Analyse und Implementierung eines Datenschutzmanagements am Beispiel eines mittelständischen Unternehmens

Bachelorarbeit zur Erlangung des Bachelor-Grades
Bachelor of Science im Studiengang Wirtschaftsinformatik
an der Fakultät für Informatik und Ingenieurwissenschaften
der Technischen Hochschule Köln

vorgelegt von: Marco Nentwig
Matrikel-Nr.: 1111 7198
Adresse:

marco.nentwig@smail.th-koeln.de

eingereicht bei: Prof. Dr. Birgit Bertelsmeier

Zweitgutachterin: Prof. Dr. Heide Faeskorn-Woyke

Gummersbach, 24.09.2021

Kontaktdaten

Ersteller: **Marco Nentwig**

marco.nentwig@smail.th-koeln.de

Erstprüferin: **Prof. Dr. Birgit Bertelsmeier**

Campus Gummersbach

Steinmüllerallee 1

51643 Gummersbach

Raum 2.230

birgit.bertelsmeier@th-koeln.de

Zweitprüferin: **Prof. Dr. Heide Faeskorn-Woyke**

Campus Gummersbach

Steinmüllerallee 1

51643 Gummersbach

Raum 2.229 / 3.228

heide.faeskorn-woyke@th-koeln.de

Erklärung

Ich versichere, die von mir vorgelegte Arbeit selbstständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer oder der Verfasserin/des Verfassers selbst entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

Ort, Datum

Rechtsverbindliche Unterschrift

Kurzfassung/Abstract

Titel: Analyse und Implementierung eines Datenschutzmanagements am Beispiel eines mittelständischen Unternehmens

Zusammenfassung: Ziel dieser Bachelorarbeit ist die Analyse und die Implementierung eines Datenschutzmanagements, gemäß den geltenden EU-Datenschutzvorschriften, am Beispiel eines mittelständischen Unternehmens. Nach einer Zusammenfassung der wichtigsten theoretischen und rechtlichen Grundlagen, werden geeignete Methoden zur Umsetzung vorgestellt. Anschließend wird der Aufbau des Datenschutzmanagements analysiert und an einem Beispielunternehmen implementiert. Die Zielgruppe dieser Bachelorarbeit sind in erster Linie Unternehmen, Selbstständige oder Beschäftigte mit Datenschutzaufgaben.

Schlüsselwörter: Datenschutz, DSGVO, Datenschutzmanagement, DSM

Title: Analysis and implementation of data protection management using the example of a medium-sized company

Abstract: The aim of this bachelor thesis is the analysis and implementation of data protection management in accordance with the applicable EU data protection regulations using the example of a medium-sized company. After a summary of the most important theoretical and legal bases, suitable methods for implementation are presented. Then the structure of the data protection management is analyzed and implemented in a sample company. The target group of this bachelor thesis are primarily companies, self-employed or employees with data protection tasks.

Keywords: Data protection, GDPR, DSM

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

Das folgende Kapitel gibt einen Überblick über die Vorstellung, Gliederung und das Ziel der Bachelorarbeit. Die Motivation beschreibt die derzeitige Ausgangssituation und die treibende Idee hinter der Durchführung. Die Zielsetzung behandelt die Anforderungen an das zu erreichende Endprodukt, welches durch diese Bachelorarbeit umgesetzt werden soll. Die Gliederung beschreibt den Aufbau und den dazugehörigen Inhalt der vorliegenden Bachelorarbeit.

Das in dieser Bachelorarbeit gewählte Maskulinum bezieht sich zugleich auf die männliche, die weibliche und andere Geschlechteridentitäten. Zur besseren Lesbarkeit wird auf die Verwendung männlicher und weiblicher Sprachformen verzichtet. Alle Geschlechteridentitäten werden ausdrücklich mitgemeint, soweit die Aussagen dies erfordern.

1.1 Motivation

Am 25. Mai 2016 ist die EU-Datenschutz-Grundverordnung in Kraft getreten. Zwei Jahre konnten sich Unternehmen auf die neue Verordnung vorbereiten, welche seit dem 25. Mai 2018 verbindlich ist.[1]

Viele Unternehmen waren anfangs verunsichert, welches Ausmaß die neue Verordnung mit sich bringt. Die meisten Großunternehmen haben sich bereits weitreichend mit dem Thema befasst, eigene Abteilungen für den Datenschutz gebildet und erfüllen ihre rechtlichen Vorgaben. Kleine und mittelständische Unternehmen besitzen in den meisten Fällen weder die finanziellen Mittel noch ausreichende Kapazitäten, um einen Datenschutzbeauftragten, welcher die Umsetzung des Datenschutzes im Unternehmen übernimmt, zu bestellen. Infolgedessen wird der Datenschutz vernachlässigt und rückt in Vergessenheit. Sollte es jedoch zu einem schweren datenschutzrechtlichen Verstoß kommen, könnte dieser ein Unternehmen zur Existenzbedrohung führen.

Damit Unternehmer wissen, wie und was genau im Bereich Datenschutz umzusetzen und einzuhalten ist, benötigen diese weitgehendes technisches und rechtliches Fachwissen. Als „Geprüfter Datenschutzbeauftragter und Zertifizierte Fachkraft nach BDSG und DSGVO“ besitze ich die notwendigen Fachkenntnisse nach BDSG[2] und DSGVO[3], um Unternehmen als Datenschutzbeauftragter zur Seite zu stehen und alle rechtlichen Vorgaben zu analysieren und durchzuführen.

Im Zusammenhang mit Datenschutz werden vorgefertigte Datenschutzmanagementsysteme immer mehr zum Trend. Diese Systeme decken zwar die größten Risiken ab, können aber auf die Individualität einzelner Unternehmen nicht eingehen. Unternehmen sollten individuell betrachtet werden und ein Datenschutzkonzept mit einem eigenen Datenschutzmanagement verfolgen.

[1] [DSGVO] Vgl. Inkrafttreten und Anwendung, Art. 99

[2] [BDSG] Vgl. Datenschutzbeauftragter nicht öffentlicher Stellen, Art. 38 Abs. 6

[3] [DSGVO] Vgl. Benennung eines Datenschutzbeauftragten, Art. 37 Abs. 5

1.2 Zielsetzung

Die vorliegende Arbeit befasst sich mit dem Ziel, kleinen und mittelständischen Unternehmen die Notwendigkeit eines datenschutzkonformen Unternehmens zu erläutern, sowie eine allgemeine Hilfestellung zum Aufbau eines Datenschutzmanagements zu geben.

Der Aufbau eines Datenschutzmanagements ist ein umfangreicher, kontinuierlicher Prozess. Ziel ist es, diesen Prozess schrittweise und nachvollziehbar anhand eines mittelständischen Unternehmens abzubilden. Im Anschluss soll eine vollständige Übersicht über alle erzielten Ergebnisse, sowie alle organisatorischen, technischen und rechtlichen Maßnahmen des zu betrachtenden Unternehmens vorliegen.

Grundsätzlich sollen drei wesentliche Ziele durch den Aufbau eines Datenschutzmanagements abdeckt werden. Ein Unternehmen datenschutzkonform zu gestalten, damit alle rechtlichen Anforderungen und Pflichten eingehalten werden können, die Bereitschaft zu einem datenschutzkonformen Verhalten der Belegschaft zu fördern und ein Bewusstsein für datenschutzrechtliche Probleme zu schaffen. Weiterhin sollten die Themen fachfremden Personen verständlich gemacht werden, ohne zu detailliert auf einzelne Gesetze und Normen einzugehen.

Idealerweise kann die Arbeit verschiedensten Unternehmen als Vorlage und Nachschlagewerk für die Implementierung des eigenen Datenschutzmanagements dienen und somit den Datenschutz für die Unternehmen erhöhen.

1.3 Gliederung der Arbeit

Diese Arbeit behandelt im Kapitel 2 zunächst die theoretischen und rechtlichen Grundlagen des Datenschutzes für die zu erarbeitende praktische Umsetzung des Datenschutzmanagements. Zu Beginn in Kapitel 2.1 wird die geschichtliche Entwicklung und Bedeutung des Datenschutzes beschrieben. Fortführend im Kapitel 2.2 werden die rechtlichen Grundlagen und der dazugehörige sachliche und räumliche Anwendungsbereich analysiert. Das Kapitel 2.3 beschreibt die grundsätzlichen Anforderungen und Pflichten, welche Unternehmen laut datenschutzrechtlichen Bestimmungen umzusetzen und einzuhalten haben. Das letzte Kapitel 2.4 erläutert, wie ein Datenschutzmanagement diese Pflichten und Anforderung erfüllt und welche Notwendigkeit dieses mitbringt.

Im Kapitel 3 werden die Methoden zur Verwirklichung des Datenschutzmanagements vorgestellt. Zunächst wird in Kapitel 3.1 ein fiktives Unternehmen beschrieben, welches als Beispiel zum Aufbau des Datenschutzmanagements dient. Anschließend werden in Kapitel 3.2 die GAP-Analyse vorgestellt und in Kapitel 3.3 der PDCA-Zyklus erläutert, welcher zur Umsetzung genutzt wird.

Das vierte Kapitel behandelt die Analyse und Implementierung des Datenschutzmanagements. Hier werden zunächst in Kapitel 4.1 die Aufbauorganisation und in Kapitel 4.2 die Ablauforganisation beschrieben. Im Kapitel 4.3 werden die Auftragsverarbeiter analysiert und beschrieben welche Vorkehrungen bezüglich diesen getroffen werden sollten.

Zum Schutz der natürlichen Personen werden in Kapitel 4.4 der Umgang und die Handhabung mit Kunden- und Mitarbeiterdaten geregelt. Im Kapitel 4.5 geht es um die ergriffenen technisch-organisatorischen Maßnahmen, welche als wichtige technische Bausteine zum Schutz dienen. Das vorletzte Kapitel zu 4.6 beschreibt die grundsätzlichen Tätigkeiten des bestellten Datenschutzbeauftragten. Eine zusammenfassende Dokumentation zu den Aufwendungen ist im Kapitel 4.7 dargestellt.

Das fünfte und letzte Kapitel evaluiert welche Anforderungen umgesetzt werden konnten und ob Verbesserungspotential besteht. Abschließend wird ein Fazit gezogen und die Zukunft des Projektes betrachtet.

2 Theoretische Grundlagen

Das folgende Kapitel gibt einen Überblick über die Theorie und Inhalte der unterschiedlichen rechtlichen Grundlagen und Anforderungen des Datenschutzes. Die Themen umfassen die wichtigsten historischen und rechtlichen Grundlagen, sowie eine Analyse der Anforderungen und Pflichten für die Unternehmen.

Im Kapitel 2.1 Geschichte des Datenschutzes werden zunächst die historischen Meilensteine erläutert, welche als Vorlage heutiger Datenschutzgesetze dienten.

Anschließend werden in den Unterkapiteln zu 2.2 Rechtsgrundlagen die wichtigsten Rechtsquellen, sowie der dazugehörige sachliche und räumliche Anwendungsbereich analysiert. Dort wird unter anderem erläutern welche Gesetze es einzuhalten gilt, wo diese Gesetze ihren Ursprung haben und in welchen Anwendungsbereichen diese gelten.

Das dritte Unterkapitel 2.3 Anforderungen und Pflichten an ein Unternehmen beschreibt die notwendigen gesetzlichen Anforderungen und Pflichten, welche gemäß Datenschutzgesetzen vorgeschrieben und zu erfüllen sind. Hier werden unter anderem die Datenschutzgrundsätze, Rechte der Betroffenen oder auch die Dokumentationspflicht erläutert.

Abschließend wird in Kapitel 2.4 Datenschutzmanagement beschrieben, wie ein Datenschutzmanagement zu definieren ist und wie dieses bei den Anforderungen und Pflichten der gelten Datenschutzrechte hilfreich sein kann.

