvorgangs soll für die betroffenen Personen somit gegeben sein (Wirtschaftskammer Österreich, 2018i).

5.8.2 Die Einwilligung zur Verarbeitung

Ob eine Einwilligung notwendig ist, hängt von mehreren Rechtsgrundlagen ab. Bevor eine Einwilligung eingeholt wird, sollte zunächst geprüft werden, ob eine solche angesichts einer Rechtsgrundlage notwendig ist und daher bereits vorliegt. Ist keine Rechtsgrundlage vorhanden, dann muss von der betroffenen Person eine Einwilligung eingeholt werden. Eine Einwilligung ist eine freiwillige, unmissverständlich abgegebene Willenserklärung durch welche die betroffene Person eindeutig zu verstehen gibt, dass sie mit der Verarbeitung, der sie betreffenden personenbezogenen Daten in Bezug auf einen speziellen Zweck einverstanden ist. Eine Einwilligung muss schriftlich, mündlich oder elektronisch (durch aktives Anklicken) kundgetan werden. Bloßes Schweigen oder ein bereits ausgefülltes Zustimmen-Häkchen ist nicht zulässig. Besonders bei der Verarbeitung von sensiblen Daten muss eine ausdrückliche Einwilligungserklärung vorliegen (Wirtschaftskammer Österreich, 2018h).

In den AGBs können Informationen zur Einwilligung eingebettet werden. Die Einwilligungserklärung muss sich von den anderen Sachverhalten klar unterscheiden. Sind bereits Einwilligungserklärungen vor Inkrafttreten der DSGVO vorhanden, so muss diesen nicht erneut zugestimmt werden, sofern sie der neuen Rechtslage entsprechen (Wirtschaftskammer Österreich, 2018h).

5.8.3 Wird die Informationspflicht erfüllt?

Nach der DSGVO muss der Verantwortliche gewisse Informationen über die Datenverarbeitung der betroffenen Person zur Verfügung stellen. Es sollte überprüft werden, ob das Unternehmen bereits die Informationspflichten erfüllt hat oder darauf vorbereitet ist, auf etwaige Anfragen innerhalb der vorgeschriebenen Frist (spätestens ein Monat) zu reagieren. Die Informationen und alle Mitteilungen müssen in einer präzisen, transparenten, verständlichen, sprachlich einfach zu verstehenden und leicht zugänglichen Form übermittelt werden (Wirtschaftskammer Österreich, 2018j).

In den Experteninterviews wurde von allen Experten erwähnt, dass in ihrem Unternehmen spezifische Prozesse zur Erfüllung der Informations- und Auskunftspflicht entwickelt und dementsprechend zuständige Personen bzw. Abteilungen definiert wurden. Diese Prozesse wurden bereits getestet und auch im Echtbetrieb angewandt.

5.8.4 Dokumentationspflicht und Verarbeitungsverzeichnis

Die Pflicht ein Datenverarbeitungsverzeichnis zu führen, betrifft den Verantwortlichen sowie den Auftragsverarbeiter. Jedoch ist der Umfang für den Auftragsverarbeiter nicht so hoch wie für den Verantwortlichen. Vom Verantwortlichen muss ein schriftliches Verzeichnis mit sämtlichen personenbezogenen Datenverarbeitungstätigkeiten, die in seinen Zuständigkeitsbereich fallen,

geführt werden. Der Verantwortliche, jeder Auftragsverarbeiter sowie deren Vertreter müssen bei der Pflichterfüllung mit der Aufsichtsbehörde zusammenarbeiten. Das Verarbeitungsverzeichnis soll der Aufsichtsbehörde ermöglichen die Verarbeitungsvorgänge zu kontrollieren (Wirtschaftskammer Österreich, 2018g).

Ein Verarbeitungsverzeichnis könnte wie in der folgenden Abbildung dargestellt aussehen:

Verarbeitungsverzeichnis nach Artikel 30 Abs. 1 DSGVO

Name und Kontaktdaten des Verantwortlichen			
Name	Anschrift	E-Mail Adresse	Tel.Nr

Name und Kontaktdaten des Datenschutzbeauftragen(falls vorhanden)			
Name	Anschrift	E-Mail Adresse	Tel.Nr

Name und Kontaktdaten des Vertreters des Verantwortlichen(falls vorhanden)			
Name	Anschrift	E-Mail Adresse	Tel.Nr

Verfahrens-name	Zweck der Verarbeitung und Beschreibung	Verantwort-licher	Kategorie der betroffenen Personen	Kategorie der personenbezogen en Daten	Empfängern in Drittländer u. internationalen Organisationen	Löschfrist u. Speicher-dauer	Technische u.organisatorische Maßnahmen

Abbildung 4: Beispiel eines Verarbeitungsverzeichnisses (Eigene Darstellung)

Die in der Abbildung enthaltenen Informationen muss ein gültiges Verarbeitungsverzeichnis als Mindeststandards aufweisen.

Bei Unternehmen unter 250 Mitarbeitern entfällt die Pflicht zur Führung eines Verarbeitungsverzeichnisses dann, wenn die Datenverarbeitung nur gelegentlich erfolgt, es keine sensiblen Daten oder strafrechtliche Verurteilungen beinhaltet oder wenn keine Risiken für die Rechte und Freiheiten der betroffenen Personen bestehen. Wenn ein Unternehmen eine Lohnverrechnung und/oder Kundendaten führt, wird ein Verarbeitungsverzeichnis benötigt, da die Verarbeitung in diesem Fall nicht nur gelegentlich erfolgt (Wirtschaftskammer Österreich, 2018g).

Wenn Verarbeitungsvorgänge bei der Ist-Analyse identifiziert werden, so sind diese auch gleich in ein Verarbeitungsverzeichnis aufzunehmen, sofern dies für den jeweiligen Verarbeitungsvorgang vorgeschrieben ist. Die fehlenden Informationen bzw. Maßnahmen können dann im späteren Verlauf nachgetragen werden.

Die Auswertung der Experteninterviews ergab, dass ähnlich wie bei der Erhebung von vorhanden personenbezogenen Daten auch hinsichtlich der Einführung eines Verarbeitungsverzeichnisses

eine bereichsübergreifende Vorgehensweise optimal ist. Hierbei füllen die zuständigen Personen das Verarbeitungsverzeichnis mit den jeweiligen Informationen aus ihrem Fachbereich.

5.8.5 Werden Betroffenenrechte erfüllt?

Nach der DSGVO haben Betroffene einige Rechte gegenüber dem Verantwortlichen. Vom Verantwortlichen ist dafür zu sorgen, dass alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form für die betroffenen Personen verfügbar sind. Die betroffenen Personen haben folgende Rechte:

- Das zuvor erwähnte Informationsrecht
- Das Auskunftsrecht
- Das Recht auf Berichtigung
- Das Recht auf Löschung bzw. das Recht des Vergessens
- Das Recht zur Verarbeitungseinschränkung
- Das Recht zur Datenübertragbarkeit
- Das Widerspruchsrecht

  (Wirtschaftskammer Österreich, 2018c)

Es sollte herausgefunden werden, inwieweit bereits Prozesse zur Erfüllung der Pflichten vorhanden sind und ob die definierten Fristen eingehalten werden. Ebenfalls ist relevant, ob zuständige Personen mit ausreichenden Befugnissen nominiert wurden, ob eine dedizierte Anlaufstelle existiert und ob etwaige Anfragen korrekt bearbeitet werden (Wirtschaftskammer Österreich, 2018c).

Die Experten bezeichneten in den Interviews eine einheitliche Vorgehensweise und eine ausgewiesene und speziell dafür zuständige Anlaufstelle als wichtigste Aspekte zur adäquaten Erfüllung der Betroffenenrechte. Die jeweiligen damit betrauten Unternehmensabteilungen werden diesbezüglich von einer zentralen Stelle über notwendige Tätigkeiten informiert und hinsichtlich ihrer Aufgaben instruiert.

5.9 Datenschutz-Folgenabschätzung

Seit Inkrafttreten der DSGVO ist der Verantwortliche nicht mehr zur Meldung der Datenverarbeitungsvorgänge an das Datenverarbeitungsregister verpflichtet. Stattdessen wird vom Verantwortlichen gefordert, die Evaluierung der Datenverarbeitungsvorgänge in Eigenregie umzusetzen. Mit der Datenschutzfolgeabschätzung sollen die Auswirkungen und Risiken der Datenverarbeitung analysiert, die Rechte und Freiheiten der betroffenen Person geachtet und die Folgen der vorgesehenen Datenverarbeitung für den Datenschutz erhoben werden. Dadurch sollen die benötigten technischen und organisatorischen Maßnahmen zur Abhilfe definiert werden (Wirtschaftskammer Österreich, 2019c).

5.9.1 Ist die Datenschutz-Folgenabschätzung notwendig?

Zunächst sollte geprüft werden, inwieweit die Durchführung einer Datenschutz-Folgenabschätzung überhaupt verpflichtend ist. Trifft eine der folgenden Voraussetzungen zu, ist eine Datenschutz-Folgenabschätzung laut DSGVO verpflichtend:

- Wenn Profiling zur Bewertung von personenbezogenen Aspekten herangezogen wird und die daraus resultierenden Entscheidungen Einfluss auf die Rechte der natürlichen Person haben oder sich auf ähnlich erhebliche Weise aus auswirken (Beispiel: Kreditvergabe);
- Wenn sensible Daten oder strafrechtliche Verurteilungen und Straftaten in umfangreicher Art und Weise verarbeitet werden;
- Wenn Überwachungsdaten von öffentlich zugänglichen Bereichen in umfangreicher und systematischer Art und Weise verarbeitet werden. Dies gilt insbesondere für Bild- und damit verbunden Akustikinformationen;
- Wenn Die Datenverarbeitung mittels neuartiger technischer oder organisatorischer Lösungen durchgeführt wird, welche eine Auswirkungsabschätzung erschweren. Dies gilt insbesondere für die Verarbeitung von biometrischen Informationen und den Einsatz von künstlicher Intelligenz;
- Wenn Datensätze von zwei oder mehreren Verarbeitungen, die für unterschiedliche Zwecke und/oder von verschiedenen Verantwortlichen durchgeführt wurden. Oder wenn Datensätze zusammengelegt bzw. abgeglichen wurden und wenn danach durch Algorithmen Entscheidungen getroffen werden, die eine betroffene Person in erheblicher Weise beeinträchtigen können;
- Wenn Die Verarbeitungstätigkeit in der Blacklist bzw. nicht in der Whitelist der Datenschutzbehörde angeführt wird.