2.1 Geschichte des Datenschutzes

Der Gedanke eines umfassenden Datenschutzes ist recht neu und besteht erst seit dem 20. Jahrhundert. Doch schon in älteren Abkommen und Regelungen existierte der Schutz der Privatsphäre. Bereits der Hippokratische Eid von ungefähr 400 v.Chr. oder das Beichtgeheimnis für Geistliche enthielten Regelungen zur Schweigepflicht.

Erst im 19. Jahrhundert wurde die Privatsphäre aufgrund von technischen Entwicklungen (z.B. Erfindung der Fotographie) und der Verletzung der Privatsphäre durch journalistische Aktivitäten stärker diskutiert. Ein wichtiger Meilenstein hierbei war der in den USA erschienen Beitrag der Juristen Samuel Warren und Louis Brandeis „The Right to Privacy", welcher Privatsphäre auch als „the right to be let alone“ definierte.[4]

Im 20. Jahrhundert gewann das Konzept des Schutzes der Privatsphäre weiter an Bedeutung. 1948 nahm die Generalversammlung der Vereinten Nationen die „Allgemeine Erklärung der Menschenrechte“ an, welche in Artikel 12 den rechtlichen Schutz gegen

[4] [SWL] Vgl. The Right of Privacy

Eingriffe ins Privatleben beinhaltete.[5] Vergleichbares findet sich auch in Artikel 8 der Europäischen Menschenrechtskonvention[6] wieder, welche 1950 durch den Europarat ausgearbeitet wurde und 1953 in Kraft getreten ist. Obwohl diese Entwicklungen einen wichtigen Bezug zum Datenschutz haben, beruhte die Verletzung der Privatsphäre nicht auf der Datenverarbeitung. Vielmehr wurde die Privat- und Intimsphäre beispielweise durch unberechtigte Wohnungsdurchsuchungen oder das Abhören des Telefonanschlusses gefährdet. In den 1960er Jahren verlagerte sich der Fokus durch die Entwicklung der Computertechnik auf die Datenverarbeitung. Der damalige US-Präsident John F. Kennedy forderte ein „National Data Center“, mit dem Ziel, eine umfassende Datenbank über alle amerikanischen Bürger zu erhalten. Allerdings führte der Plan zu großen Protesten insbesondere in den USA und scheiterte schlussendlich an der Durchsetzung. Infolgedessen wurde die Debatte um eine einheitliche Privatsphäre wieder aufgerollt, mit dem Ergebnis der Einführung des „Privacy Act“[7] im Jahre 1974.

Auch in Deutschland wurde über die Begrifflichkeit „Privacy“ gestritten. Dies mündete in der Erschaffung des Wortes Datenschutz. Hessen verabschiedete im Jahre 1970 das weltweit erste Datenschutzgesetz.[8] Sieben Jahre später folgte auf bundesweiter Ebene das Bundesdatenschutzgesetz.[9]

Um innerhalb der Europäischen Union den Datenaustausch sicher zu ermöglichen wurde 1995 die EG-Datenschutzrichtlinie 95/46/EG[10] verabschiedet, welche alle EU-Staaten rechtlich auf den Schutz der personenbezogenen Daten verpflichten sollte. Daraufhin wurde 1999/2000 die Charta der Grundrechte der Europäischen Union erarbeitet und aufgrund der Unstimmigkeiten um den Europäischen Verfassungsvertrag erst 2009 rechtskräftig umgesetzt. Diese enthielt insbesondere in Artikel 8 ein eigenes Datenschutz-Grundrecht.[11]

Leider wurde mit der Zeit deutlich, dass trotz der Charta der Grundrechte der EU und der Richtlinie von 1995 kein ausreichendes Datenschutzniveau in allen Mitgliedsstaaten der EU erreicht wurde. Infolgedessen legte die Europäische Kommission im Jahr 2012 einen Entwurf für ein neues Datenschutzgesetz vor. Nach langer Verhandlung wurde schlussendlich die Datenschutz-Grundverordnung[12] am 27. April 2016 beschlossen. Sie trat am 25. Mai 2018 endgültig in Kraft. Neben den EU-Mitgliedstaaten gilt die DSGVO auch im Europäischen Wirtschaftsraum, wozu die Nicht-EU-Staaten Island, Liechtenstein und Norwegen gehören.[13]

[5] [AEM] Vgl. Universal Declaration of Human Rights of 1948

[6] [EMK] Convention for the Protection of Human Rights and Fundamental Freedoms of1950

[7] [PA] Privacy Act of 1974

[8] [DHS] Datenschutzgesetz Hessen von 1970

[9] [BDSGA] Bundesdatenschutzgesetz von 1977

[10] [DEG] Datenschutzrichtlinie 95/46/EG von 1995

[11] [CEU] Vgl. Charta der Grundrechte der EU, Kap. 2 Art.8

[12] [DSGVO] Datenschutzgrundverordnung

[13] [PSD] Vgl. Datenschutzrecht, Kap. 11, S.140 -142

2.2 Rechtsgrundlagen

2.2.1 Rechtsquellen

Basierend auf der historischen Geschichte des Datenschutzes bezieht sich geltendes Datenschutzrecht auf viele einzuhaltende Rechtsquellen. Aus der Sicht der Bundesrepublik Deutschland steht das EU-Recht bzw. das Europarecht an oberster Stelle.

Das Europarecht besteht aus dem primären Unionsrecht, dem sekundären Unionsrecht, dem Tertiärrecht und den völkerrechtlichen Verträgen der EU. Gemäß der Rangordnung steht das Primärrecht an erster Stelle und keine Normen anderer sekundärer Rechte dürfen Normen des Primärrechts widersprechen.

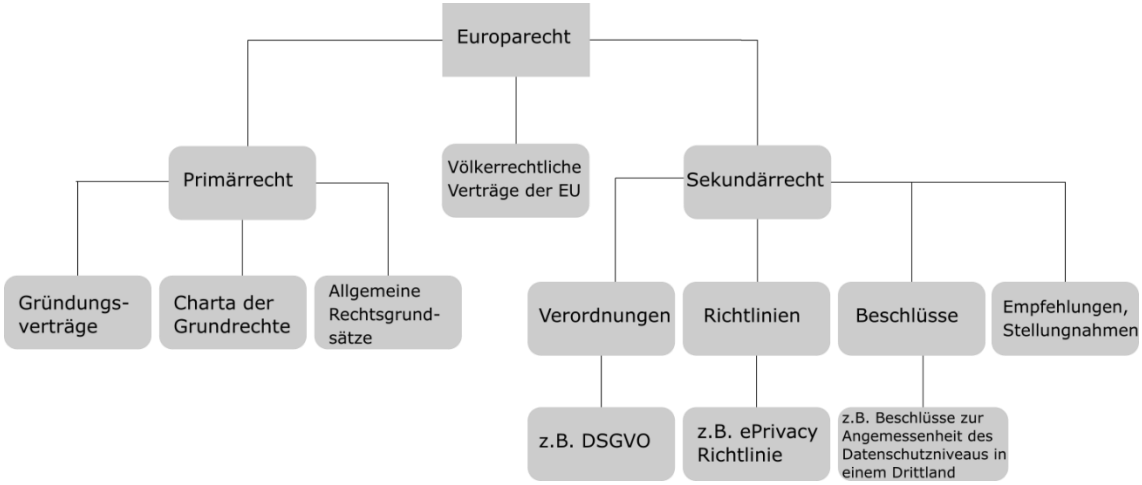

Abbildung 1: Datenschutz im Europarecht[14]

Im Primärrecht findet man in Bezug auf den Datenschutz die beiden Grundrechte der Charta der Grundrechte in Artikel 8 den „Schutz personenbezogener Daten“ und Artikel 7 „Achtung des Privat- und Familienlebens“. Gleichwohl ist zu beachten, dass alle Grundrechte miteinander in Gleichgewicht zu bringen sind. Somit können sich Verantwortliche auch auf das Recht auf Berufsfreiheit (Art. 15 GRCh), die unternehmerische Freiheit (Art. 16 GRCh) und das Eigentumsrecht (Art. 17 GRCh) beziehen, wenn sie personenbezogene Daten verarbeiten.[15]

Im Sekundärrecht finden wir die Datenschutzgrundverordnung.[16] Im Gegensatz zu Richtlinien müssen Verordnungen in jedem Mitgliedsstaat unmittelbar in vollem Umfang umgesetzt werden. Da die Datenschutzverordnung viele Rechte, Pflichten und Änderungen mit sich bringt, steht die Frage der Umsetzung der Verordnung in dieser Arbeit im Fokus. Unternehmen sind im Allgemeinen dazu, die DSGVO einzuhalten.

Nach der Normenhierarchie der Bundesrepublik Deutschland folgt dann das Grundgesetz, das Völkerrecht, das Bundesrecht und zuletzt das Landesrecht.

[14] [DBH] Rechtsquellen, Kap.5, S.33 Abb.1

[15] [CEU] Vgl. Art. 7,8,15,16,17

[16] [DSGVO] Datenschutzgrundverordnung

„*Das Grundgesetz gewährleistet jeder Bürgerin und jedem Bürger das Recht, über Verwendung und Preisgabe seiner persönlichen Daten zu bestimmen (Grundrecht auf informationelle Selbstbestimmung). Geschützt werden also nicht Daten, sondern die Freiheit der Menschen, selbst zu entscheiden, wer, was, wann und bei welcher Gelegenheit über sie weiß*.“[17]

Im Bundesrecht findet sich als Rechtsquelle für den Datenschutz das Bundesdatenschutzgesetz[18]. Die Regelungen des Bundesdatenschutzgesetzes können ergänzend zur Datenschutzgrundverordnung herangezogen werden. Ebenfalls sind in vielen anderen nationalen Gesetzen, Teile für den Datenschutz enthalten, beispielsweise im Strafgesetzbuch, dem Telekommunikationsgesetz, dem Informationsfreiheitsgesetz oder auch im Betriebsverfassungsgesetz.

Auf Landesebene wurden für jedes Bundesland ein eigener Landesdatenschutzbeauftragter und Aufsichtsbehörden bereitgestellt. Die Länder besitzen ebenfalls eigene Landesdatenschutzgesetze. Diese sind dennoch auf Grundlage der Datenschutzgrundverordnung aufgebaut. Somit sollte sich vor allem bei dem Aufbau eines Datenschutzmanagements und der dazugehörigen Verarbeitung von personenbezogenen Daten auf die Datenschutzgrundverordnung und das Bundesdatenschutzgesetz bezogen werden.

2.2.2 Sachlicher und räumlicher Anwendungsbereich

Der sachliche und räumliche Anwendungsbereich ist in der EU-Datenschutzgrundverordnung in Artikel 2 und 3 weitgehend abgegrenzt. Zur besseren Verdeutlichung wird bei dem sachlichen Anwendungsbereich eine negative Abgrenzung vorgenommen.

„*Für was findet die DSGVO keine Anwendungen?*

1. *Die DSGVO findet keine Anwendung, wenn die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (sog. Haushaltsprivileg) erfolgt.*
2. *oder nichtautomatisiert erfolgt und keine Speicherung der Dateien in einem Dateisystem erfolgt oder erfolgen soll.*
3. *oder durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Polizei, Staatsanwalt, etc.) erfolgt.“*[19]

Das Haushaltsprivileg umfasst nur die Verarbeitung personenbezogener Daten im privaten Umfeld. Hierzu gehören unter anderem private Fotographien, Geburtstags- oder Telefonlisten, Einladungen oder auch die Nutzung sozialer Netzwerke. Die Veröffentli-

[17] [BFDI] Was ist Datenschutz [online]

[18] [BDSG] Bundesdatenschutzgesetz

[19] [DBH] Sachlicher und räumlicher Anwendungsbereich, Kap. 5.2, S. 36

chung dieser Daten an einen unbestimmten Personenkreis, z.B. über eine Internetseite, unterliegt jedoch nicht dem Haushaltsprivileg und das geltende Datenschutzrecht muss in diesem Falle eingehalten werden.
Der Begriff des Dateisystems ist in der DSGVO wie folgt definiert: „*Ein Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.*“[20] Infolgedessen sind nicht nur elektronische Systeme, sondern auch analoge Systeme, wie beispielweise eine Anordnung von Kundendaten in Karteikartenformat oder ausgedruckte Listen mit Lieferantenadressen, ein Dateisystem. Die nicht erforderliche Anwendung der Datenschutzgrundverordnung durch zuständige Behörden zum Schutze des Landes sollte selbsterklärend sein.