  (Wirtschaftskammer Österreich, 2019b)

Die zuständige Datenschutzbehörde führt eine Blacklist über alle Verarbeitungstätigkeiten bei denen eine Datenschutz-Folgenabschätzung zwingend notwendig ist. Für Österreich ist die Blacklist in der „Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) - BGBl. II Nr. 278/2018“, erlassen worden. Diese umfasst detaillierte Informationen zu den oben genannten Aspekten (Wirtschaftskammer Österreich, 2019b).

Alternativ oder zusätzlich kann eine Whitelist veröffentlicht werden. Die Whitelist beinhaltet alle Verarbeitungstätigkeiten, bei denen keine Datenschutz-Folgenabschätzung vorgeschrieben ist. In Österreich trat am 25. Mai 2018 die „Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) - BGBl. II Nr. 108/2018“ in Kraft (Wirtschaftskammer Österreich, 2019b).

5.9.2 Inhalt einer Datenschutz-Folgenabschätzung

Nachdem erhoben wurde, ob eine Datenschutz-Folgenabschätzung für die jeweiligen Verarbeitungsprozesse notwendig ist, kann mit der Erstellung der Folgeabschätzung begonnen werden. Vom Datenschutzgremium wurden einige Kriterien empfohlen, die zwar nicht verpflichtend sind, aber ein gutes Grundgerüst darstellen. Die Datenschutz-Folgenabschätzung sollte die folgenden Kriterien beinhalten:

- Eine systematische Beschreibung aller geplanten Verarbeitungsvorgänge. Dies umfasst die Art, den Umfang, die Umstände der Datenverarbeitung, die personenbezogenen Daten, die Empfänger, die Speicherfrist, eine funktionale Beschreibung der Verarbeitungsvorgänge, eine Beschreibung der Wirtschaftsgüter auf die sich die personenbezogenen Daten stützen und gegebenenfalls genehmigte Verhaltensregeln;
- Eine Beschreibung der Verarbeitungszwecke;
- Eine Bewertung über die Notwendigkeit bzw. Verhältnismäßigkeit der Datenverarbeitung. Die folgenden Überprüfungskriterien können zur Bewertung herangezogen werden:
    - Die Datenverarbeitung erfolgt für eindeutige legitime Zwecke;
    - Eine Rechtmäßigkeitsgrundlage liegt vor;
    - Die Datenverarbeitung ist für den Zweck angemessen sowie auf das nötige Maß beschränkt;
    - Es sind Maßnahmen für die Erfüllung der Betroffenenrechte vorhanden;
    - Die Auftragsverarbeiter sind zuverlässig oder werden durch einen Vertrag verpflichtet;
    - Es wird eine Konsultation der Datenschutzbehörde benötigt, da trotz ergriffener Maßnahmen weiterhin ein hohes Risiko besteht.
- Risikoidentifizierung und -bewertung für die Rechte und Freiheiten der betroffenen Person;
- Die gewählten Abhilfemaßnahmen zur Reduzierung bzw. Bewältigung der Risiken;
- Die Empfehlungen des Datenschutzbeauftragten und die dazu gehörenden Entscheidungen;
- Der Standpunkt der Betroffenen oder deren Vertreter (falls vorhanden);
- Falls die Entscheidung des Verantwortlichen vom Standpunkt der Betroffenen oder deren Vertreter abweicht, muss ein Grund angeführt werden.

  (Wirtschaftskammer Österreich, 2019c)

5.9.3 Risikoanalyse und Bewertung

Der erste Schritt der Risikobewertung bzw. der Risikoanalyse ist die Identifikation der möglichen Risiken. Die Risiken werden anhand der folgenden vier Schutzziele gemessen und bewertet.

Datenverfügbarkeit: Besteht ein Risiko durch die geplante Datenverarbeitung für die Erfüllung der Betroffenenrechte.

Integrität und Vertraulichkeit: Besteht ein Risiko durch die geplante Datenverarbeitung hinsichtlich des Schutzes der Privatsphäre des Betroffenen und des Datengeheimnisses in Bezug auf unbeabsichtigten Verlust, Zerstörung oder Schädigung.

Zweckbindung: Bestehen Risiken für die Einhaltung des ursprünglichen Zwecks der Datenverarbeitung bzw. besteht die Gefahr, dass von dem eigentlich geplanten Verarbeitungszweck abgewichen wird.

Sonstige Datenschutzprinzipien: Besteht das Risiko, dass anderen Datenschutzgrundsätzen bei der Datenverarbeitung nicht nachgekommen wird. Darunter fallen beispielsweise Datenminimierung, Richtigkeit, Speicherbegrenzung, Rechtmäßigkeit, Transparenz oder das der Informationspflicht nicht nachgekommen werden kann.

(Wirtschaftskammer Österreich, 2019b)

Nachdem die potentiellen Risiken identifiziert wurden, kann eine Risikoanalyse durchgeführt werden. Zunächst werden Informationen zu den Bedrohungen festgehalten. Darunter fallen Kriterien wie: Was könnten die Motive und Ursachen der Bedrohung sein oder welche Ziele werden verfolgt.

Danach werden die Eintrittswahrscheinlichkeit und die potentielle Auswirkung auf die betroffene Person, unter Berücksichtigung der Art, des Umfangs, der Umstände, der Verarbeitungszwecke und der Ursache des Risikos bewertet. Zur leichteren Bewertung kann eine Risikobewertungsmatrix herangezogen werden (Wirtschaftskammer Österreich, 2019b).

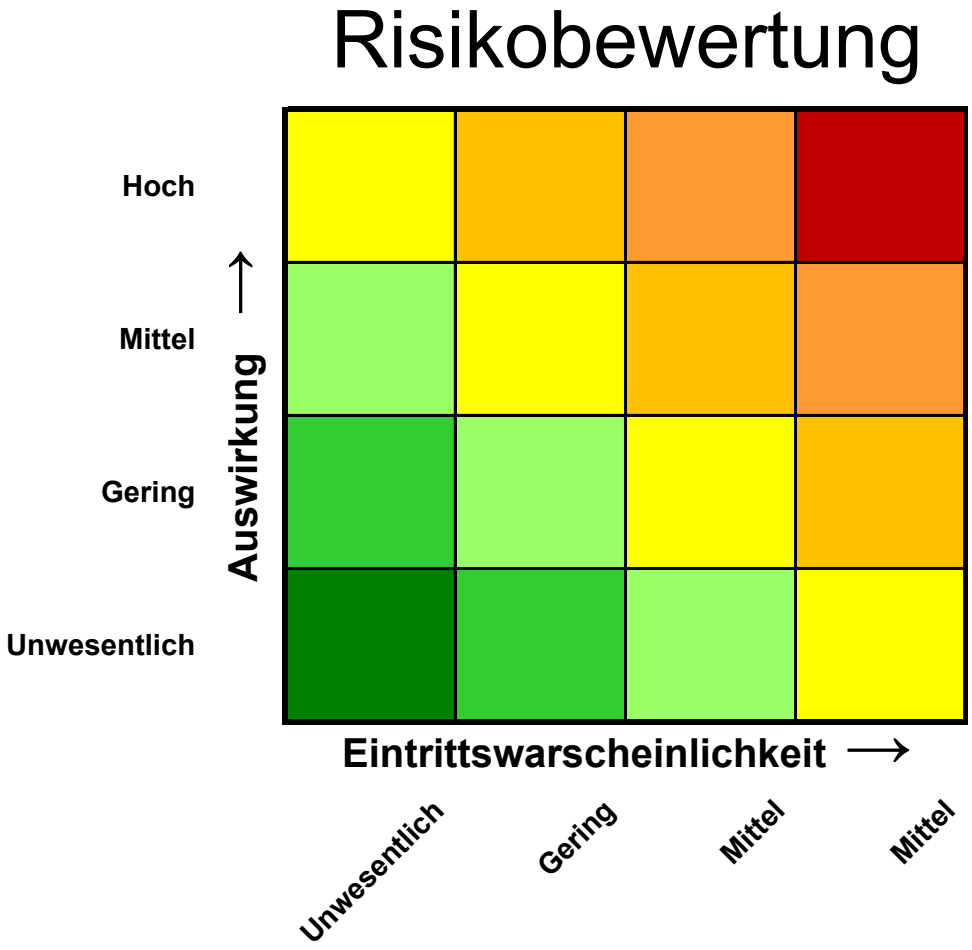

Abbildung 5: Risikobewertungsmatrix (in Anlehnung an Bayerisches Landesamt für Datenschutzaufsicht, 2017)

Die Folgen für die Betroffenenrechte einer Risikoverwirklichung können beispielsweise sein:

- *physischer, materieller und immaterieller Schaden beim Betroffenen*
- *Verlust der Kontrolle über die Daten*
- *Einschränkung bei der Erfüllung der Betroffenenrechte*
- *Diskriminierung*
- *Identitätsdiebstahl oder -betrug*
- *finanzielle Verluste*
- *unbefugte Aufhebung der Pseudonymisierung*
- *Rufschädigung*
- *Verlust der Vertraulichkeit (der Privatsphäre)*
- *erhebliche wirtschaftliche oder gesellschaftliche Nachteile*
- *(Wirtschaftskammer Österreich, 2019b)*

5.9.4 Maßnahme zur Abhilfe

Sobald die Risiken identifiziert und bewertet wurden, kann mit der Erhebung der bisher getroffenen Abhilfemaßnahmen begonnen werden. Hierbei wird die Ist-Situation der Maßnahmen zur Minimierung oder Abschaffung der Risiken betrachtet.

Im Anschluss wird der Soll-Ist-Vergleich durchgeführt und ein Maßnahmenplan zur Gewährleistung der Schutzziele definiert. Durch die zuvor erhobenen Prüfschritte können etwaige „Lücken" hinsichtlich der Risikominimierung und -behebung identifiziert werden. Ein Maßnahmenplan kann sich beispielsweise aus den folgenden Bereichen zusammensetzen:

- Personelle Maßnahmen
- Technische und organisatorische Maßnahmen
- Computersicherheit und Virenschutz
- Netzwerksicherheit
- Datensicherung und Notfallvorsorge
- Bauliche und infrastrukturelle Maßnahmen

  (Wirtschaftskammer Österreich, 2019b)

Die möglichen Maßnahmen werden in Kapitel sechs näher behandelt.

5.9.5 Konsultation mit der Aufsichtsbehörde

Sollte ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen durch die Datenschutz-Folgenabschätzung identifiziert werden und sollte der Verantwortliche keine Maßnahmen zur Risikominimierung treffen können, so muss der Verantwortliche die Datenschutzbehörde konsultieren. Innerhalb von acht Wochen wird dem Verantwortlichen oder dem Auftragsverarbeiter eine schriftliche Empfehlung von der zuständigen Datenschutzbehörde zugesandt. Diese Frist kann um weitere sechs Wochen verlängert werden, wenn der beabsichtigte Datenverarbeitungsvorgang eine hohe Komplexität aufweist.

Die folgenden Informationen sind der Konsultationsanfrage beizulegen:

- Angaben über die Zuständigkeiten des Verantwortlichen sowie der gemeinsam Verantwortlichen und allen an dem Datenverarbeitungsvorgang beteiligten Auftragsverarbeitern, insbesondere bei der Verarbeitung innerhalb einer Unternehmensgruppe;
- Beabsichtigte Verarbeitungszwecke und -mittel;
- Die vorgesehenen Maßnahmen und Garantien zum Schutz der Rechte der betroffenen Personen;
- Den Datenverarbeitungsvorgang betreffende Datenschutz-Folgenabschätzungen;
- Falls vorhanden: Die Kontaktdaten des Datenschutzbeauftragten;

- Falls vorhanden: Bereits angeforderte Informationen der Datenschutzbehörde.

(Wirtschaftskammer Österreich, 2019c)

6 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Sobald die Ist-Analyse der Verarbeitungssituation abgeschlossen ist, sollte unter anderem ein Verarbeitungsverzeichnis bestehen sowie eine Datenschutz-Folgenabschätzung vorliegen. In beiden Dokumenten sollten die bereits vorhandenen TOMs, zur Abhilfeschaffung aufgelistet sein. In Kapitel fünf wurde ebenfalls erwähnt, dass es sinnvoll ist alle vorhandenen TOMs zusätzlich in einer eigenen Liste festzuhalten. Anhand dieser Maßnahmenliste können die bereits getroffenen Maßnahmen leichter evaluiert und auf deren Aktualität bzw. Angemessenheit geprüft werden wie auch bei Anfragen von Angestellten, Kunden oder Geschäftspartnern schneller zur Verfügung stehen.

6.1 Datenschutz durch Technik und Voreinstellung

Um den Schutz von personenbezogenen Daten zu gewährleisten, müssen von dem Verantwortlichen und dem Auftragsverarbeiter die IT-Grundsätze „Datenschutz durch Technik (Privacy by Design)“ und „Datenschutzfreundliche Voreinstellungen (Privacy by Default)“ berücksichtigt sowie geeignete Strategien bzw. Maßnahmen definiert und umgesetzt werden (Wöhrl & Becker, 2018, S. 21).

6.1.1 Datenschutz durch Technik - Privacy by Design

Bei der Planung sowie der Datenverarbeitung selbst, müssen der Verantwortliche und die Auftragsverarbeiter dafür sorgen, dass geeignete technische und organisatorische Maßnahmen angewandt werden um ein dem Risiko entsprechendes Schutzniveau zu gewährleisten. Ein Beispiel hierfür ist Pseudonymisierung. Die gewählten Maßnahmen müssen den in Kapitel 6.3 erläuterten Datenschutzkriterien entsprechen (Wöhrl & Becker, 2018, S. 21).

6.1.2 Datenschutz durch Voreinstellung - Privacy by Default

Der Verantwortliche und die Auftragsverarbeiter müssen dafür sorgen, dass geeignete TOMs angewandt werden um sicherzustellen, dass bereits durch die Voreinstellungen nur personenbezogene Daten verarbeitet werden können, die für den jeweiligen Verarbeitungszweck notwendig sind. Derartige Maßnahmen müssen so gestaltet sein, dass personenbezogene Daten, nicht für andere natürliche Personen zugänglich sind (Wöhrl & Becker, 2018, S. 21).

6.2 Datenschutzgrundsätze

Besonders bei der Verarbeitung von personenbezogenen Daten müssen der Verantwortliche und die Auftragsverarbeiter Maßnahmen anwenden um die angeführten Datenschutzgrundsätze umzusetzen. In der DSGVO werden einige dieser Datenschutzgrundsätze wie z.B. Integrität,

Vertraulichkeit und Transparenz besonders betont. In den folgenden Unterkapiteln werden die wichtigsten Datenschutzgrundsätze näher erläutert.

6.2.1 Verhältnismäßigkeit

Die angewandten Maßnahmen sind dann als verhältnismäßig anzusehen, wenn sie für einen legitimen Zweck sowohl erforderlich, geeignet als auch angemessen sind. Bei der Umsetzung der Datenschutzmaßnahmen müssen sich die Unternehmen vor allem an diesem Prinzip orientieren (Loomans, Matz & Wiedemann, 2014, S. 9).

6.2.2 Datenminimierung und -vermeidung

Das Prinzip der Datenminimierung besagt, dass nur unbedingt notwendige personenbezogene Daten für den jeweiligen Zweck erhoben und verarbeitet werden. Dies kann dazu führen, dass auf personenbezogene Daten bei einigen Verfahren komplett verzichtet werden muss. Die Pseudonymisierung oder auch Anonymisierung der personenbezogenen Daten sind diesbezüglich die bevorzugten Strategien (Loomans, Matz & Wiedemann, 2014, S. 9).

6.2.3 Zweckbindung

Die personenbezogenen Daten dürfen nur für legitime, festgelegte und eindeutige Zwecke erhoben und auch nur für diese Zwecke verarbeitet werden. Bereits erhobene Daten dürfen nicht für andere als die ursprünglich vereinbarten verwendet werden. Ausnahmen hierbei sind die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche, historische oder statistische Zwecke (Robert Kaiser, 2014).

6.2.4 Transparenz

Verarbeitungsvorgänge, die auf personenbezogene Daten zurückgreifen, müssen für die betroffene Person transparent verarbeitet werden. Die Datenerarbeitung muss für die jeweilige Person nachvollziehbar gestaltet sein damit sie ihre Rechte in Bezug auf die jeweiligen persönlichen Daten in Anspruch nehmen kann (Loomans, Matz & Wiedemann, 2014, S. 10).

6.2.5 Verfügbarkeit

Die Verfügbarkeit von personenbezogenen Daten und generell von IT-Systemen ist nicht nur von der DSGVO gefordert, sondern auch ein wichtiger Faktor für Geschäftsprozesse. Um die Verfügbarkeit zu steigern, muss zunächst identifiziert werden ob bzw. wo sich Single-Point-of-Failure befinden, die bei Ausfällen bzw. Fehlern den Geschäftsprozess unterbrechen können. Danach müssen geeignete technische oder organisatorische Maßnahmen gesetzt werden um die Risiken zu minimieren bzw. zu beheben. Hierzu gehören unter anderem: das Schaffen von

Redundanzen, Hot-Standby, Cold-Standby, die Behebung von Softwaremängel, die Vermeidung von Fehlbedienung und -administration (Wöhrl & Becker, 2018, S. 18).

6.2.6 Integrität

Unter Integrität von personenbezogenen Daten versteht man, dass diese vor Veränderungen geschützt werden. Die Integrität kann durch fehlerhafte Soft- und Hardware oder durch einen Angriff wie z.B. die Verfälschung von Nachrichten an E-Mailempfänger verletzt werden. Eine technische Maßnahme gegen Integritätsverletzungen kann beispielsweise die Verwendung von digitalen Signaturen sein. Die Protokollierung von Zugriffen auf personenbezogene Daten ist ein Beispiel für eine organisatorische Maßnahme (Wöhrl & Becker, 2018, S. 18).

6.2.7 Vertraulichkeit

Nur berechtigte Personen dürfen Zugriff auf personenbezogene Daten haben. Diese Personen müssen bezüglich des korrekten Umgangs mit personenbezogenen Daten geschult werden und diese Daten vertraulich behandeln. Eine gut gepflegte Zugriffsberechtigungskontrolle auf Datenstrukturen sorgt dafür, dass nur Personen Zugriff auf Daten haben, die sie für ihre Tätigkeiten bzw. das jeweilige Projekt benötigen (Wöhrl & Becker, 2018, S. 18).

6.2.8 Belastbarkeit

Der Ausfall einzelner oder mehrerer Services wegen Überlastung kann zum Zusammenbruch ganzer Systeme und eventuell auch zum Stillstand der Geschäftsprozesse führen. Die Belastbarkeit steht in einem engen Zusammenhang mit der Verfügbarkeit. Technische Maßnahmen wie Hot-Standby oder Loadbalancing können hier die Auslastung auf einzelne Systeme verringern und Redundanzen schaffen. Um kritischen Situationen vorzubeugen sollte eine durchdachte Monitoring-Lösung zur Erkennung von potentiellen Ressourcenengpässen eingeführt werden (Wöhrl & Becker, 2018, S. 19).

6.2.9 Wiederherstellbarkeit

Die Wiederherstellungsstrategie bzw. Backupstrategie eines Unternehmens hängt von der Bedeutung der IT-Systeme und deren Verfügbarkeit für die Firmenprozesse ab. Um eine geeignete Strategie zu entwickeln, sollten zunächst die folgenden vier Fragen beantwortet werden.

- Wie lange dürfen IT-Systeme bzw. ein Teil des Systems ausfallen?
- Wird Ersatzhardware für die Fehlerbehebung benötigt?
- In welchem Zeitraum können Ersatzsysteme beschafft werden?
- Wie lange dauert eine Re-Installation, Wiederherstellung und/oder eine erneute Inbetriebnahme?

Besonders bei der Wiederherstellung sind Dokumentationen für die korrekte und aktuelle Vorgehensweise wichtig. Es muss gewährleistet sein, dass Datenbanken, Server oder Services auch bei Ausfall eines Mitarbeiters wiederhergestellt und in Betrieb genommen werden können. Die folgenden Themen sollten in der Backupstrategie zumindest bedacht werden:

Backuptypen

Welche Backuptypen von einem Unternehmen verwendet werden bzw. wie diese miteinander abgestimmt sind, hängt von mehreren Faktoren ab. In der Praxis werden meist vollständige, inkrementelle und in seltenen Fällen differenzielle Backups genutzt.

- Vollständige Backups bilden ein gesamtes System bzw. Datenstrukturen ab;
- Inkrementelle Backups sichern nur die Datenänderungen seit der letzten inkrementellen oder vollständigen Sicherung (falls kein inkrementelles Backup dazwischen war);
- Differenzielle Backups speichern alle Datenänderungen seit der letzten vollständigen Sicherung.