„*Auch der räumliche Anwendungsbereich wird durch die DSGVO weit gefasst. Er umfasst folgende Konstellationen:*

1. *Die Verarbeitung der personenbezogenen Daten findet im Rahmen einer Tätigkeit einer Niederlassung in der EU statt (Art. 3 Abs. 1 DSGVO). Die Verarbeitung an sich muss dabei nicht in der EU stattfinden. Zudem ist unerheblich, ob es sich um den Hauptsitz oder nur eine untergeordnete Abteilung des Unternehmens handelt – entscheidend ist vielmehr (nur), dass sich die Niederlassung in einem EU-Mitgliedsstaat befindet.*
2. *Der Verantwortliche hat keine Niederlassung in der EU, verarbeitet die Daten aber mit Bezug zu einer Ware oder Dienstleistung, die sich an EU-Bürger richtet (Art. 3 Abs. 2 lit. a) DSGVO). Hier muss streng geprüft werden, ob das Produkt auch wirklich an EU-Bürger gerichtet ist: Hinweise darauf liegen vor, wenn ein Unternehmen eine Website mit einer Top Level Domain eines EU-Mitgliedsstaates verwendet (zum Beispiel .de) oder eine Zahlung in Euro anbietet.*
3. *Der Verantwortliche hat keine Niederlassung in der EU, verarbeitet die Daten aber, um das Verhalten sich in der Union aufhaltender Personen zu beobachten (Art. 3 Abs. 2 lit. b) DSGVO). Entscheidend ist dabei nicht die Staatsangehörigkeit, sondern nur, dass die betroffene Person sich momentan in der EU aufhält. Hiervon umfasst ist insbesondere das datenbasierte Nachvollziehen der Aktivitäten des Betroffenen im Internet im Rahmen des sogenannten Tracking.*“[21]

Zusammenfassend lässt sich hinsichtlich des räumlichen Anwendungsbereiches der DSGVO nach dem Niederlassungs- und dem Marktortprinzip differenzieren. Das Niederlassungsprinzip (siehe Punkt 1) knüpft die räumliche Anwendung der DSGVO an den Hauptsitz oder mindestens einer Niederlassung eines Unternehmens in der Europäischen Union. Das mit der DGSVO neu hinzugekommene Marktortprinzip (siehe Punkte 2,3) regelt den grenzüberschreitenden Verkehr zu Drittstaaten außerhalb der EU, somit

[20] [DSGVO] Begriffsbestimmung, Art.4 Abs. 6

[21] [HAU] Anwendungsbereich der DSGVO [online]

ist jeder Verantwortliche, welcher Daten einer in der EU aufhaltenden Person verarbeitet, rechtlich an die DSGVO gebunden.

2.3 Anforderungen und Pflichten an ein Unternehmen

Im Laufe des Lebens erzeugt jede Person viele Informationen. Diese werden in Form von Daten in unterschiedlichen Bereichen von Verwaltung und Wirtschaft erhoben, verarbeitet und gespeichert. Die Verarbeitung dieser Daten birgt Gefahren für die Persönlichkeitsentwicklung und die Persönlichkeitsentfaltung. Ein Individuum kann sich nicht mehr selbst ein Bild für die Umwelt erschaffen, wenn es nicht weiß, was andere Menschen bereits über seine Person wissen. [22] Aus diesem Grunde werden datenverarbeitenden Unternehmen gewisse Anforderungen und Pflichten vorgegeben, welche den Schutz personenbezogener Daten gewährleisten soll.

Bei Missachtung der rechtlichen Anforderungen und Pflichten und somit bei Verstößen gegen das geltende Datenschutzrecht können verschiedene Sanktionen verhängt werden. Je nach Schweregrad eines Vorfalls kann gegen unterschiedliche Gesetze verstoßen werden. Die derzeitige Höchststrafe bei einer Geldstrafe beträgt bis zu 20.000.000 Euro oder 4 % des gesamten, weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens. [23] Es können aber auch Freiheitsstrafen von bis zu drei Jahren verhängt werden, wenn wissentlich, unberechtigt, nicht allgemein zugängliche personenbezogene Daten, beispielsweise an Dritte, weitergegeben werden.[24]

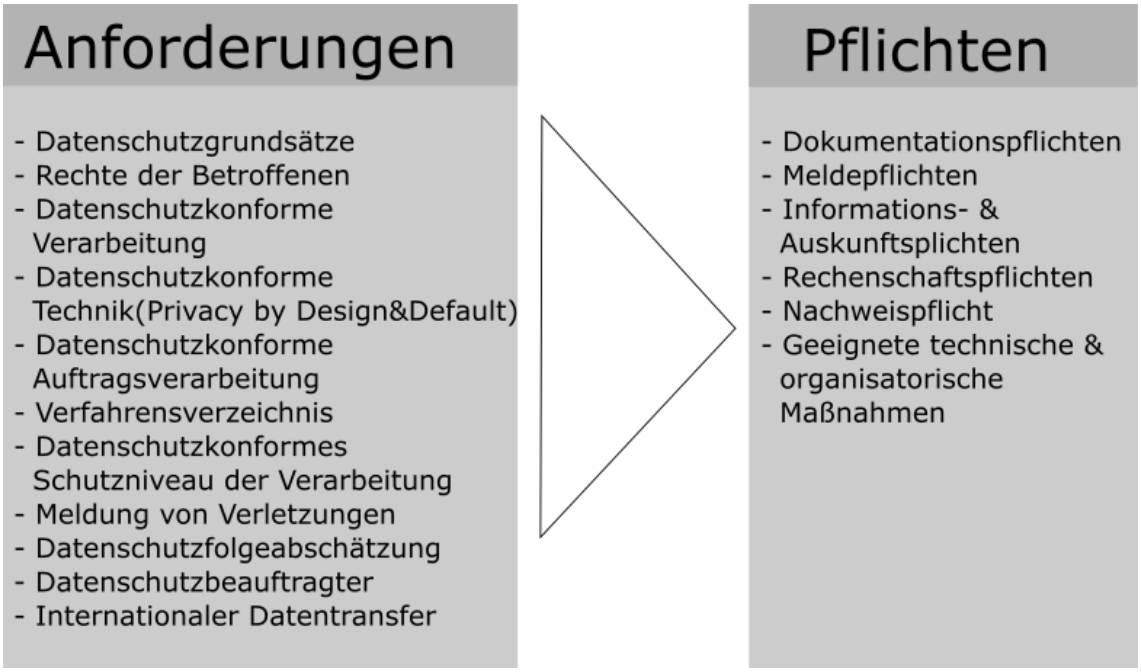

Abbildung 2: Umsetzung der Rechenschaftspflicht[25]

[22] [LDI] Vgl. Was ist Datenschutz [online]

[23] [DSGVO] Vgl. Allgemeine Bestimmung für die Verhängung von Geldbußen, Art. 83 Abs. 5

[24] [BDSG] Vgl. Strafvorschriften, Art. 42 Abs. 1

[25] [DCD] In Anlehnung an: Umsetzung der Rechenschaftspflicht, S.200 Abb. 78

In den folgenden zwei Unterkapiteln zu 2.3.1 Anforderungen und 2.3.2 Pflichten werden die umzusetzenden Anforderungen und Pflichten für die Rechenschaftspflicht (siehe Abbildung 2: Umsetzung der Rechenschaftspflicht) theoretisch zusammengefasst und analysiert.

2.3.1 Anforderungen

Datenschutzgrundsätze

Die Datenschutzgrundsätze regeln, wie personenbezogene Daten zu verarbeiten sind. Grundsätzlich ist die Verarbeitung personenbezogener Daten verboten, es sei denn, es liegt eine Erlaubnis bzw. eine *Rechtsmäßigkeit* vor. Die Rechtsmäßigkeit beschreibt auch die datenschutzkonforme Verarbeitung der Daten.

Jeder Verarbeitungsvorgang von personenbezogenen Daten muss einem eindeutigen, festgelegten Zweck unterliegen. Die *Zweckbindung* regelt gesetzlich, dass bereits erhobene Daten nicht für andere Zwecke missbraucht werden. Ein konkretes Beispiel ist die Verlockung, mit bereits gesammelten Daten für vertragliche Maßnahmen eine Werbekampagne zu starten.

Weiterhin muss zu jedem eindeutigen Zweck eine *Datenminimierung* vorgenommen werden. Die erforderlichen Daten müssen dem Zweck angemessen und auf das Notwendigste beschränkt sein. Dies gilt nicht nur für die Menge der erhobenen Daten, sondern auch für den Umfang der Verarbeitung, sowie die Zugriffsberechtigung. Eine Vorratsdatenspeicherung ist nicht erlaubt.

Die verwendeten Daten müssen immer einer *Richtigkeit* unterliegen. Falsche Informationen können sich negativ auf ein Personenbild auswirken und müssen schnellstmöglich berichtigt werden. Dies bezieht sich nicht nur auf Kundendaten, sondern auch auf die Daten von Mitarbeitern, Lieferanten und Geschäftspartnern.

Als weiteres Instrument der Datenschutzgrundsätze gilt die *Speicherbegrenzung*. Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie für den festgelegten Zweck erforderlich sind. Die Daten müssen nicht in jedem Fall gelöscht werden, eine Anonymisierung der Informationen reicht aus. Bei den Löschfristen müssen gesetzliche Aufbewahrungspflichten (z.B. Steuerrechtliche Aufbewahrungspflicht von 7 Jahren nach § 132 Abs. 1 BAO) beachtet werden.

Der letzte Grundsatz beschreibt den technischen und organisatorischen Schutz bei der Verarbeitung personenbezogener Daten. Personenbezogene Daten unterliegen den Schutzzielen der *Integrität, Vertraulichkeit und Verfügbarkeit*. Die Integrität beschreibt, dass Daten nicht unbefugt bzw. unerkannt verändert werden dürfen. Die Vertraulichkeit beschreibt, dass die Daten nur von Personen eingesehen werden dürfen, welche auch die erforderlichen Berechtigungen besitzen. Zum Beispiel müssen sensible Räumlichkeiten, wie ein Serverraum oder die Lohnbuchhaltung, besonders gesichert werden. Die

Verfügbarkeit beschreibt die Zeit, in der die Daten verfügbar sind. Beispiele für die Verfügbarkeit sind funktionsfähige IT-Systeme bei digitalen Informationen, aber auch der Brandschutz bei analogen Informationen.[26]

Rechte der Betroffenen

Die Rechte der Betroffenen wurden bereits im Praxisprojekt analysiert und im Folgenden erneut dargestellt:

„Jede betroffene Person kann von gewissen Rechten Gebrauch machen, falls ein Unternehmen Daten über sie verarbeitet. Um überhaupt fest zu stellen, welche Daten über einen gespeichert sind, kann das *Recht auf Auskunft* ausgeübt werden. Der Verantwortliche muss der betroffenen Person alle Verarbeitungszwecke, die Kategorien und personenbezogener Daten, sowie alle Empfänger, die Dauer und die Herkunft ihrer Daten preisgeben. Hierfür wird dem Verantwortlichen eine Frist von maximal einem Monat bereitgestellt.

Sollten falsche bzw. unrichtige Informationen in Umlauf geraten sein, kann das *Recht auf Berichtigung* durchgesetzt werden. Hierbei kann ein Betroffener veranlassen, dass seine Daten vervollständigt bzw. berichtigt werden. Der Verantwortliche hat somit Sorge zu tragen, alle internen und externen Empfänger zu Benachrichtigen und die Daten ändern zu lassen.