  (Wöhrl & Becker, 2018, S. 20)

Backupzeiten

An welchen Tagen und zu welchen Uhrzeiten gesichert wird, sollte ebenfalls in der Backupstrategie bedacht werden, denn Backups können Auswirkungen auf Systemressourcen bzw. Storage-Zugriffszeiten mit sich bringen (Wöhrl & Becker, 2018, S. 20).

Backupsicherheit

Es muss sichergestellt sein, dass Backups nicht auf firmenfremden Systemen wiederhergestellt und somit Daten durch Diebstahl von Backupmedien veröffentlicht werden können. Backupverschlüsselungen oder Aufbewahrung der Medien in einem abgeschlossenen und gesicherten Bereich können diesbezüglich als Maßnahmen betrachtet werden (Wöhrl & Becker, 2018, S. 20).

6.2.10 Richtigkeit

Es muss gewährleistet sein, dass personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem aktuellen Stand sind. Durch den Einsatz von geeigneten Maßnahmen müssen fehlerhafte bzw. falsche personenbezogene Daten gelöscht bzw. berichtigt werden (Wirtschaftskammer Österreich, 2018i).

6.3 Auswahl der Datensicherheitsmaßnahmen

In Paragraph 54 des österreichischen Datenschutz Anpassungsgesetzes 2018 werden die einzelnen Datensicherheitsmaßnahmen behandelt. In diesem Kapitel werden die angeführten Maßnahmen näher erläutert und passende technische Lösungen aufgezeigt. Die

Maßnahmenwahl des Verantwortlichen oder des Auftragsverarbeiters muss unter Berücksichtigung der folgenden Datenschutzkriterien durchgeführt werden:

- Stand der Technik
- Implementierungskosten
- Verarbeitungsart, Verarbeitungsumfang, Verarbeitungszweck sowie Verarbeitungsumstände
- Eintrittswahrscheinlichkeit und schwere des Risikos

  (Österreichisches Parlament, 2017, S. 24–25)

6.3.1 Stand der Technik

Der Begriff „Stand der Technik“ wird sowohl in der DSGVO wie auch im DSG verwendet und nimmt Bezug auf die Entwicklung der Technik. Besonders im IT-Bereich findet eine fortlaufende Weiterentwicklung statt. Deshalb muss von den zuständigen Fachkräften innerhalb des Unternehmens oder durch externe Experten sichergestellt werden, dass sich die betriebsnotwendigen Technologien auf einem aktuellen Stand befinden. Besonders im Bereich der IT-Security ist auf die Aktualität zu achten, da auch potentielle Angreifer auf neueste Techniken zurückgreifen (Wöhrl & Becker, 2018, S. 17).

6.3.2 Implementierungskosten

Mit der Umsetzung von Datensicherheitsmaßnahmen sind im Normallfall Investitionskosten zur Umsetzung dieser verbunden. Die getätigten Investitionen müssen nicht direkt monetärer Natur sein, sondern können sich auch aus internen Ressourcenaufwendungen oder externen Beratungs- und Implementierungskosten zusammensetzen. In den meisten Fällen gilt: Je höher die Risiken der Datenverarbeitung, desto höher können die Implementierungskosten zur Abhilfeschaffung bzw. Reduzierung ausfallen. Deshalb kann es auch sein, dass eine mögliche Maßnahme nicht implementiert wird, da ihre Kosten den Nutzen übersteigen.

6.3.3 Verarbeitungskriterien

Jede Verarbeitung von personenbezogenen Daten kann anhand von Verarbeitungskriterien klassifiziert werden. In der DSGVO werden die folgenden Verarbeitungskriterien genannt:

Verarbeitungsart
Auf welche Art bzw. durch welche Technologie werden die Daten verarbeitet.

Verarbeitungsumfang
Welche Menge an Daten wird verarbeitet.

Verarbeitungszweck
Welchem Zweck dient die ursprüngliche Datenverarbeitung.

Verarbeitungsumstände
Unter welchen Umständen wird die Datenverarbeitung durchgeführt.

6.3.4 Eintrittswahrscheinlichkeit und schwere des Risikos

Um geeignete Maßnahmen auswählen zu können, muss ebenfalls das etwaige Risiko für die personenbezogenen Daten der betroffenen Personen abgeschätzt werden. Aufgrund eines geringen Risikos kann daher von einer kostspieligen Abhilfemaßnahme abgesehen werden oder angesichts eines hohen Risikos müssen teurere Maßnahmen bzw. mehrere Maßnahmen vom Unternehmen umgesetzt werden, damit das Risikopotential minimiert wird. In Kapitel fünf wurde das Thema Risikobewertung und -analyse bereits näher erklärt.

6.4 Datensicherheitsmaßnahmen

Um die folgenden Schutzzwecke zu erreichen, werden mehrere mögliche Optionen vorgestellt. Es können zusätzlich weitere Maßnahmen, die hier nicht explizit angeführt sind, herangezogen werden um das jeweilige Risiko zu reduzieren bzw. zu beheben.

6.4.1 Zutrittskontrolle und Zugangsbeschränkung

In Verarbeitungsanlagen, die zur Verarbeitung von personenbezogenen Daten verwendet werden, sollte Unbefugten der Zutritt verwehrt werden. Um die Zugangskontrolle umzusetzen, gibt es eine Vielzahl an Optionen (Österreichisches Parlament, 2017, S. 25).
Zur Umsetzung der Zutrittskontrolle können sowohl bauliche, technische sowie organisatorische Maßnahmen herangezogen werden.

Beispiele für bauliche und/oder technische Maßnahmen:

- Der Serverraum ist nur mit Schlüssel oder Schlüsselkarte zu betreten - eventuell auch per biometrischer Identifikation wie Iris-Scans oder Fingerabdruck;
- Alarmanlage mit Meldungen an Polizei oder Sicherheitsfirmen;
- Videoüberwachungssysteme.

Beispiele für organisatorische Maßnahmen:

- Besuchern wird erst nach Identifikation durch einen Mitarbeiter der Zutritt gewährt;
- Besucher dürfen die Büro-Räumlichkeiten nur in Begleitung eines Angestellten betreten;
- Führung eines Besucherprotokolls. Ein Protokoll könnte Daten wie Name, Firma, Datum, Uhrzeit, Grund des Besuchs umfassen;
- Gedruckte Dokumente mit personenbezogenen Daten können in versperrten Stahlschränken bzw. Safes aufbewahrt werden.

  (Wöhrl & Becker, 2018, S. 44)

In einem der Experteninterviews wurden die Zutrittskontrollmaßnahmen explizit als ein wesentlicher Faktor für die Datensicherheit hervorgehoben. Der befragte Experte gab an, dass zunächst auf betrieblicher Ebene gar nicht darüber nachgedacht wurde, dass IT-Sicherheit schon bei der Zutrittskontrolle beginnt. Einfache Schlösser bzw. Schließsysteme wurden zu Beginn nicht als IT sicherheitsrelevante Problembereiche identifiziert.

6.4.2 Datenträgerkontrolle

Mit der Datenträgerkontrolle soll unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Datenträgern unterbunden werden (Österreichisches Parlament, 2017, S. 25).

Die personenbezogenen Daten bzw. alle anderen schützenswerten Ressourcen sollten auf einem durch Sicherheitsmaßnahmen geschützten Datenträger liegen. Dies umfasst physische und virtuelle Laufwerke in Client-Computern und Servern.

Beispiele für bauliche und/oder technische Maßnahmen:

- Die Speichermedien werden in einem geschlossenen Bereich bzw. Sicherheitsbereich wie beispielsweise einem Safe oder Stahlschränken aufbewahrt;
- Die Löschung bei Wiederverwendung von Laufwerken oder Speichermedien durch datenschutzgerechte Methoden.

Beispiele für organisatorische Maßnahmen:

- Benutzte Speichermedien und Geräte mit integrierten Datenträgern werden protokolliert entsorgt und mittels Methoden gelöscht bzw. zerstört, die eine Datenwiederherstellung unmöglich machen;
- Die Ausgabe von mobilen Speichermedien wird protokolliert;
- Die Weitergabe von personenbezogenen Daten wird protokolliert bzw. kontrolliert.

  (Wöhrl & Becker, 2018, S. 42)

6.4.3 Speicherkontrolle

Mit der Speicherkontrolle wird das unbefugte Eingeben, Lesen, Kopieren, Verändern oder Löschen von personenbezogenen Daten verstanden (Österreichisches Parlament, 2017, S. 25).

Nur befugte Personen dürfen auf personenbezogene Daten zugreifen und diese bearbeiten.

Beispiele für technische Maßnahmen:

- Benutzeridentifikation;
- Sperre des Clients (Arbeitsplatz bzw. Notebooks sind nach zehn Minuten inaktiv);
- Trennung von Produktions- und Administrationsbereich;
- Verarbeitungsanlagen vor unbefugtem Zugriff schützen;
- Personenbezogene Daten werden nur auf verschlüsselten Partitionen gespeichert.

Beispiel für organisatorische Maßnahmen:

- Durchdachtes Rechtemanagement.

  (Wöhrl & Becker, 2018, S. 43)

6.4.4 Benutzerkontrolle

Benutzerberechtigungen werden durch den Administrator nach dem „principle of least privilege (PoLP)" vergeben. Das heißt es werden lediglich die nötigen Zugriffs- bzw. Nutzungsberechtigungen an Anwender vergeben um deren Tätigkeiten nachzukommen. Es sollen dadurch nur Befugte auf Daten zugreifen können.

Beispiele für technische Maßnahmen:

- Firewalls
- Intrusion Protection/Detection Systeme;
- Benutzeridentifikation;
- Netzwerkabsicherung - network access control;
- Computerabsicherung.

Beispiele für organisatorische Maßnahmen:

- Protokollierung von Benutzeraktivitäten;
- Zutrittsberechtigungen von Benutzern festlegen;
- Kennwortrichtlinie;
- Clean-Desk Richtlinie.

  (Wöhrl & Becker, 2018, S. 41)

6.4.5 Zugriffskontrolle

Es muss gewährleistet sein, dass Benutzer ausschließlich Zugang zu den personenbezogenen Daten haben, die ihrer Zugangsberechtigung entspricht (Österreichisches Parlament, 2017, S. 25).

Dafür wird eine unternehmensweit angewendete Kennwortrichtlinie genutzt, die ausdrücklich und nachweislich an alle Mitarbeiter kommuniziert wird.

Beispiele für technische Maßnahmen:

- Angewendetes Berechtigungskonzept;
- Benutzeridentifikation;
- Sicherung der Schnittstellen;
- Verschlüsselung;

- Fremdgeräten keinen Netzwerkzugriff gewähren.

Beispiele für organisatorische Maßnahmen:

- Zugriffskontrolle verwalten und überprüfen;
- Zugriffe kontrollieren bzw. protokollieren;
- Maßnahmen zur Datenvernichtung protokollieren.

  (Wöhrl & Becker, 2018, S. 45)

6.4.6 Übertragungskontrolle

Es muss überprüfbar und feststellbar sein an welchen Stellen personenbezogene Daten mittels Datenübertragung übermittelt oder zur Verfügung gestellt wurden bzw. werden können (Österreichisches Parlament, 2017, S. 25).

Alle personenbezogenen Daten werden an Kunden bzw. Geschäftspartner nur mittels verschlüsselten Datenträgermedien übergeben, per SSL/TLS bzw. HTTPS (Websites) oder per VPN (Virtual Private Networks) übertragen.

Beispiele für technische Maßnahmen:

- Verwendung von Verschlüsselungsprogrammen;
- Verwendung von SSL/TLS Encryption und HTTPS auf Websites;
- Verwendung von VPN Verbindungen.

Beispiele für organisatorische Maßnahmen:

- Festlegen von berechtigten Sendern, Empfängern und Übertragungswegen;
- Protokollierung bzw. Logging von Datenübermittlungen;
- Erhebung der Übermittlungsmöglichkeiten.

  (Wöhrl & Becker, 2018, S. 40)

6.4.7 Eingabekontrolle

Es muss nachvollziehbar sein zu welchem Zeitpunkt und von wem personenbezogene Daten in ein Verarbeitungssystem eingegeben bzw. geändert oder gelöscht wurden (Österreichisches Parlament, 2017, S. 25).

Per Logfiles wird protokolliert welcher Benutzer zu welchem Zeitraum auf welchem Arbeitsplatz eingeloggt war und welche Daten bearbeitet wurden.

Beispiele für technische Maßnahmen:

- Benutzeridentifikation;

- Logging für Benutzeraktivitäten.

Beispiele für organisatorische Maßnahmen:

- Projektbezogene Benutzerberechtigungen festlegen;
- Eine sichere Protokollablage;
- Löschen der Logfiles bzw. Protokolle am Ende des Folgejahres der ursprünglichen Speicherung.

  (Wöhrl & Becker, 2018, S. 42)

6.4.8 Transportkontrolle

Es soll verhindert werden, dass personenbezogene Daten bei der Übermittlung und dem Transport von Datenträgern von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können (Österreichisches Parlament, 2017, S. 25).

Durch eine dienstliche Anweisung soll sichergestellt werden, dass auf keinen Fall personenbezogene Daten unverschlüsselt auf Datenträgern (USB-Sticks, externe Festplatten, Smartphones) gespeichert werden. Clientcomputer dürfen nur von befugten Personen benutzt werden.

Beispiele für technische Maßnahmen:

- Verschlüsselte Speicherung von personenbezogenen Daten auf den Datenträgern;
- Verschlüsselte Datenübermittlung über VPN verwenden.

Beispiele für organisatorische Maßnahmen:

- Anweisung zur Handhabung von Datenträgern;
- Protokollierung der Datenträgerübergabe (Ein- und Ausgang).

  (Wöhrl & Becker, 2018, S. 43)

6.4.9 Wiederherstellung

Es müssen Maßnahmen bereit stehen um eingesetzte Systeme im Störungsfall wiederherstellen zu können (Österreichisches Parlament, 2017, S. 25).

Das Unternehmen sollte eine Backup-Strategie verfolgen. Vom Administrator muss eine Sicherungskopie eingespielt oder ein kompletter Restore aller wichtigen Systeme und Ressourcen durchgeführt werden können. Ein Test des Restore-Prozesses sollte zwei Mal pro Jahr durchgeführt werden.

Beispiele für technische Maßnahmen:

- Tägliche, wöchentliche oder monatliche Backups aller wichtigen Systeme;

- Alle sechs Monate ein Backup aller Daten (Masterbackup) auf ein externes Medium sichern;
- Cold-Standby Backup der Server.

Beispiele für organisatorische Maßnahmen:

- Backup- und Wiederherstellungsstrategie bzw. -plan;
- Backup Strategie verfolgen (Vollsicherung, inkrementell und/oder differenziell);
- Fernzugriff per VPN zu allen Servern für Systemadministratoren ermöglichen;
- Serveradministratoren können jederzeit lokal in den Serverraum.

  (Wöhrl & Becker, 2018, S. 44)

In den Experteninterviews wurde das Potential der Risikominimierung durch die Backuplösung explizit hervorgehoben. Diesbezüglich ist darauf zu achten, dass eine angemessene Backupstrategie im Unternehmen auch gelebt wird und alle Teile der Strategie ordnungsgemäß umgesetzt werden. Die Funktionalität der Sicherungs- und Wiederherstellungsmaßnahmen sollte ebenfalls einer regelmäßigen Kontrolle unterliegen.

6.4.10 Zuverlässigkeit und Datenintegrität

Alle Funktionen des Systems müssen zur Verfügung stehen und etwaige auftretende Fehlfunktionen müssen gemeldet werden. Die gespeicherten personenbezogenen Daten dürfen durch einen Systemfehler bzw. eine Fehlfunktion nicht beschädigt oder gelöscht werden (Österreichisches Parlament, 2017, S. 25).

Um die Datenintegrität sicherzustellen, sollten Server- und Clientupdates entweder automatisch oder geplant (je nach Strategie) erfolgen. Programme bzw. Softwareprodukte sollten ebenfalls regelmäßig auf den neuesten Stand gebracht werden.

Beispiele für technische Maßnahmen:

- Tägliche, wöchentliche oder monatliche Backups aller wichtigen Systeme;
- Verwendung von Antivirensoftware;
- Software-Firewall (Client);
- Hardware-Firewall (LAN, WAN, Internet);
- E-Mail Spamfilter;
- USV (Unterbrechungsfreie Stromversorgung) im Serverbereich bzw. Notstromaggregate;
- Automatisches Reporting bei Ausfällen (SMS, Email);
- Redundante IT-Architecture (Alle Systeme existieren doppelt an unterschiedlichen Standorten).

Beispiele für organisatorische Maßnahmen:

- Backup- und Wiederherstellungsstrategie bzw. -plan;
- Systemüberwachung von Hard- und Software;
- Serveradministratoren können jederzeit lokal in den Serverraum.

(Wöhrl & Becker, 2018, S. 41)

6.5 Mitarbeiterdaten, Schulung und Sensibilisierung

Die besten IT-Sicherheitsmaßnahmen können ihren Zweck nur erfüllen, wenn die Angestellten der jeweiligen Unternehmen sicherheitsbewusst handeln und in der Lage sind die geforderten Maßnahmen anzuwenden. Werden Themen wie Kennwortrichtlinien, Clean-Desk-Policy oder Arbeitsplatzsperrung nicht unternehmensweit berücksichtigt, so besteht ein erhöhtes Sicherheitsrisiko.

6.5.1 Personenbezogene Daten der Mitarbeiter

Bereits beim Unternehmenseintritt bzw. beim Bewerbungsverfahren werden personenbezogene Daten verarbeitet. Diesbezüglich müssen geeignete technische und organisatorische Maßnahmen angewandt werden um die korrekte Handhabung dieser Daten zu gewährleisten. Diese Daten sind gleich zu behandeln wie andere personenbezogene Daten und müssen dem gleichen Schutzniveau unterliegen (Wöhrl & Becker, 2018, S. 24).

6.5.2 Anpassungen am Einstellungs- und Austrittsprozess

Sobald eine Person in das jeweilige Unternehmen eintritt, muss die Schulung von spezifischen Richtlinien bzw. Verhaltensweisen im IT-Bereich ein Teil des Einstellungsprozesses sein. Für das Unternehmen empfiehlt es sich zusätzlich eine Verpflichtungserklärung, zur Anwendung der Richtlinien von dem Angestellten unterzeichnen zu lassen. Unter anderem sollten die folgenden Themen behandelt werden:

- Benutzungsregeln von IT-Equipment (Laptops, PCs, Tablets oder Mobiltelefonen)
- Nutzungsregeln von Internet und E-Mail
- Verpflichtungserklärung zum Datengeheimnis
- Bring your own device (BYOD) Richtlinie (falls notwendig)

Die IT-Richtlinien für Angestellte sollten möglichst einfach bzw. verständlich formuliert werden (angepasst an die jeweilige Zielgruppe) und einen nicht zu großen Umfang haben (ca. 1-2 A4 Seiten). Prüfmethoden zur Einhaltung der Richtlinien und der Wirksamkeit von Schulungs- bzw. Weiterbildungsmaßnahmen sollten gegeben oder möglich sein.

Die Stellenbeschreibung der Angestellten muss alle sicherheitsrelevanten Aufgaben und Verantwortlichkeiten beinhalten. Dies gilt besonders für Angestellte mit erhöhtem Rechtsstatus bzw. weitreichenden Befugnissen wie Datenschutzbeauftragte, Projektverantwortliche und IT-Administratoren. IT-Administratoren haben meist umfassende Berechtigungen und sind daher in der Lage auf viele bzw. alle personenbezogenen Daten zuzugreifen, diese zu bearbeiten oder zu löschen. Daher ist bei Missbrauch von einer der genannten Personen von einem erhöhten Sicherheitsrisiko auszugehen (Wöhrl & Becker, 2018, S. 24).

Beim Unternehmensaustritt der Mitarbeiter sind ebenfalls einige Sicherheitsthemen zu beachten. Die folgenden Punkte sollten beim Austrittsprozess bedacht werden:

- Alle verwendeten IT-Ressourcen müssen zurückgegeben werden (außer bei speziellen Sondervereinbarungen);
- Die Zugriffsberechtigungen müssen entzogen, angepasst oder gelöscht werden;
- Wenn Konten von mehreren Anwendern verwendet werden, müssen die Passwörter dieser Konten geändert werden (dies gilt besonders für IT-Administratoren);
- Benutzerkonten ehemaliger Angestellter sollten nicht wiederverwendet werden;
- Der Austrittsprozess könnte durch die Verwendung einer Checkliste gestützt werden.

  (Wöhrl & Becker, 2018, S. 24)

Aus den Experteninterviews ging hervor, dass die Verarbeitung der personenbezogenen Daten von Kunden bzw. externen Personen priorisiert werden sollte, jedoch auch Mitarbeiterinformationen mit angemessenen Maßnahmen geschützt werden müssen.