Um unnötiges Massenspeichern zu verhindern, wurde das *Recht auf Löschung* bzw. das *Recht auf Vergessenwerden* eingeräumt. Bei Beendigung des Zwecks, müssen alle nicht mehr benötigten Daten vernichtet werden. Auch wenn die betroffene Person die Verarbeitung nicht mehr wünscht oder einen Widerspruch einlegt, muss der Verantwortliche alle verarbeiteten Daten rechtmäßig vernichten. Es muss berücksichtigt werden, dass nicht alle Daten bedenkenlos gelöscht werden können, da die gesetzlichen Aufbewahrungsfristen Vorrang haben.

Bei Unklarheiten bezüglich der Verarbeitung kann das *Recht auf Einschränkung der Verarbeitung* bzw. *Recht auf Sperrung* genutzt werden. Gibt es Schwierigkeiten bei der Richtigkeit, Rechtmäßigkeit, Zweckbindung oder eines unrechtmäßigen Widerspruchs, müssen die entsprechenden Daten für den Zeitraum gesperrt werden. Der Betroffene und alle beteiligten Stellen sind über die Sperrung, sowie über die Aufhebung zu informieren.

Zu den weiteren Rechten gehört die *Mitteilungspflicht.* Wie bereits erwähnt, muss der Verantwortliche bei Berichtigung, Löschung oder Sperrung der personenbezogenen Daten den Betroffenen und allen internen sowie externen Empfänger benachrichtigen.

Um einen leichten Wechsel, beispielsweise von Verträgen, zu ermöglichen, kann das *Recht auf Datenübertragbarkeit* genutzt werden. Demnach muss der Verantwortliche

[26] [ADP] Vgl. Grundprinzipien der DSGVO, S. 59-67

alle Daten in einem strukturierten, gängigen und maschinenlesbaren Format entweder bereitstellen oder bei Beauftragung einem anderen Verantwortlichen direkt übermitteln.

Weiterhin haben Betroffene das Recht, nicht *ausschließlich automatisierten Entscheidungen bzw. Profiling* unterworfen zu sein. Beispielweise bei einem online beantragten Kredit, dürfen die Entscheidungen, ob ein Kredit gewährleistet wird oder nicht, nicht allein aufgrund von Algorithmen entschieden werden.

Falls ein Betroffener nicht mit der Verarbeitung seiner Daten zufrieden ist, kann sich auf das *Widerspruchsrecht* gestützt werden. Dies ist meistens bei Zwecken der Direktwerbung oder eines Profilings sehr nützlich. Der Verantwortliche darf die Daten für den gewünschten Zweck dann nicht mehr nutzen.

Bei Fragen über die Verarbeitung hat ein Betroffener immer das Recht*, den Datenschutzbeauftragten zu konsultieren* und bei berechtigten Beschwerden auch das *Recht auf Beschwerde bei einer Aufsichtsbehörde*.“[27]

Datenschutzkonforme Verarbeitung

Eine Verarbeitung beschreibt die Erhebung, Veränderung oder Löschung von personenbezogenen Daten. Für die datenschutzkonforme Verarbeitung ist die Rechtmäßigkeit zuständig. Jeder Verarbeitungsvorgang muss sich auf ein Recht beziehen. Diese Rechtmäßigkeit kann durch folgende Aspekte einberufen werden:

Die Datenverarbeitung für die *Vertragserfüllung und vorvertragliche Maßnahmen* sind generell erlaubt. Ein Verbot würde nur unnötig den Handel erschweren.

Gesetzliche Aspekte finden sich unter den *gesetzlichen Grundlagen* (z.B. Steuerpflicht), der *Wahrung des Öffentlichen Interesses* (z.B. Öffentliche Gewalt) und dem *lebenswichtigen Interesse* (z.B. Medizinische Notfälle) wieder.

Das *berechtigte Interesse* bei der Verarbeitung bezeichnet die vernünftigen Erwartungen der betroffenen Person bezüglich ihrer Beziehung zum Verantwortlichen. Es wird unter anderem für den Versand von Informationen an bestehende Kunden verwendet.

Eine *Einwilligung bzw. Zustimmung* zur Verarbeitung muss in jedem Falle freiwillig, informiert und jederzeit widerruflich sein. Die Einwilligungserklärung ist ein beliebtes Mittel als Alleskönner, sollte jedoch besonnen eingesetzt werden, da diese oft für Werbezwecke missbraucht wird.

Datenschutzkonforme Technik

Der Datenschutz in technischen Umgebungen sollte nach dem *Privacy-by-Design* und *Privacy-by-Default-Prinzip* aufgebaut werden. Privacy by Design bezeichnet den Datenschutz durch Technikgestaltung. Bereits bei der Entwicklung und dem Design von Hard- und Software ist zu beachten, dass geeignete technische Maßnahmen zum Datenschutz getroffen werden. Die Maßnahmen sind so auszulegen, dass die gesetzlich geforderten

[27] [ICH] Rechte der Betroffenen, Kap. 2.1.6, S. 8-9

Datenschutzgrundsätze unter Berücksichtigung des Stands der Technik wirksam umgesetzt werden.

Privacy by Default bezeichnet den Datenschutz durch datenschutzfreundliche Voreinstellungen. Dementsprechend sollen die Werkseinstellungen in Systemen, Programmen und sonstigen Anwendungen entsprechend so gestaltet sein, dass die Privatsphäre der Nutzer geschützt ist, ohne dass sie passende Einstellungen noch zusätzlich vornehmen müssen.

Beide Konzepte haben sich zum Ziel gesetzt, die Zweckbindung und Datenminimierung zu optimieren. Sie beziehen sich vor allem auf die Art, den Umfang, die Speicherfristen und die Zugänglichkeit der zu verarbeitenden Daten.

Datenschutzkonforme Auftragsverarbeitung

Eine Auftragsverarbeitung bezeichnet die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Dienstleister im Auftrag des Verantwortlichen. Da die Weitergabe an Dritte grundsätzlich nur durch einen speziellen Erlaubnistatbestand oder durch die Einwilligung des Betroffenen erlaubt ist, bedarf es einer eigenen Regelung in der Auftragsverarbeitung. Ein Erlaubnistatbestand liegt vor, wenn der Dienstleister nur für einen bestimmten Zweck personenbezogene Daten sammelt und eine interne Verarbeitung beim Verantwortlichen erfolgt.

Zum Abschluss einer Datenverarbeitung mit Dritten ist eine Vereinbarung bzw. ein Auftragsverarbeitungsvertrag notwendig. Diese Vereinbarung stellt sicher, dass sich der externe Dienstleister den erforderlichen Datenschutzregelungen verpflichtet und die personenbezogenen Daten in sicheren Händen sind.

Wann ein Auftragsverarbeitungsvertrag abzuschließen ist, muss je nach Dienstleistung selbst geprüft werden. Grundsätzlich ist der Vertrag vom Dienstleister auszustellen, die Haftung bei fehlendem Vertrag liegt jedoch bei beiden Parteien. Steuerberater, Rechtsanwälte, Betriebsärzte und einige weitere Berufsgruppen zählen zu den sogenannten fremden Fachleistungen. Sie sind selbst für die Daten verantwortlich und benötigen somit keinen Auftragsverarbeitungsvertrag.[28]

Verfahrensverzeichnis

Jedes Unternehmen ab 250 Mitarbeitern und Unternehmen, welche nicht nur gelegentlich Daten verarbeiten, sind dazu verpflichtet, ein Verfahrensverzeichnis bzw. ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Da fast jedes Unternehmen mehr als gelegentlich Daten verarbeiten muss, (z.B. Kunden-, Mitarbeiter-, Lieferantenkontakte) geht man davon aus, dass nahezu jedes Unternehmen ein Verzeichnis führen sollte.

[28] [FHD] Vereinbarung der Auftragsverarbeitung, S.611-618

Das Verfahrensverzeichnis ist eine Auflistung über alle Prozesse im gesamten Unternehmen. „*Die Datenschutz-Grundverordnung verpflichtet nach Art. 30 EU-DSGVO dazu eine schriftliche Dokumentation und Übersicht über Verfahren zu führen, bei denen personenbezogene Daten verarbeitet werden. In dem Verzeichnis von Verarbeitungstätigkeiten müssen wesentliche Angaben zur Datenverarbeitung aufgeführt werden, wie u.a. die Datenkategorie, der Kreis der betroffenen Personen, der Zweck der Verarbeitung und die Datenempfänger. Auf Anfrage ist es der Aufsichtsbehörde vollständig zur Verfügung zu stellen.“*[29]

Die Anfertigung des Verzeichnisses sollte von jeder Abteilung im Unternehmen selbst durchgeführt werden, da diese ihre Prozesse besser kennen als die Geschäftsführung des Unternehmens, den sogenannten Verantwortlichen. Der Datenschutzbeauftragte übernimmt in den meisten Fällen die Koordination zur Erstellung des Verzeichnisses und kontrolliert dieses im Anschluss.

Datenschutzkonformes Schutzniveau der Verarbeitung

Zum technischen und organisatorischen Schutze der personenbezogenen Daten ist der Verantwortliche verpflichtet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung geeignete Maßnahmen zu treffen.

Der Umfang der technischen und organisatorischen Maßnahmen wird an den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit bemessen. Als technische Maßnahmen werden Systeme oder Dienste bezeichnet, wie Firewalls, Überwachungen der Räumlichkeiten oder Backup-Systeme. Als organisatorischen Maßnahmen werden unter anderem Verschwiegenheitserklärungen, Verpflichtungen zum Datenschutz oder auch Richtlinien zur Sicherheit im Unternehmen bezeichnet. Weiterhin wird ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technisch organisatorischen Maßnahmen verlangt.

Zur Bewertung des erforderlichen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen. Mit Hilfe des Verarbeitungsverzeichnisses sollte für jeden Prozess eine Risikoanalyse mit den Parametern Eintrittswahrscheinlich und Schwere des potenziellen Schadens durchgeführt werden. Anhand der Risiken können entgegenwirkende technisch organisatorische Maßnahmen getroffen werden.

Meldung von Schutzverletzungen

Eine Datenschutzpanne beschreibt im Allgemeinen den Verlust der Kontrolle über die Daten. Eine Verletzung ist ein Verstoß gegen die Datensicherheit und den Datenschutz, indem personenbezogene Daten von Unberechtigten vermutlich oder erwiesenermaßen

[29] [ICS] Verzeichnis von Verarbeitungstätigkeiten [online]

eingesehen, vernichtet oder bekannt werden. Es gibt viele Ursachen für einen Sicherheitsvorfall, die bekanntesten sind Hackerangriffe, Diebstahl oder der Verlust von Hardware oder Unterlagen.

Das Verhalten innerhalb eines Unternehmens bei einer Datenpannen, sollte in einem Notfallplan erklärt sein. Eine schnelle Reaktion ist unbedingt notwendig. Der zeitliche Aspekt spielt zum einen für die forensische Analyse der Sicherheitslücke eine wichtige Rolle. Zum anderen müssen schwere Sicherheitsverletzung innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde gemeldet werden. Wann eine Datenpanne der Aufsichtsbehörde gemeldet werden sollte, liegt im Ermessen des Datenschutzbeauftragten und dem Verantwortlichen. Sicherheitsverletzungen, welche voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der Betroffen führen, müssen grundsätzlich nicht gemeldet werden.

Neben der Meldung an die Aufsichtsbehörde sind auch die Betroffenen darüber zu informieren, in welchem Rahmen ihre personenbezogenen Daten missbraucht wurden. Da es zu einer Rufschädigung des Unternehmens kommt, kann in dieser Information den Betroffenen direkt die Lage und zukünftige Maßnahmen erläutert werden.

Datenschutz-Folgeabschätzung

Die Datenschutz-Folgeabschätzung ist ein spezielles Mittel des Datenschutz-Risikomanagements zur Beurteilung und Behandlung von Risiken im Datenschutz. Verantwortliche müssen eine Datenschutzfolgeabschätzung, kurz DSFA, durchführen, wenn die Verarbeitung von personenbezogenen Daten voraussichtlich ein hohes Risiko mit sich bringt. Wann genau eine Datenschutzfolgeabschätzung notwendig ist, lässt sich mit der Risikobeurteilung feststellen. Sollte bei der Feststellung der Schwellenwertanalyse ein hohes Risiko bestehen, ist für den Verarbeitungsvorgang eine DSFA notwendig.