6.5.3 Sicherheitsschulung und Sensibilisierung

Eine der wichtigsten Maßnahmen zur Steigerung der IT-Sicherheit ist die Erweiterung des Sicherheitswissens (Security Awareness) der Angestellten. Die Angestellten sollten über angemessene Kenntnisse im Umgang mit IT-Geräten bzw. Systemen und potentielle Gefahren sowie deren Gegenmaßnahmen, zumindest in ihrem eigenen Arbeitsbereich, verfügen. Zur Steigerung des Sicherheitswissens der Angestellten können verschiedene Maßnahmen herangezogen werden. Bestenfalls werden die Mitarbeiter motiviert, sich selbstständig Kenntnisse anzueignen und sich sicherheitsbewusst zu verhalten (Wöhrl & Becker, 2018, S. 24–25).

Mögliche Schulungsmethoden sind:

- Persönliche vor Ort Schulung durch Sicherheitsexperten bzw. externe Fachpersonen;
- Online Seminare mit Fokus auf Sicherheits- bzw. Datenschutzthemen;
- Schulungsvideos zu relevanten Datenschutzthemen;
- Online, App- bzw. Anwendungsgestützte Sicherheitsfragebögen inkl. Ausführungen zu den Fragen;
- Digitale oder analoge Schulungsunterlagen.

Die Auswertung der Experteninterviews führt zu der Schlussfolgerung, dass sich eine Kombination aus verschiedenen Maßnahmen am besten eignet um das Sicherheitsfachwissen der Angestellten zu steigern. Personen in Positionen mit sicherheitsrelevanten Tätigkeiten bzw. mit Verantwortung sollten wenn möglich an einer persönlichen Schulungsmaßnahme teilnehmen. Für alle anderen Angestellten empfiehlt sich die Verwendung von Schulungsunterlagen und Fragebögen bzw. Tests damit das Wissen der Angestellten vertieft werden kann.

Bei der Erstellung von Schulungen bzw. den verwendeten Unterlagen, sollten die firmenrelevanten IT-Sicherheitsthemen betrachtet werden. Falls beispielsweise BYOD firmenweit verboten ist, sollte dies zwar kurz in den Schulungsunterlagen erwähnt werden, aber keinen größeren Bereich einnehmen.

Mögliche Schulungsthemen sind:

- Informationen zur DSGVO
- Kennwortrichtlinie
- Korrektes Verhalten bei Sicherheitsproblemen
- Umgang mit personenbezogenen Daten
- Arten und potentielle Auswirkungen von Schadprogrammen
- Erkennung eines Schadprogrammbefalls
- Maßnahmen bei Entdeckung eines Schadprogrammbefalls
- Korrektes Verhalten im Internet
- Korrektes Verhalten bei unrechtmäßigen Anfragen
- Risiken für die Verwendung von IT-Ressourcen
- Die Bedeutung von Datensicherheitsmaßnahmen
- Potentielle Angriffe wie Phishing oder Social-Engineering
- Clear-Desk und Clear-Screen Policy
- Handhabung von Papierdokumenten
- Sicherheitsrisiken durch Fehlbedienung
- Korrekte Nutzung von Systemen und Services
- Richtlinien zum Teleworking bzw. Home-Office
- Privatnutzung der Firmenressourcen (Laptops, Mobiltelefone, Internet, usw.)
- BYOD Richtlinien

(Wöhrl & Becker, 2018, S. 26–33)

6.6 Nachweise für die DSGVO-Konformität

Laut DSGVO kann die zuständige Datenschutzbehörde beim Verantwortlichen oder dem Auftragsverarbeiter eine Kontrolle der TOMs durchführen bzw. anordnen. Geschäftspartner oder Kunden können ebenfalls eine Anfrage über die getroffenen Maßnahmen zum Schutz der personenbezogenen Daten bzw. generell zum Sicherheitsniveau des etwaigen Unternehmens stellen. In diesem Kapitel werden Optionen behandelt, die ein Unternehmen auf derartige Anfragen vorbereiten können.

6.6.1 Maßnahmenliste

Um schnell auf Anfragen der Datenschutzbehörde zu reagieren, sollten alle TOMs zum Datenschutz in einer Maßnahmenliste festgehalten werden. Diese Liste sollte stets gepflegt und auf dem aktuellen Stand sein. Im vorgeschrieben Verarbeitungsverzeichnis werden zwar die meisten Maßnahmen zum Datenschutz angeführt, allerdings kann eine Liste über alle vorhandenen Maßnahmen samt Version und Beschreibung helfen um die Anfragen von potentiellen Kunden oder Geschäftspartnern zum Sicherheitsstand des Unternehmens ausführlicher zu beantworten. Dies gilt jedoch nur sofern die Offenlegung der Maßnahmen kein Sicherheitsrisiko mit sich bringt.

6.6.2 Zertifizierung

Zertifikate sind Zeugnisse über abgelegte Prüfungen oder Prüfverfahren. Es können unter anderem Personen, Systeme und Unternehmen bzw. Unternehmensbereiche zertifiziert werden. Meist haben die ausgestellten Zertifikate eine begrenzte Gültigkeitszeit und müssen nach Ablauf der Gültigkeit erneut ausgestellt bzw. geprüft werden. Zertifikate werden von einer akkreditierten Zertifizierungsstelle ausgestellt. Laut DSGVO werden Zertifizierungsstellen durch die jeweils zuständige Datenschutzbehörde geprüft, woraufhin sie auch Prüfverfahren bei anderen Unternehmen bzw. von bestimmten Personen durchführen dürfen (Wöhrl & Becker, 2018, S. 36).

Personenzertifizierungen

Zur DSGVO gibt es keine direkte Personenzertifizierung, sondern eine Reihe an Ausbildungsverfahren von unterschiedlichen Zertifizierungsstellen, die sich mit dem Thema befassen. Anhand einer internationalen Norm haben Organisationen wie beispielsweise der TÜV einen Anforderungskatalog definiert, wodurch die jeweiligen Zertifizierungsstellen ähnliche Prüfverfahren verwenden um Personen als Datenschutzexperten oder -beauftragte einheitlich zertifizieren zu können (Wöhrl & Becker, 2018, S. 36).

ISO/IEC 27001

Die ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) 27000 ist eine Reihe von Dokumenten, mit dem Fokus auf verschiedene Aspekte des Informationssicherheitsmanagements. Da es sich bei der ISO um eine internationale Organisation handelt wird die Verbreitung, Bedeutung und Akzeptanz dieser Dokumente

maßgeblich erhöht. Das wichtigste Dokument der Reihe ist die ISO/IEC 27001 (Brenner, Gentschen Felde, Hommel, Metzger, Reiser, Schaaf, 2017, S. 1).

Unternehmen können ihr Informationssicherheitsmanagementsystem (ISMS) von einer Zertifizierungsstelle prüfen lassen. Wenn das ISMS den geforderten Spezifikationen entspricht, kann das Unternehmen ein Zertifikat für den geprüften Unternehmensbereich erhalten. Die ausgestellten Zertifikate haben eine begrenzte Gültigkeit und müssen wie die meisten anderen Zertifizierungen nach Ablauf der Gültigkeit erneut ausgestellt bzw. geprüft werden (Calder, 2017, S. 24).

Die Experteninterviews ergaben, dass meisten Unternehmen nur dann Personen- bzw. Systemzertifizierungen durchgeführt haben, wenn dies ausdrücklich gefordert wurde oder einen Wettbewerbsvorteil mit sich brachte. Da mit einem Zertifizierungsverfahren ein Kosten- bzw. Ressourceneinsatz verbunden ist, sollten die Resultate laut den Experten auch einen messbaren Mehrwert für das Unternehmen generieren.

6.6.3 Dokumentationen

Die Dokumentation der technischen und organisatorischen Maßnahmen kann sowohl zur Qualitätssicherung als auch zur Rechtfertigung vor der Datenschutzbehörde herangezogen werden. Diese Dokumente sollten übersichtlich gestaltet sein und nach Möglichkeit einem einheitlichen Schema folgen.

Die folgenden Informationen sollten in einer Maßnahmendokumentation enthalten sein:

- Autor des Dokuments, Prüfer und von welcher Person eine Freigabe erfolgte
- Art des Dokuments
- Datum und eventuell Uhrzeit
- Version des Dokuments
- Betroffene Personengruppen

  (Wöhrl & Becker, 2018, S. 22)

Sollten größere Änderungen bezogen auf die jeweiligen Maßnahmen durchgeführt werden, muss auch die dazu gehörende Dokumentation aktualisiert werden. Bei kleineren Änderungen kann jedoch davon abgesehen werden. Wie bei anderen schützenswerten Daten muss verhindert werden, dass unbefugte Personen die Dokumentationen lesen, ändern oder löschen können.

6.7 Fortlaufende Kontrolle und Anpassung der Maßnahmen

Laut DSGVO sind personenbezogene Daten durch technische und organisatorische Maßnahmen nach dem gegenwärtigen „Stand der Technik“ zu schützen. Besonders technische Maßnahmen sind hierbei zu beachten. Die IT Branche entwickelt sich stetig weiter, wodurch ein

wiederkehrendes Verfahren zur Kontrolle der Wirksamkeit der derzeit angewandten Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus notwendig ist.

Derartige wiederkehrende Kontrollmaßnahmen sollten nach dem PDCA-Zyklus (Demingkreis) entworfen werden. Die vier Phasen „Plan“, „Do“, „Check“ und „Act“ werden in einem nie endenden Kreislauf durchlaufen, sodass sichergestellt ist, dass eine fortwährende Verbesserung der Maßnahmen erzielt wird.

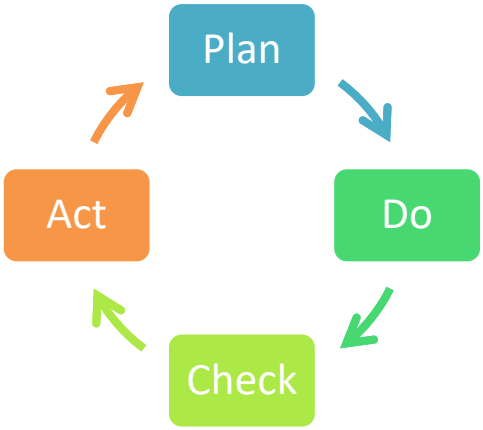

Abbildung 6: PDCA-Zyklus (vgl. Wöhrl, M. & Becker, V., 2018)

Plan – Planen

Neue TOMs bzw. die Ablösung alter TOMs durch Aktuelle wird geplant.