Der Prozess wird zunächst durch die Verantwortlichen und die zuständigen Abteilungen auf Datenflüsse und Systemen analysiert. Anhand der Datenflüsse lassen sich die personenbezogenen Daten bestimmen. Eine erweiterte Risikoanalyse wird vorgenommen und Risiken identifiziert, analysiert und sodann beurteilt. Anschließend müssen geeignete technische und organisatorische Maßnahmen zur Minderung des Risikos beschlossen werden. Sollten ein hohes Risiko bestehen, welches nicht durch Maßnahmen gelindert werden kann, ist die zuständige Aufsichtsbehörde zu konsultieren.[30]

Datenschutzbeauftragter

Als erster Ansprechpartner im Unternehmen zum Thema Datenschutz steht grundsätzlich der Datenschutzbeauftragte zur Verfügung. Die Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, wenn im Unternehmen entweder umfangreiche Verarbeitungen personenbezogener Daten stattfinden, mindestens 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind oder besonders sensible Daten ver-

[30] [DCD] Vgl. Datenschutz-Risikomanagement, Kap.6, S. 140-152

arbeitet werden. Der Datenschutzbeauftragte ist in erster Linie für die Kontrolle des Datenschutzes im Unternehmen zuständig. Aus diesem Grunde handelt er einerseits weisungsfrei, anderseits erteilt er aber keine Anweisungen. Er besitzt die Position eines Beraters und gibt Handlungsempfehlungen. Die Entscheidung zur Umsetzung liegt beim Verantwortlichen.

Internationaler Datentransfer

Bei der Übermittlung von personenbezogenen Daten an Drittstaaten ist zwischen Ländern der Europäischen Union bzw. EWR und nicht EU-Mitgliedstaaten bzw. EWR-Staaten zu unterscheiden. Die Übermittlung an EU-Mitgliedstaaten ist grundsätzlich erlaubt.

„*Im Falle einer Datenübermittlung in Drittstaaten ist eine zweistufige Prüfung vorzunehmen. Zunächst muss, wie bei Datenübermittlungen im Inland beziehungsweise Übermittlungen in das EU- und EWR-Ausland, ein Rechtfertigungsgrund des Artikel 6 DSGVO greifen (etwa ein überwiegendes berechtigtes Interesse des Verantwortlichen). Ist dies der Fall, muss in einem zweiten Schritt festgestellt werden, ob beim Drittstaat oder zu mindestens beim konkreten Empfänger ein angemessenes Datenschutzniveau besteht. Hierbei ist allerdings in der Regel keine eigene Abwägung des Verantwortlichen gefragt.*“[31]

Die Abwägung kann durch verschiedene Instrumente bewirkt werden. Die EU-Kommission stellt per Angemessenheitsbeschluss fest, in welchen Drittstaaten, Gebieten oder auch Sektoren ein angemessenes Datenschutzniveau besteht. Beispielstaaten mit angemessenen Datenschutzniveau sind Israel, Kanada oder auch Uruguay.

Ein anderes Instrument sind die EU-Standarddatenschutzklauseln oder Abkommen, wie das EU-US-Privacy Shield, wonach amerikanische Unternehmen ein spezielles Zertifizierungsverfahren durchlaufen müssen.

Praxisrelevant für Unternehmen zur Übermittlung in Drittstaaten sind insbesondere die Einwilligung des Betroffenen und die Datenübermittlung zur Vertragserfüllung, welche als Ausnahmetatbestände vorliegen können.

2.3.2 Pflichten

Dokumentationspflicht

Die Dokumentationspflicht beschreibt die Notwendigkeit der Dokumentation einzelner oben genannten Anforderungen und weiterer Bemühungen zur Einhaltung der Datenschutzgesetze. Zum einen umfasst die Dokumentationspflicht die Anfertigung von Pflichtdokumenten, wie das Verzeichnis von Verarbeitungstätigkeiten oder die Dokumentation von Datenpannen. Zum anderen sind weitergehende Maßnahmen, wie die Schulung der Mitarbeiter oder das Einsetzen von Datenschutzleitlinien verpflichtet. Grundsätzlich sollte alles zum Thema Datenschutz im Unternehmen an einem Ort ordnungsgemäß dokumentiert werden.

[31] [ADP] Datenübermittlung in Drittstaaten, S.116-119

Meldepflicht

Unternehmen müssen sich kooperativ gegenüber den Aufsichtsbehörden zeigen. Aus diesem Grund sind Meldungen an die zuständige Behörde notwendig.

Die Kommunikation zwischen Verantwortlichen und Aufsichtsbehörden erfolgt in den meisten Fällen durch den vom Unternehmen berufenen Datenschutzbeauftragten. Damit die Aufsichtsbehörde über die Person des aktuell zuständigen Datenschutzbeauftragten Kenntnis hat, muss bei Berufung, Änderung oder Abberufung des Datenschutzbeauftragten die Behörde informiert werden. Dieser wird im Anschluss in einer zentralen Datenbank hinterlegt.

Eine weitere Pflicht ist die Meldung bei Datenverletzung. Die Meldung hat innerhalb von 72 Stunden nach Kenntniserlangung bei der zuständigen Behörde vorzuliegen. Hierzu stellt die Aufsichtsbehörde spezielle Formulare zur Verfügung, um die Datenschutzverletzung aufzuzeichnen, den Schweregrad zur ermittelt und geeignet Gegenmaßnahmen zu treffen. In welchen Fällen eine meldepflichtige Datenschutzverletzung vorliegt, sollten der Verantwortliche und der Datenschutzbeauftragte abwägen.

Sollte bei der Erstellung des Verfahrensverzeichnisses und einer nachfolgenden Datenschutzfolgeabschätzung bei einem Prozess ein erhöhtes Risiko, welches nicht durch geeignete Gegenmaßnahmen abgeschwächt werden kann, festgestellt werden, ist dieser Prozess der Aufsichtsbehörde zu melden.

Informations- und Auskunftspflicht

Die DSGVO fordert eine umfassende Informations- und Auskunftspflicht gegenüber den Betroffenen. Zum einen muss der Verantwortliche bereits bei der Erfassung von personenbezogenen Daten transparent handeln, indem Betroffenen alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form bereitgestellt werden. Zum anderen muss der Verantwortliche den Betroffenen, bei Beantragung, eine umfassende Auskunft über die gespeicherten und verarbeiteten Daten geben. Nach Beantragung ist dem Verantwortlichen hierfür eine Frist von einem Monat zu gewähren.

Weitere Auskünfte sind Betroffenen bei der Berichtigung, Löschung oder Sperrung ihrer personenbezogenen Daten zu geben.[32]

Rechenschaftspflicht

Eine weitere Pflicht der DSGVO ist die Rechenschaftspflicht. Die Rechenschaftspflicht erfordert, dass die Grundsätze der Verarbeitung personenbezogener Daten eingehalten werden. Erreichbar ist dies zum einen durch das Verzeichnis von Verarbeitungstätigkeiten, in dem die Rechtmäßigkeit, Zweckbindung und Datentypen zur Datenminimierung beschrieben sind. Zum anderen durch die getroffenen technisch-organisatorischen Maßnahmen. Die Maßnahmen müssen lediglich angemessen sein.[33]

[32] [DSGVO] Vgl. Informations- und Auskunftspflicht, Art. 15

[33] [DSGVO] Vgl. Rechenschaftspflicht, Art. 5 Abs. 2

Nachweispflicht

Nachweispflicht bedeutet, dass Unternehmen auf Nachfrage der Aufsichtsbehörde belegen können müssen, dass die Vorgaben der DSGVO eingehalten werden. In den meisten Fällen stellt die Aufsichtsbehörde eine Liste mit Dokumenten zur Verfügung, welche sie einzusehen fordert. Bei der Offenlegung des gesamten Datenschutzkonzeptes ist zu beachten, dass es sich zwar einerseits positiv auf das Verhältnis zur Aufsichtsbehörde auswirken kann. Anderseits ermöglicht dies aber auch die Aufdeckung möglicher Mängel oder Lücken im Gesamtkonzept. Nach dem Gebot der Selbstbezichtigung müssen Unternehmen keine Dokumente zur Verfügung stellen, welche sie selbst belasten können.

Geeignete technische und organisatorische Maßnahmen

Verantwortliche sind verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten einzusetzen, um sicherzustellen und nachweisen zu können, dass sie die Vorgaben der DSGVO umsetzen. Bei der Festlegung von Maßnahmen sind Art, Umfang, Umstände, die Verarbeitungszwecke ebenso wie unterschiedliche Eintrittswahrscheinlichkeiten und die Schwere der Risiken zu berücksichtigen. Der Nachweis erfolgt über eine entsprechende Beschreibung dieser Maßnahmen, z. B. in einem Vertrag über Auftragsverarbeitung und/oder im sog. Verzeichnis für Verarbeitungstätigkeiten. Können Verantwortliche im Zusammenhang mit der Verarbeitung auf genehmigte Verhaltensregeln oder auf genehmigte Zertifizierungen zurückgreifen, so können diese herangezogen werden, um die Umsetzung dieser Verpflichtung nachzuweisen. Dieser Punkt sollte bei einer Dokumentation berücksichtigt werden.[34]

2.4 Datenschutzmanagement

Die Einhaltung des Datenschutzes ist die Aufgabe jeder im Unternehmen angestellten Person. Der Verantwortliche steht zwar im Fokus der Verantwortung, kann aber nicht zu jeder Zeit und an jedem Ort im Unternehmen anwesend sein. Zur Verwaltung und Verbesserung des Datenschutzes ist die Einführung eines Datenschutzmanagements sinnvoll.

Ein Datenschutzmanagement regelt, wie im Unternehmen mit personenbezogenen Daten umzugehen ist. Es stellt einen internen Leitfaden dar, welcher den Datenschutz regeln, planen, steuern, umsetzen und kontrollieren soll. Alle Mitarbeiter im Unternehmen können sich somit an diesem Leitfaden orientieren und den Schutz der personenbezogenen Daten optimal einhalten.

Ein erfolgreiches Datenschutzmanagement muss alle rechtlichen Anforderungen und Pflichten (siehe Abbildung 2: Umsetzung der Rechenschaftspflicht) erfüllen und die Einhaltung nachweisen können, indem es die rechtlichen, organisatorische und technischen Maßnahmen sicherstellt und die sichere Verarbeitung personenbezogener Daten ge-

[34] [IHK] Dokumentationspflicht, Art.24 [online]

währleistet. Im Falle einer Kontrolle durch die Aufsichtsbehörde können geforderte Dokumente in kürzerer Zeit gefunden und der interne Datenschutz konkret nachgewiesen werden. Infolgedessen können drohende Bußgelder oder Kontrollen abgeschwächt oder verhindert werden.

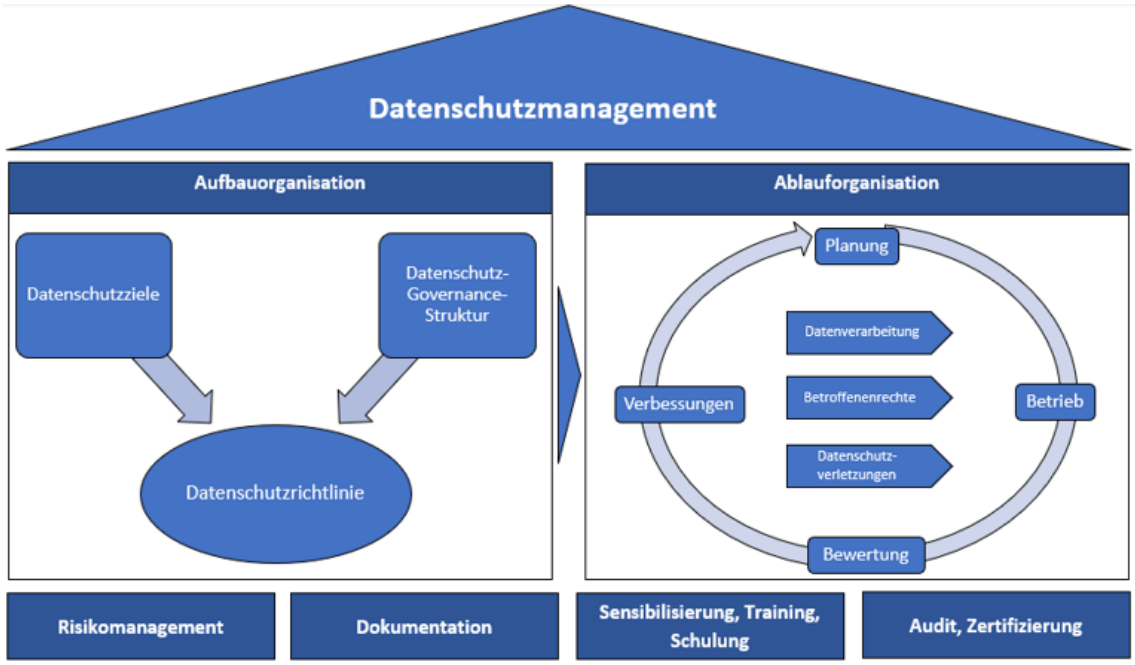

Abbildung 3: Datenschutzmanagement[35]

Zu den grundsätzlichen Zielen des Datenschutzmanagements (siehe Abbildung 3: Datenschutzmanagement) zählt eine datenschutzkonforme Aufbau-, sowie Ablauforganisation. Die Etablierung wesentlicher Standards wie Risikomanagement, Schulungen und Audits sind zu planen. Auftragsverarbeitungsverträge, technisch-organisatorische Maßnahmen, Rechenschaftsplicht oder auch die Bestellung eines Datenschutzbeauftragten müssen umgesetzt werden und die Einführung standardisierter Prozesse für Datenschutzverletzungen, Betroffenenrechte oder Löschanfragen sind zu dokumentieren. Weiterhin ist die Herausgabe einer Übersicht über die Umsetzung der DSGVO an Mitarbeiter mit entsprechenden Leitlinien und konkrete Handlungsempfehlungen empfehlenswert.[36]

[35] [DCD] In Anlehnung an: Übersicht über ein Datenschutz-Managementsystems, Kap. 10.2, S.202, Abb. 80

[36] [DED] Vgl. Definition Datenschutzmanagement [online]

3 Methoden

Das folgende Kapitel gibt einen Überblick über die im Rahmen der Durchführung der Bachelorarbeit verwendeten Methoden, welche als Grundlagen zum Aufbau eines Datenschutzmanagements dienen. Für das bessere Verständnis für die Durchführung der benötigten Analysen und der Implementierung des Datenschutzmanagements wird zuerst ein mittelständisches Beispielunternehmen beschrieben. Weiterführend werden zwei Methoden erläutert, welche sich als sehr nützlich für Schwachstellenanalysen und kontinuierlicher Weiterentwicklung erwiesen haben.

Im ersten Unterkapitel 3.1 wird beispielhaft ein mittelständisches Unternehmen dargestellt. Als Erstes wird der grundsätzliche Aufbau und die Hierarchie des Unternehmens analysiert. Da Informationen über die Verarbeitungsvorgänge im Unternehmen benötigt werden, wird die Ablauforganisation der Abteilungen beschrieben und ausgewertet. Als letztes wird die technische Netzwerkumgebung anschaulich dargestellt und die Notwendigkeit erläutert.

Das zweite Unterkapitel zu 3.2 GAP-Analyse beschreibt die verwendete GAP-Analyse, welches als Management-Instrument zur Analyse der Schwachstellen auf strategischer und operativer Ebene eingesetzt werden kann.

Das letzte Unterkapitel 3.3 PDCA-Zyklus erläutert den verwendeten PDCA-Zyklus zur kontinuierlichen Verbesserung des Datenschutzes im Unternehmen.

3.1 Beispiel für ein mittelständisches Unternehmen

Zur besseren Veranschaulichung und zum Vergleich zu anderen Unternehmen wird in diesem Projekt die E-Tech GmbH beschrieben. Bei einem mittelständischen Unternehmen handelt es sich nach der Definition um ein Unternehmen, welches zwischen 50 und 250 Mitarbeiter beschäftigt oder einen Jahresumsatz von einer Millionen Euro bis 50 Millionen Euro erwirtschaftet. Die E-Tech GmbH ist ein mittelständisches Unternehmen mit Sitz in Köln. Sie beschäftigt 150 Mitarbeiter und erwirtschaftet einen Jahresumsatz von 15 Millionen Euro. Zu ihrem Kerngeschäft gehören die Herstellung und der Verkauf von speziellen Elektronikkleinteilen. Der Verkauf erfolgt sowohl an Business-Partner als auch an Privatkunden.

3.1.1 Analyse Aufbauorganisation

Die Analyse der Aufbauorganisation kann durch eine strukturierte Unternehmensbeschreibung oder durch eine grafische Darstellung erfolgen. Um den Aufbau des Unternehmens zu bestimmen, wird zuerst ein Organigramm verwendet. Ein Organigramm stellt die internen Strukturen einer Organisation in einer klaren visuellen Darstellung dar. In diesem Falle wird ein einfaches Organigramm aus Abteilungen erschaffen. Zur besseren Verdeutlichung sollten in einem Organigramm auch direkt die Ansprechpartner abgebildet sein. Da es sich um ein Beispielunternehmen handelt, wird in dieser Arbeit auf die Abbildungen der Mitarbeiter verzichtet.

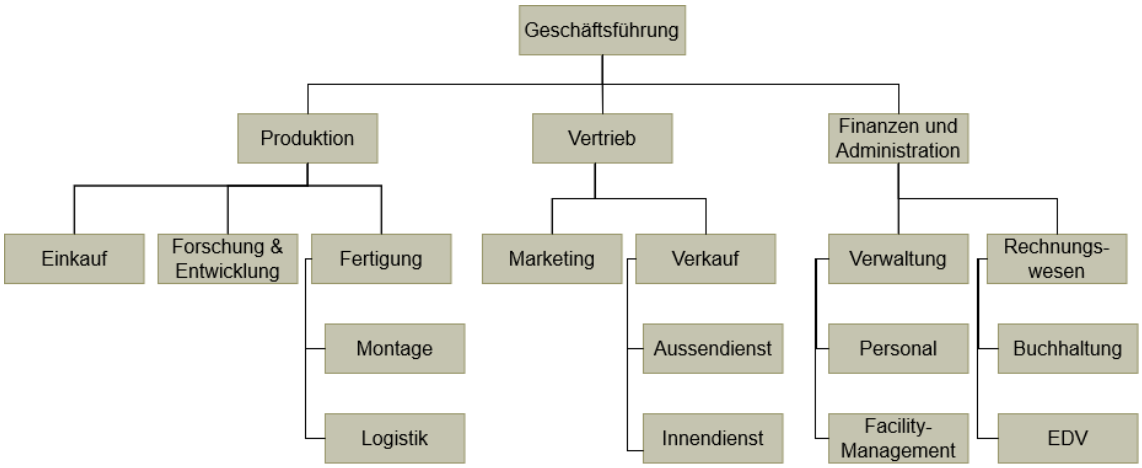

Abbildung 4: Organigramm

Als weiteres Mittel zur Analyse der Organisation dient die Unternehmensbeschreibung. Aus dem Organigramm (siehe Abbildung 4: Organigramm) können wir bereits ablesen, welche Abteilungen vorhanden sind. Eine folgende Beschreibung der Abteilungen hilft, den Unternehmensaufbau besser zu verstehen.

Unternehmensbeschreibung

Die Geschäftsführung der E-Tech GmbH besteht aus dem CEO, CMO und CFO. Der CEO (Chief Executive Officer) ist der Vorsitzender der Geschäftsführung und verantwortlich für alle Rechtsbelange. Der CMO (Chief Marketing Officer) ist Verantwortlicher für den Vertrieb und das Marketing. Der CFO (Chief Financial Officer) ist Finanzvorstand und verantwortlich für die Interessen von Finanzen, den Einkauf und die Logistik.

Die Produktion des Unternehmens gliedert sich in den Einkauf, die Forschung und Entwicklung und die eigentliche Fertigung des Produktes. Der Einkauf ist für die Beschaffung der Rohstoffe und den Kontakt mit Lieferanten zuständig. Die Forschung und Entwicklung entwickeln neue Produkte. Die Fertigung teilt sich in die eigentliche Montage der Endprodukte und die anschließende Logistik.

Der Vertrieb spaltet sich in das Marketing und den Verkauf mit dem Innendienst und dem Außendienst. Das Marketing ist zuständig für alle Werbemaßnahmen, wie Werbekampagnen, Social-Media-Auftritte oder auch Direktwerbungen. Da der Verkauf B2B und B2C erfolgt, trennt sich die Abteilung in Innendienst und Außendienst. Der Innendienst ist für den Vertrieb von Produkten an Privatkunden zuständig und der Außendienst für den Handel mit Businesskunden.

Die Abteilung Finanzen und Administration unterteilt sich in die Verwaltung und das Rechnungswesen. Die Personalverwaltung ist zuständige für alle Belangen um die Mitarbeiter, wie Recruiting, Urlaubsplanung oder die allgemeine Personalverwaltung. Das

Facility-Management kümmert sich um die Technik der Fertigungsmaschinen, sowie um alle Räumlichkeiten, sowie den Zutrittsschutz. Das Rechnungswesen ist mit der Buchhaltung für alle finanziellen Angelegenheiten zuständig. Da die EDV-Abteilung in finanzieller Sicht stark vom Rechnungswesen abhängig ist, untersteht sie derzeitig der Abteilung Rechnungswesen. Der Aufgabenbereich der EDV-Abteilung liegt in der Verwaltung aller systemtechnischen Geräten, der Gewährleistung des Schutzes der Daten auf technologischer Ebene und als Hilfestelle für alle technischen Fragen.

3.1.2 Analyse Ablauforganisation

Um den Ablauf der Organisation und der einzelnen Abteilungen zu verstehen, ist es wichtig, eine geeignete Struktur für die Prozessanalyse zu finden. Einerseits können durch eine Prozessanalyse Fehler und Probleme besser erkannt werden. Anderseits lassen sich Prozesse bei genauer Betrachtung verbessern. Für das Datenschutzmanagement müssen alle Prozesse, welche sich mit der Erhebung oder Verarbeitung personenbezogenen Daten befassen, betrachtet werden.

Eine häufig verwendete Methodik zur Prozessbeschreibung sind Prozessmodelle. „*Prozessmodelle sind vereinfachte Abbildungen von Prozessen einer Organisation. Sie stellen die chronologisch-sachlogische Abfolge von Funktionen beziehungsweise Tätigkeiten dar. Prozessmodelle können, je nach Zielstellung, in unterschiedlichem Detaillierungsgrad und Umfang modelliert werden. Aufgrund der Komplexität können meist nicht alle zu betrachtenden Prozesse in einem Prozessmodell dargestellt werden*.“[37] Zur Auswahl stehen einfache Flussdiagramme, Ereignisprozessketten und das Business Process Model and Notation (BPMN). Das zurzeit aktuelle BMPN in der Version 2 ist der führende Standard zur Erstellung von Geschäftsprozessen in der IT und wird von der Organisation Object Management Group bereitgestellt. Es bietet die Möglichkeit, Geschäftsabläufe standardisiert und in einer grafischen Notation darzustellen und somit einfacher zu verstehen.[38] Weiterhin werden direkt Datenobjekte und Datenflüsse beschrieben, welche die Umsetzung des Datenschutzmanagements weiter erleichtern.