Do - Durchführen

Die erhobenen TOMs werden in einem kleinen Rahmen getestet.

Check - Überprüfen

Die Wirksamkeit der gewählten TOMs wird überprüft und gegebenenfalls angepasst bzw. korrigiert.

Act - Anpassen

Die getesteten und überprüften TOMs werden in den jeweiligen Bereichen produktiv angewandt.

(Wöhrl & Becker, 2018, S. 13)

Die fortwährende Verbesserung aller getroffenen Maßnahmen zur Gewährleistung der Datensicherheit wurde auch in den Experteninterviews als ein besonders wichtiger Aspekt angesprochen. Alle Experten waren sich einig, dass nur regelmäßig geprüfte und verbesserte Maßnahmen ein angemessenes Sicherheitsniveau bieten können.

7 ERGEBNISSE UND FAZIT

In der DSGVO werden viele wichtige Vorgaben zum korrekten Umgang mit personenbezogenen Daten angeführt. Zusätzliches Fachwissen, branchenspezifische Informationen und Vorlagen für alle nötigen Dokumente zur DSGVO können auf der Website der Wirtschaftskammer Österreich gefunden werden. In jedem Experteninterview wurde die WKO Seite als Anlaufstelle für Informationen und Ressourcen genannt.

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Unterstuetzung-zur-Umsetzung-der-DSGVO.html

Neben der unternehmensinternen Informationssammlung durch Fachliteratur oder Schulungen ist die Beratung durch externe Fachexperten auch eine gute Option zur Steigerung des Fachwissens. Die Konsultation von Rechtsanwälten mit Fokus auf Datenschutzangelegenheiten oder die Prüfung bzw. Zertifizierung durch einen externen IT-Dienstleister kann die firmeninternen Verantwortlichen bei ihren Tätigkeiten unterstützen. Besonders bei kleineren Unternehmen kann der Ressourceneinsatz zur Schulung bzw. Ausbildung interner Mitarbeiter die Beratungskosten durch externe Fachpersonen schnell übersteigen.

7.1 Hypothesenverifizierung

Ausgehend von der Grundhypothese „Die Umsetzung der durch die DSGVO vorgeschriebenen Anforderungen führt bei Klein- und Mittelbetrieben branchenübergreifend zu den gleichen grundlegenden Vorgehensweisen“ lässt sich sagen, dass diese als verifiziert gilt. Zumal sämtliche Experten in den Interviews darauf hinwiesen, dass sie bei der Umsetzung der notwendigen Maßnahmen zur DSGVO-Konformität grundlegend auf die gleiche Art und Weise vorgegangen sind. Daraus lässt sich schlussfolgern, dass KMUs sich an einer einheitlichen Vorgehensweise bzw. Methodik orientieren können um eine schnellere bzw. effizientere Umsetzung der durch die DSGVO vorgeschriebenen Tätigkeiten und Maßnahmen zu ermöglichen. Eine Best Practice Vorgehensweise bzw. eine Checkliste, wie sie in der vorliegenden Masterarbeit entwickelt wurde, bietet KMUs eine strukturierte Vorlage aller wichtigen Vorgehensweisen und zu setzenden Maßnahmen für die DSGVO Umsetzung.

7.2 DSGVO Best Practice Checklist

Um die Best Practice Vorgehensweise zur Umsetzung der DSGVO Anforderung zu erheben, wurde eine Checklist mit allen relevanten Bereichen zum Datenschutz erstellt. Die Checklist teilt sich, wie auch diese Masterarbeit, in die Bereiche: Vorbereitung, Ist-Analyse sowie technische und organisatorische Maßnahmen. Es werden Fragen zu den einzelnen Teilbereichen gestellt und mögliche Maßnahmen angeführt. Bei der Ausarbeitung dieser Maßnahmen wurde auf eine explizite Lösungsdefinition verzichtet, da meist eine Vielzahl an Optionen zum Datenschutz zur Verfügung stehen.

7.3 Ein Ausblick - Datenschutz in der Zukunft

Die Weiterentwicklung geschieht in kaum einem Bereich so rasant wie in der Informationstechnologie. Technologieinnovationen bringen jedoch meist neue Sicherheitsprobleme und demnach auch Sicherheitsmaßnahmen mit sich. Deshalb ist es für Unternehmen von höchster Priorität die Sicherheitsmaßnahmen dem Risikoniveau entsprechend anzupassen und sich am aktuellen Stand der Technik zu orientieren.

Mit der DSGVO und dem DSG sind bereits einige vielversprechende Ansätze zum Schutz von personenbezogenen Daten gesetzt worden. Da sich das Umfeld, in dem die Daten verarbeitet werden stetig ändert ist davon auszugehen, dass eine Anpassung und Erweiterung der Verordnung auch in Zukunft weiterhin stattfinden wird.

Derzeit bezieht sich die DSGVO auf die Mitgliedsstaaten der Europäischen Union. Es wurde zwar für einige Drittländer ein Angemessenheitsbeschluss des Datenschutzniveaus von der Kommission gewährt und im Fall der USA die Privacy Shield Lösung entwickelt, jedoch ist die Anzahl der Länder in jenen die DSGVO gegenwärtig Anwendung findet noch immer relativ gering. In Zukunft ist davon auszugehen, dass weitere Länder einen Angemessenheitsbeschluss erhalten und ein ausreichendes Datenschutzniveau bieten, wie beispielsweise Japan seit Anfang 2019. Dass demnächst eine einheitliche Datenschutzverordnung weltweit Anwendung findet, ist jedoch stark zu bezweifeln.

ANHANG A - 1. Best Practice Checklist

Best Practice Checklist

Vorwort

Diese Best Practice Checklist soll Unternehmen bzw. die zuständigen Personen über notwendige Tätigkeiten zur Umsetzung der DSGVO Themen grundliegend Informieren. Die einzelnen Themenbereiche werden mit entsprechenden Maßnahmen verknüpft. Diese Liste gilt nicht als vollständige Auflistung aller möglichen Maßnahmen, sondern kann als Orientierungshilfe angesehen werden.

Tätigkeiten	Status	Maßnahmen
Wurde eine zuständige Person für die DSGVO Anpassungen nominiert?	JA ☐	Falls nötig, die nominierte Person schulen
	NEIN ☐	Eine externe oder interne Person mit geeigneten Qualifikationen auswählen
Wird ein Datenschutzbeauftragter benötigt?	JA ☐	Eine externe oder interne Person mit geeigneten Qualifikationen auswählen
	NEIN ☐	Keine Maßnahme notwendig
Wurde die Budget- Zeit- und Ressourcenplanung durchgeführt und dokumentiert?	JA ☐	Die erstelle Dokumentation auf Vollständigkeit prüfen
	NEIN ☐	Nötige Ressourcen erheben und dokumentieren
Wurden die Führungskräfte über die DSGVO informiert?	JA ☐	Informationen in der Datenstruktur ablegen, damit erneuter Zugriff möglich ist
	NEIN ☐	Führungskräfte über Kernfakten der DSGVO informieren und sensibilisieren
Wurde erhoben welche personenbezogenen Daten derzeit verarbeitet werden?	JA ☐	Verarbeitungsverzeichnis erstellen bzw. überprüfen
	NEIN ☐	Daten bereichsweise erheben und im Verarbeitungsverzeichnis festhalten
Wurde erhoben welche Datenverarbeitungsvorgänge bestehen?	JA ☐	Verarbeitungsverzeichnis erstellen bzw. überprüfen
	NEIN ☐	Daten bereichsweise erheben und im Verarbeitungsverzeichnis festhalten
Wurden Verarbeitungsvorgänge im Datenverarbeitungsregister registriert?	JA ☐	Daten aus dem Register exportieren (bis Ende 2019 möglich)
	NEIN ☐	In der Dokumentation gegebenenfalls vermerken
Werden sensible Daten verarbeitet?	JA ☐	Im Verarbeitungsverzeichnis vermerken und prüfen ob diese notwendig bzw. konform sind
	NEIN ☐	In der Dokumentation vermerken
Wird eine Überwachung bzw. Bildverarbeitung durchgeführt?	JA ☐	Im Verarbeitungsverzeichnis vermerken und prüfen ob diese notwendig bzw. konform sind
	NEIN ☐	In der Dokumentation vermerken

Best Practice Checklist

Tätigkeiten	Status	Maßnahmen
Wird profiling angewandt?	JA ☐	Konformität der TOMs und die Erfüllung der Rechte der betroffenen Personen prüfen
	NEIN ☐	In der Dokumentation vermerken
Wurden Datenschutzerklärungen, AGBs, Verträge usw. auf deren Richtigkeit geprüft?	JA ☐	Gegebenenfalls Anpassungen vornehmen und Nutzer über Änderungen informieren
	NEIN ☐	Verträge auf Konformität prüfen, anpassen und Nutzer über Änderungen informieren
Werden Kindern Dienste angeboten?	JA ☐	Mindestalter und Gültigkeit der Dienstnutzung prüfen
	NEIN ☐	In der Dokumentation vermerken
Sind die Verträge und Vereinbarungen mit den Angestellten aktuell?	JA ☐	In der Dokumentation vermerken
	NEIN ☐	Die Dokumente überarbeiten und von den Angestellten unterzeichnen lassen
Ist bekannt für welche Zwecke personenbezogene Daten verarbeitet werden?	JA ☐	Die Verarbeitungszwecke im Verarbeitungsregister vermerken
	NEIN ☐	Die Verarbeitungszwecke überprüfen und im Verarbeitungsregister vermerken
Werden Daten an Drittländer oder internationale Unternehmen übermittelt?	JA ☐	Prüfen ob die Datenweitergabe und die Verträge/Garantien DSGVO konform sind
	NEIN ☐	In der Dokumentation vermerken
Werden Auftragsverarbeiter zur Datenverarbeitung herangezogen?	JA ☐	Die Datenweitergabe und den Auftragsverarbeitungsvertrag auf DSGVO Konformität prüfen
	NEIN ☐	Auftragsverarbeitungsvertrag vorbereiten und in der Dokumentation vermerken
Werden die Betroffenenrechte erfüllt und wurden Vorgänge zur Erfüllung dieser entwickelt?	JA ☐	Dokumentation über den Prozess, Schnittstellen, zuständige Personen usw.
	NEIN ☐	Notwendige Schritte zur Erfüllung der Betroffenenrechte einleiten und diese dokumentieren
Wird die Informationspflicht erfüllt?	JA ☐	Dokumentation über den Prozess, Schnittstellen, zuständige Personen usw.
	NEIN ☐	Notwendige Schritte zur Erfüllung der Informationspflicht einleiten und diese dokumentieren
Muss eine Datenschutz-Folgenabschätzung durchgeführt werden?	JA ☐	Die Datenschutz-Folgenabschätzung durchführen
	NEIN ☐	In der Dokumentation vermerken
Werden externe Ressourcen benötigt?	JA ☐	Mögliche externe Partner evaluieren und auswählen
	NEIN ☐	Keine Maßnahme notwendig