Als Beispiel (Abbildung 10: Anhang: Beispiel BPMN2) wird aus der Abteilung Verkauf die Auftragsbearbeitung behandelt. Die Auftragsbearbeitung nimmt den Auftrag an und erhebt und verarbeitet in diesem Schritt bereits personenbezogene Daten, welche sich im Datenobjekt Auftrag befinden. Der Auftrag wird ausgeführt und die Lieferung erfolgt. Wenn der Auftrag beendet ist, übergibt die Auftragsverarbeitung die Daten an das Finanzwesen. In diesem Falle werden personenbezogene Daten abteilungsübergreifend verarbeitet. Anschließend wird eine Rechnung als Datenobjekt ausgestellt und dem Kunden übergeben. Je nach Übertragungsweg sind unterschiedliche Schutzmaßnahmen zu treffen. Die Zahlung wird getätigt und danach von dem Finanzwesen überprüft.

[37] [BBH] Vgl. Prozessmodelle, Kap. 6.2.4, S.270

[38] [OMG] BPMN2 [online]

In diesem Beispiel können bereits mindestens drei Verarbeitungsvorgänge im Vertrieb und zwei im Finanzwesen identifiziert werden. Diese können nachfolgend ins Verzeichnis von Verarbeitungstätigkeiten übertragen und weiter analysiert werden.

3.1.3 Netzwerk

Zur Unterstützung der Datenschutzdokumentation, sowie der Identifizierung möglicher technischer Maßnahmen sollte eine IT-Dokumentation vorhanden sein. Ein Netzwerkplan ist die Aufzeichnung des IST-Zustands eines Unternehmensnetzwerkes. Er enthält in tabellarischer, grafischer und dokumentarischer Form alle Informationen über die gesamte Netzwerkinfrastruktur des Betriebs. Neben der standortspezifischen Hardware sollten auch die eingesetzten Softwareanwendungen, Internetzugänge und Sicherheitsvorkehrungen aufgelistet werden. Durch die Dokumentation können einerseits Schwachstellen schneller aufgedeckt werden, anderseits bringt diese auch einen wirtschaftlichen Aspekt mit. Neuinvestitionen können zielgerechter geplant und Zeit, sowie Kosten bei der Umsetzung der geplanten Anforderungen des Gesetzgebers gespart werden.

Aus datenschutzrechtlicher Sicht können mithilfe einer IT-Dokumentation folgende Fragestellungen bereits beantwortet werden:

- Welche Systeme befinden sich im Einsatz?
- Wo werden Daten gespeichert?
- Welche Daten werden durch wen verarbeitet?
- Wer ist für die Verarbeitung verantwortlich und wer ist beteiligt?
- Welche externen Faktoren sind betroffen?

Im Falle der E-Tech GmbH wurde ein beispielhafter Netzwerkplan (Abbildung 9: Anhang: Netzwerkdiagramm) und eine Auflistung der eingesetzten Hard- und Software (Anhang 4: Netzwerkdokumentation E-Tech GmbH) erstellt. Durch diese Beispiele können bereits die oben genannten Fragestellungen im Datenschutz beantwortet werden. Weiterhin lassen sich technischen Maßnahmen, wie Firewall- oder Backup-Systeme identifizieren.

3.2 GAP-Analyse

Die GAP-Analyse, auch Lückenanalyse genannt, ist ein Management-Instrument zur Identifizierung strategischer und operativer Lücken und wurde von *Igor H. Ansoff* entwickelt. Mithilfe der GAP-Analyse lassen sich Abweichungen zwischen geplanten und voraussichtlich zu erwartenden Entwicklungen ermitteln. Ihren Ursprung findet die GAP-Analyse im Bereich des Finanzcontrollings, allerdings kann die Methode auch in anderen Bereichen eingesetzt werden.[39]

In diesem Projekt wird die bestehende Infrastruktur eines Unternehmens gegen einen Standard, die DSGVO, geprüft.

[39] [SCB] Vgl. Strategische Controllinginstrumente, Kap.2.6.2, S. 180-183

Die nachfolgende Abbildung (Abbildung 5: GAP-Analyse) zeigt die Vorgehensweise der DSGVO-Prüfung des TÜV Rheinlands.

Abbildung 5: GAP-Analyse[40]

Ablauf der GAP-Analyse

Der Ablauf gliedert sich von der Analyse bereits bestehender Dokumentation und technischen Maßnahmen bis hin zu Risikobewertungen und einem Abschlussbericht mit möglichen Verbesserungsvorschlägen.

Im ersten Schritt wird eine IST-Analyse aller bereits vorhandenen Dokumentationen durchgeführt. Neben den wesenhaften Datenschutzdokumentationen, wie Verarbeitungsverzeichnis oder Auftragsverarbeitungsverträgen, sollten auch IT-Dokumentationen, Notfallpläne, Unternehmensleitlinien, o.Ä. überprüft werden.

Der zweite Schritt findet auf persönlicher Ebene durch Interviews mit Geschäftsführung und Ansprechpartnern der Fachabteilungen statt. Durch die persönlichen Gespräche kann das Empfinden des Datenschutzes auf Mitarbeiterebene analysiert werden und bereits das Bewusstsein für den Datenschutz erhöht werden.

Folgend werden alle implementierten technischen Maßnahmen und IT-Systeme hinsichtlich ihrer Datenschutzkonformität analysiert. Die Prüfung findet auf technischer Ebene in Absprache mit den jeweiligen IT-Abteilung statt.

Anschließend folgt eine Risikoklassifizierung und Bewertung über die gesichteten Befunde. Auf diese Weise kann eine Priorisierung der empfohlenen Maßnahmen erfolgen.

Abschließend wird ein Abschlussbericht mit empfohlenen Maßnahmen und ein Behebungsplan erstellt.[41]

[40] [TÜV] GAP-Analyse [online]

[41] [TÜV] Vgl. Ablauf GAP-Analyse [online]

3.3 PDCA-Zyklus

Der PDCA-Zyklus, auch Deming-Kreis genannt, wurde von *William Edwards Deming* entwickelt und beschreibt einen vierstufigen Regelkreis zur kontinuierlichen Verbesserung. Dieser Prozess erreicht durch ständiges Wiederholen eine Verbesserung von Produkten, Dienstleistungen oder Prozessen. Aufgeteilt wird der PDCA-Zyklus (Abbildung 6: Deming-Kreis / PDCA-Zyklus) in die vier Bereiche Planung, Durchführung, Überprüfung und Handlung. Meist wird der Prozess im Qualitätsmanagement verwendet. Auf Grund dessen, dass der Datenschutz im Unternehmen ein kontinuierlicher Prozess darstellt, ist der PDCA-Zyklus nützlich für die Umsetzung und das Aufrechthalten der Standards.

Gemäß *Deming* kann grundsätzlich jede Tätigkeit als ein eigenständiger Prozess interpretiert werden, welcher im Rahmen des kontinuierlichen Verbesserungsprozesses optimiert werden kann.

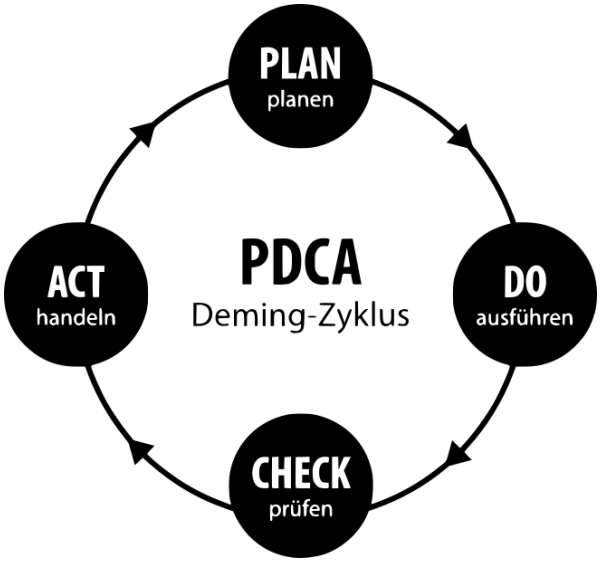

Abbildung 6: Deming-Kreis / PDCA-Zyklus

In den vier Zyklus-Phasen Planen (=Plan), Umsetzen (=Do), Überprüfen (=Check), Handeln / Verbessern (=Act) wird ein Geschäftsprozess systematisch analysiert und optimiert.

Dabei wird in der ersten Phase eine Analyse des IST-Zustandes durchgeführt, als Basis für den zu entwickelnden Verbesserungsplan. Die Analyse kann beispielsweise über Datenerhebungen oder Datenauswertungen erfolgen. Es sollte jedoch beachtet werden, dass aus dieser Analyse realistische Ziele zur Verbesserung abgeleitet werden können sollten. Im Anschluss an die Planung erfolgt die Umsetzung. Dazu werden die relevanten Mitarbeiter mit dem zuvor entwickelten Verbesserungsplan und den enthaltenen Zielen vertraut gemacht und das Konzept umgesetzt. Um in der dritten Phase des PDCA-Zyklus überprüfen zu können, ob die in der Planung festgelegten Ziele erreicht wurden, müssen entsprechende Daten erfasst und ausgewertet werden. Abschließend wird ein SOLL-IST-Abgleich durchgeführt. Stimmt der SOLL-Zustand mit den geplanten Zielen überein, ist eine Standardisierung anzustreben. Stimmen SOLL und IST noch nicht überein, müssen die Phasen „Planen“ und „Umsetzen“ so lange durchlaufen werden, bis eine ausreichende Verbesserung erreicht wurde. Sobald eine Verbesserung umgesetzt und standardisiert wurde, können darauf aufbauend weitere Optimierungsmöglichkeiten angestoßen werden. Dadurch werden die vier Zyklus-Phasen dauerhaft durchlaufen und der Vorgang ist als ein kontinuierlicher Verbesserungsprozess zu verstehen.[42]

[42] [EMG] Vgl. PDCA-Zyklus, Kap. 3.1.3, S.118-120

4 Analyse und Implementierung des DSM

Nachdem die theoretischen Grundlagen für die Umsetzung erläutert und die Methoden gewählt wurden, kann die Analyse und die Implementierung des Datenschutzmanagements erfolgen.

Die Ausgangssituation des Beispielunternehmens ist, dass zurzeit kein bzw. nicht geeigneter Datenschutz vorhanden ist. Da das Unternehmen seinen Sitz in der Europäischen Union hat, sind auch die europäischen Gesetze anzuwenden.

Das folgende Kapitel gibt einen Überblick über die im Rahmen der Durchführung des Projektes erzeugten Analysen und Implementierungen des Datenschutzmanagements.

Im ersten Unterkapitel zu 4.1 wird die Aufbauorganisation erläutert. Dementsprechend werden zuerst die unternehmensweiten Datenschutzziele definiert und eine Datenschutz-Governance-Struktur aufgebaut. Hierbei lassen sich bereits Datenschutzleitlinien und Richtlinien ableiten.

Das zweite Unterkapitel zu 4.2 beschreibt die Ablauforganisation. Zuerst wird die Verarbeitung personenbezogener Daten mit dem Verarbeitungsverzeichnis analysiert. Aufbauend folgen das Risikomanagement und eine Datenschutzfolgeabschätzung. Abschließend wird der Umgang mit Datenschutzverletzungen festgelegt.

Anschließend werden im Unterkapitel zu 4.3 die Auftragsverarbeiter analysiert und entsprechende Maßnahmen, wie Auftragsverarbeitungsvertrag, angelegt.

Folgend in Unterkapitel 4.4 wird der Kunden- und Mitarbeiterdatenschutz erläutert. In diesem Kapitel geht es vor allem um den Schutz der natürlichen Personen, wie Mitarbeiter, Kunden und Bewerbern.

Das Unterkapitel zu 4.5 beschreibt die technisch-organisatorischen Maßnahmen. Zuerst wird das Sicherheitsmanagement mit seinen Schutzzielen erläutert. Anschließend werden zuerst geeignete technischen Maßnahmen vorgestellt. Abschließend folgen organisatorische Maßnahmen.