Best Practice Checklist

Tätigkeiten	Status	Maßnahmen
Bieten die Zutrittskontrollmaßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Bieten die Datenträgerkontrollmaßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Bieten die Speicherkontrollmaßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Bieten die Benutzerkontrollmaßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Bieten die Zugriffskontrollmaßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Bieten die Übertragungs-kontrollmaßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Bieten die Eingabekontroll-maßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Bieten die Transportkontrollmaßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Bieten die Wiederherstellungsmaßnahmen ein angemessenes Schutzniveau?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Ist die Zuverlässigkeit der Systeme und Services ausreichend gewährleistet?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Ist die Integrität der Daten ausreichend gewährleistet?	JA ☐	Dokumentation der TOMs und Planung von wiederkehrenden Kontrollmaßnahmen
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren

Best Practice Checklist

Tätigkeiten	Status	Maßnahmen
Sind die durchgeführten Maßnahmen am gegenwärtigen Stand der Technik?	JA ☐	Dokumentation des aktuellen Sicherheitsstandes
	NEIN ☐	Angemessene Schutzmaßnahmen evaluieren, umsetzen und dokumentieren
Wurde ein Verfahren zur wiederkehrenden Kontrolle und Verbesserung der Toms definiert?	JA ☐	Dokumentation des Verfahrens
	NEIN ☐	Ein PDCA-Verfahren zur Verbesserung der TOMs entwickeln und dokumentieren
Wurden die Unternehmensangestellten in Sicherheitsthemen geschult bzw. sensibilisiert?	JA ☐	Wiederkehrende Verfahren zur fortlaufenden Weiterbildung planen
	NEIN ☐	Schulungsverfahren und zukünftige Maßnahmen zur Wissensauffrischung planen
Wird eine Sicherheitszertifizierung benötigt bzw. wurde eine gefordert?	JA ☐	Eine akkreditierte Zertifizierungsstelle suchen und Zertifizierungsverfahren planen
	NEIN ☐	Keine Tätigkeit notwendig

ABKÜRZUNGSVERZEICHNIS

AGB – Allgemeinen Geschäftsbedingungen
BGBI – Bundesgesetzblatt
BYOD – Bring Your Own Device
DSB – Datenschutzbehörde
DSFA – Datenschutz-Folgenabschätzung
DSG – Datenschutzgesetz
DSGVO – Datenschutz-Grundverordnung
DVR – Datenverarbeitungsregister
EG – Europäische Gemeinschaft
EU – Europäische Union
GDPR – General Data Protection Regulation
IEC – International Electrotechnical Commission
ISMS – Informationssicherheitsmanagementsystem
ISO – International Organization for Standardization
IT – Informationstechnik
LAN – Local Area Network
PC – Personal Computer
PDCA – Plan Do Check Act
POLP – Principle of least Privilege
SMS – Short Message Service
SSL – Secure Sockets Layer
TED – Technology, Entertainment, Design
TLS – Transport Layer Security
TOM – Technische und organisatorische Maßnahmen
USA – United States of America
USB – Universal Serial Bus
VPN – Virtual Private Network
WAN – Wide Area Network
WKO – Wirtschaftskammer Österreich

ABBILDUNGSVERZEICHNIS

LITERATURVERZEICHNIS

Brenner, M., Gentschen Felde, N., Hommel, W., Metzger, S., Reiser, H., Schaaf, T. (2017). *Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung* (2. Aufl.). München: Hanser.

Bundesministerium für Digitalisierung und Wirtschaftsstandort. (2018). *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutz-Folgenabschätzung*. Abgerufen am 07.03.2019 von http://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20010206/DSFA-AV%2c%20Fassung%20vom%2007.03.2019.pdf

Bundesministerium für Digitalisierung und Wirtschaftsstandort. (2019). *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzgesetz*. Abgerufen am 17.02.2019 von http://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/10001597/DSG%2c%20Fassung%20vom%2024.05.2018.pdf

Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz. (2019). *Änderung des Bundes-Verfassungsgesetzes*. Abgerufen am 17.02.2019 von https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2019_I_14/BGBLA_2019_I_14.pdfsig

Calder, A. (2017). *ISO27001/ISO27002: Ein Taschenführer.* Ely, Cambridgeshire: IT Governance Publishing.

Datenschutzbehörde Republik Österreich. (o.D.a). *Datenschutz in Österreich*. Abgerufen am 07.03.2019 von https://www.dsb.gv.at/gesetze-in-osterreich

Datenschutzbehörde Republik Österreich. (o.D.b). *Fragen und Antworten*. Abgerufen am 07.03.2019 von https://www.dsb.gv.at/fragen-und-antworten#Was_geschieht_mit_dem_Datenverarbeitungsregister

Europa.Eu. (2018). *Verordnungen, Richtlinien und sonstige Rechtsakte*. Abgerufen am 07.03.2019 von https://europa.eu/european-union/eu-law/legal-acts_de

Europäisches Parlament und Rat der Europäischen Union. (2014). *Richtlinie 95/46/EG: Schutz von personenbezogenen Daten.* Abgerufen am 07.03.2019 von https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=LEGISSUM:l14012&from=DE

Europäisches Parlament und Rat der Europäischen Union. (2016). *Verordnung (EU) 2016/679*. Abgerufen am 07.03.2019 von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

Kovacs, G. (2012). *TED2012: Tracking our online trackers*. Abgerufen am 07.03.2019 von https://www.ted.com/talks/gary_kovacs_tracking_the_trackers

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

Österreichischer Nationalrat. (1978). *Bundesgesetz: Datenschutzgesetz - DSG*. Abgerufen am 17.02.2019 von https://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.pdf

Österreichisches Parlament. (2017). *Datenschutz-Anpassungsgesetz 2018*. Abgerufen am 07.03.2019 von https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00322/fname_635512.pdf

Österreichisches Parlament. (2018a). *Änderung des Datenschutzgesetzes – DSG*. Abgerufen am 07.03.2019 von https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_I_23/BGBLA_2018_I_23.pdfsig

Österreichisches Parlament. (2018b). *Datenschutz-Deregulierungs-Gesetz 2018*. Abgerufen am 07.03.2019 von https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_I_24/BGBLA_2018_I_24.pdfsig

Kaiser, R. (2014). *Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung*. Wiesbaden: Springer VS.

Wirtschaftskammer Österreich. (2017). *Aufsichtsbehörde, Strafen und Umsetzung in Österreich nach der EU-Datenschutz-Grundverordnung - FAQ*. Abgerufen am 07.03.2019 von https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-behoerde-strafen-umsetzung-faq.html

Wirtschaftskammer Österreich. (2018a). *EU-Datenschutz-Grundverordnung (DSGVO): Kurzüberblick und Zeitplan.* Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html

Wirtschaftskammer Österreich. (2018b). *EU-Datenschutz-Grundverordnung (DSGVO). Wichtige Begriffsbestimmungen*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Wichtige-Begriffsbestimmu.html

Wirtschaftskammer Österreich. (2018c). *EU-Datenschutz-Grundverordnung (DSGVO): Betroffenenrechte.* Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Betroffenenrechte.html

Wirtschaftskammer Österreich. (2018d). *EU-Datenschutz-Grundverordnung (DSGVO): Bildverarbeitung*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-bildverarbeitung.html

Wirtschaftskammer Österreich. (2018e). *EU-Datenschutz-Grundverordnung (DSGVO): Checkliste.* Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html

Wirtschaftskammer Österreich. (2018f). *EU-Datenschutz-Grundverordnung (DSGVO): Datensicherheitsmaßnahmen*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Datensicherheit-und-Daten.html

Wirtschaftskammer Österreich. (2018g). *EU-Datenschutz-Grundverordnung (DSGVO): Dokumentationspflicht - Verzeichnis von Verarbeitungstätigkeiten*. Abgerufen am 07.03.2019 von

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html

Wirtschaftskammer Österreich. (2018h). *EU-Datenschutz-Grundverordnung (DSGVO): Einwilligungserklärung.* Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html

Wirtschaftskammer Österreich. (2018i). *EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html

Wirtschaftskammer Österreich. (2018j). *EU-Datenschutz-Grundverordnung (DSGVO): Informationspflichten*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Informationspflichten.html

Wirtschaftskammer Österreich. (2018k). *EU-Datenschutz-Grundverordnung (DSGVO): Mustervertrag für die Auftragsverarbeitung*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html

Wirtschaftskammer Österreich. (2018l). *EU-Datenschutz-Grundverordnung (DSGVO): Pflichten des Auftragsverarbeiters*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Pflichten-des-Auftragsver.html

Wirtschaftskammer Österreich. (2019a). *EU-Datenschutz-Grundverordnung (DSGVO): Datenschutzbeauftragter*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Der-Datenschutzbeauftragt.html

Wirtschaftskammer Österreich. (2019b). *EU-Datenschutz-Grundverordnung (DSGVO): Ablaufplan Datenschutz-Folgenabschätzung*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Ablaufplan-Datenschutz-Fo.html

Wirtschaftskammer Österreich. (2019c). *EU-Datenschutz-Grundverordnung (DSGVO): Datenschutz-Folgenabschätzung und vorherige Konsultation*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html

Wirtschaftskammer Österreich. (2019d).*EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr*. Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Internationaler-Datenverk.html

Wirtschaftskammer Österreich. (2019e). *EU-Datenschutz-Grundverordnung (DSGVO): Prüfschema internationaler Datenverkehr.* Abgerufen am 07.03.2019 von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-pruefschema-internationaler-datenverkehr.html

Wöhrl, M., Becker, V. (2018). *Leitfaden technische und organisatorische Maßnahmen im Rahmen der DSGVO.* Abgerufen am 07.03.2019 von https://media.wko.at/epaper/Leitfaden-Sicherheitsmassnahmen-DSGVO/epaper/Leitfaden-Massnahmen-DSGVO.pdf