Im Unterkapitel zu 4.6 werden der Datenschutzbeauftragte und seine Aufgaben vorgestellt.

Im letzten Unterkapitel zu 4.7 erfolgt schlussendlich die Datenschutzdokumentation und eine Dokumentation der Aufwände und Kosten, welche für die Projektdurchführung aufgebracht werden müssen.

4.1 Aufbauorganisation

4.1.1 Datenschutzziele

Für den Datenschutz, so wie auch für andere Unternehmensbereiche, sollte die Geschäftsführung Ziele definieren. Die Datenschutzziele sollten als Teil der Unternehmensziele ganzheitlich betrachtet werden, denn „*solange der Datenschutz nicht Teil der gemeinsamen Werte und Praktiken einer Organisation wird, und solange die Verantwortung für den Datenschutz nicht ausdrücklich zugewiesen wird, ist die tatsächliche Einhaltung der Vorschriften gefährdet und es wird weiterhin zu Pannen kommen*“[43].

Für die Zieldefinition ist wichtig, welche internen und externen Anforderungen maßgeblich sind. Hierunter fallen verschiedenste Gesetze und externe und interne Vorschriften und Regelungen. Die Ziele sollten mindestens eine größtmögliche Compliance mit den gesetzlichen Anforderungen anstreben. Ferner können aber auch über die gesetzlichen Anforderungen hinaus zusätzliche Maßnahmen angestrebt werden, welche als Wettbewerbsvorteil ausgelegt werden können. Zu beachten ist das Spannungsfeld zwischen verschiedenen Unternehmenszielen. Es können zum Beispiel Konflikte zwischen den Marketingzielen und Datenschutzzielen erzeugt werden.[44]

Für die E-Tech GmbH wurden in Zusammenarbeit mit der Geschäftsführung folgende Datenschutzziele vereinbart:

- Schaffung und Erhalt von Vertrauen und Respekt vor den Erwartungen des Einzelnen zum Thema Datenschutz
- Einhaltung der Zweckbindung und der Richtigkeit für die vom Kunden zur Verfügung gestellten Daten
- Verhinderung von Verletzung der Privatsphäre
- Einhaltung aller nationalen und internationalen Vorschriften
- Vorrang der gesetzlichen Vorgaben vor betrieblichen Entscheidungen

4.1.2 Datenschutz-Governance-Struktur

Zur Sicherstellung des Datenschutzes muss im Unternehmen eine geeignete operative Struktur erstellt werden. Die externe Verantwortung liegt zwar beim Verantwortlichen bzw. der Geschäftsführung, jedoch kann dieser die interne Verantwortung an eine geeignete Struktur abgeben. Die Datenschutz-Governance-Struktur beschreibt ein Steuerungselement aus verschiedenen Rollenverteilungen und Aufgaben. Sie kümmert sich um die Aufgaben rund um den Datenschutz und steht als beratende Stelle zur Verfügung.

Aufgrund der Tatsache, dass die E-Tech GmbH zur Benennung eines Datenschutzbeauftragten verpflichtet ist, wird ein bereits tätiger Mitarbeiter zum Datenschutzbeauftragten ausgebildet. Dieser kann seine bisherigen Tätigkeiten im Einklang mit der Tätigkeit

[43] [AWP] Die Zukunft des Datenschutzes, S.19

[44] [DCD] Vgl. Datenschutzzeile, Kap. 4.1, S.42-43

als Datenschutzbeauftragter im 40% zu 60% Arbeitszeit-Modell verrichten. Da es zu Konflikten zwischen der Beurteilung der Aufgaben als Datenschutzbeauftragter in verschiedenen Abteilungen kommen kann, wird ein Mitarbeiter benötigt, welcher zwar mit sensiblen, aber nicht mit personenbezogenen Daten arbeiten muss. Somit fallen die Abteilungen Vertrieb, Finanzen und Administration aus der Auswahl heraus. Ein Mitarbeiter des Forschungs- und Entwicklungsteam wird ausgewählt.

Ein weiteres Mitglied der Datenschutz-Governance-Struktur ist der Verantwortliche für den Datenschutz. Im Idealfall ist dieser ein Mitglied der Geschäftsführung und somit mit einer Entscheidungs- und Vollzugskompetenz ausgestattet. Da auch verschiedene Ressourcen zur Verfügung gestellt werden müssen, wird in der E-Tech GmbH der CFO (Chief Financial Officer) als Verantwortlicher für den Datenschutz ausgewählt.

Das letzte geforderte Mitglied in der Datenschutz-Governance-Struktur ist der Datenschutzkoordinator. Der Datenschutzkoordinator entlastet und vertritt den Datenschutzbeauftragten in seiner Tätigkeit. Meistens übernimmt er leichtere Routinearbeiten oder die Koordination von Anfragen. In der E-Tech GmbH wird ein Angestellter aus der Abteilung Verwaltung berufen, da dieser bereits in seiner Haupttätigkeit Verwaltungsaufgaben erledigt.

Weitere Datenschutz-Multiplikatoren können frei gewählt werden und stehen als beratende Mitglieder in der Datenschutz-Governance-Struktur zur Verfügung. Es ist ratsam einen Mitarbeiter aus der EDV- Abteilung als weiteres Mitglied aufzunehmen, da dieser die Erfahrung zur Umsetzung von technischen Maßnahmen mitbringt.

Für die Datenschutz-Governance-Struktur ist ein Dokument (Anhang 5: Datenschutz-Governance-Struktur) zu erstellen, welches die aktuellen Mitglieder und ihre Kontaktdaten und Aufgabenbereiche festhält.

4.1.3 Datenschutzleitlinien und Richtlinien

Eine Datenschutzleitlinie ist eine Selbstverpflichtung des Unternehmens zur Umsetzung der Datenschutzziele. Sie gibt den strategischen Rahmen vor, wie der Datenschutz operativ umzusetzen ist. Sie enthält jedoch keine detaillierten Handlungsweisen, sondern ist als Teils des Unternehmensleitbildes zu verstehen. Alle Mitarbeiter müssen sich somit an die Datenschutzleitlinien halten und den Erfolg der Datenschutzziele anstreben. Für den Aufbau der Leitlinien bietet sich folgende Struktur[45] an:

- Kurzbeschreibung der Datenschutzleitlinie
- Einführung / Motivation
- Anwendungsbereich
- Benennung der Vorschriften (gesetzlich) und sonstige Grundlagen für die Ableitung der Datenschutzziele
- Datenschutzziele des Unternehmens

[45] [DCD] Datenschutzstrukturen, Kap.4, S.50

- Governance-Struktur (Rollen und Verantwortlichkeiten)
- Verweis auf die operative Umsetzung (z.B. mittels Datenschutzmanagement)
- Datenschutzkonforme Verarbeitung
- Sicherstellung der Betroffenenrechte
- Handhabung von Datenschutzverletzungen
- Kontrolle und Überwachung
- Konsequenzen bei Verstößen
- Dokumentenlenkung (Eigentümer, Revisionszyklen, Definitionen etc.)

Änderungen an der Datenschutzleitlinie sind an die Zustimmung der Geschäftsführung gebunden. Somit hat es sich als praktikabel erwiesen, die Datenschutzleitlinie um eigenständige Richtlinien zu erweitern und die Datenschutzleitlinie auf diese zu verweisen. Die Richtlinien können hierdurch häufiger angepasst werden und benötigen keine Zustimmung der Geschäftsführung. Nutzungsrichtlinien, wie die Nutzung des Unternehmensnetzwerkes oder mobiler Endgeräte haben sich als sinnvoll erwiesen. Für die E-Tech GmbH wurde eine entsprechende Datenschutzleitlinie (Anhang 2: Datenschutzleitlinie) erstellt.

4.2 Ablauforganisation

4.2.1 Verarbeitung personenbezogener Daten

Für die Ablauforganisation ist es von hoher Bedeutung, dass alle Verarbeitungsvorgänge mit den Vorschriften der Datenschutzgrundverordnung konform sind. Somit muss zuallererst jeder Verarbeitungsvorgang auf folgende Datenschutzkonformität gegengeprüft werden:

- Einhaltung der Datenschutzgrundsätze (DSGVO Art. 5 Abs. 1,2)
  Unterliegt der Verarbeitungsvorgang der Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität, Vertraulichkeit und Rechenschaftspflicht?
- Geeignete Rechtmäßigkeit für die Verarbeitung (DSGVO Art. 6)
  Auf welcher Grundlage findet die Verarbeitung statt?
- Transparenz bei der Erhebung (DSGVO Art. 12)
  Wurden Informationen (z.B. Datenschutzhinweisen) für betroffene Personen bereitgestellt?
- Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen (DSGVO Art. 25 Abs.1,2)
  Die Datenschutzgrundsätze und Betroffenenrechte sind geeignet umgesetzt?
- Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen (DSGVO Art. 32)
  Es liegen geeignete technische und organisatorische Maßnahmen vor?
- Datenschutzkonforme Auftragsverarbeitung (DSGVO Art. 28)

Auftragsverarbeiter sind ausreichend geprüft und Auftragsdatenverarbeitungsverträge mit technischen und organisatorischen Maßnahmen liegen vor?

- Übermittlung personenbezogener Daten in Drittländer (DSGVO Art. 44)
  Werden Daten in Drittländer übermittelt?
- Dokumentation im Verarbeitungsverzeichnis (DSGVO Art. 30)
  Ist der Verarbeitungsvorgang ausreichend dokumentiert?[46]

4.2.2 Verarbeitungsverzeichnis

Die E-Tech GmbH ist zur Führung eines Verarbeitungsverzeichnisses nach Art. 30 DSGVO verpflichtet. Aus diesem Grunde wurden bereits alle Verarbeitungsvorgänge durch die dazugehörigen Abteilungen zusammengefasst bzw. liegen im grafischen Business Process Model und Notation in der Version 2 (BPMN2) vor.

Die Erstellung und Pflege eines Verarbeitungsverzeichnisses ist ein kontinuierlicher Prozess und unterliegt dem PDCA-Zyklus. Demzufolge sollte das Verarbeitungsverzeichnis mindestens einmal im Jahr aktualisiert werden. Nach folgendem Muster[47] kann jeder Prozess dokumentiert werden:

1. Bezeichnung der Verarbeitung mit fortlaufender Nummerierung
2. Zwecke der Verarbeitung
3. Beschreibung der Kategorien personenbezogener Daten
4. Beschreibung der Kategorien betroffener Personen
5. Kategorien von Empfänger, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
6. Übermittlung an Drittländern oder internationalen Organisationen
7. Vorgesehene Fristen zur Löschung der verschiedenen Datenkategorien
8. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

Als Beispiel für die E-Tech GmbH wurden aus der Abteilung Verkauf das BPMN2 „Auftragsverarbeitung“ (Abbildung 10: Anhang: Beispiel BPMN2) analysiert und bereits drei Verarbeitungsvorgänge in der Abteilung Verkauf herausgefiltert. Die Verarbeitungsvorgängen sind „Auftrag entgegennehmen“, „Auftrag ausführen“ und die anschließende „Lieferung“. Der Verarbeitungsvorgang „Auftrag entgegennehmen“ wurde in geeigneter Form als erster Prozess ins Verarbeitungsverzeichnis (Anhang 7: Verarbeitungsverzeichnis) überführt.

[46] [DCD] Vgl. Datenschutzprozesse, Kap. 5.1.1, S.51

[47] [DBH] Vgl. Verzeichnis von Verarbeitungstätigkeiten, Kap. 27, S.151-155

4.2.3 Risikomanagement

Der Verantwortliche muss bei jeder Verarbeitung unter Berücksichtigung des Zwecks, Umfangs, Art, Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen durch Auswahl von geeigneten technisch-organisatorischen Maßnahmen sicherstellen. Das Datenschutzrisikomanagement ist weitläufig identisch mit dem normalen Risikomanagement.

Im ersten Schritt werden mögliche Risikoquellen analysiert. Diese können in interne, externe, menschliche und nichtmenschliche Quellen zusammengefasst werden.

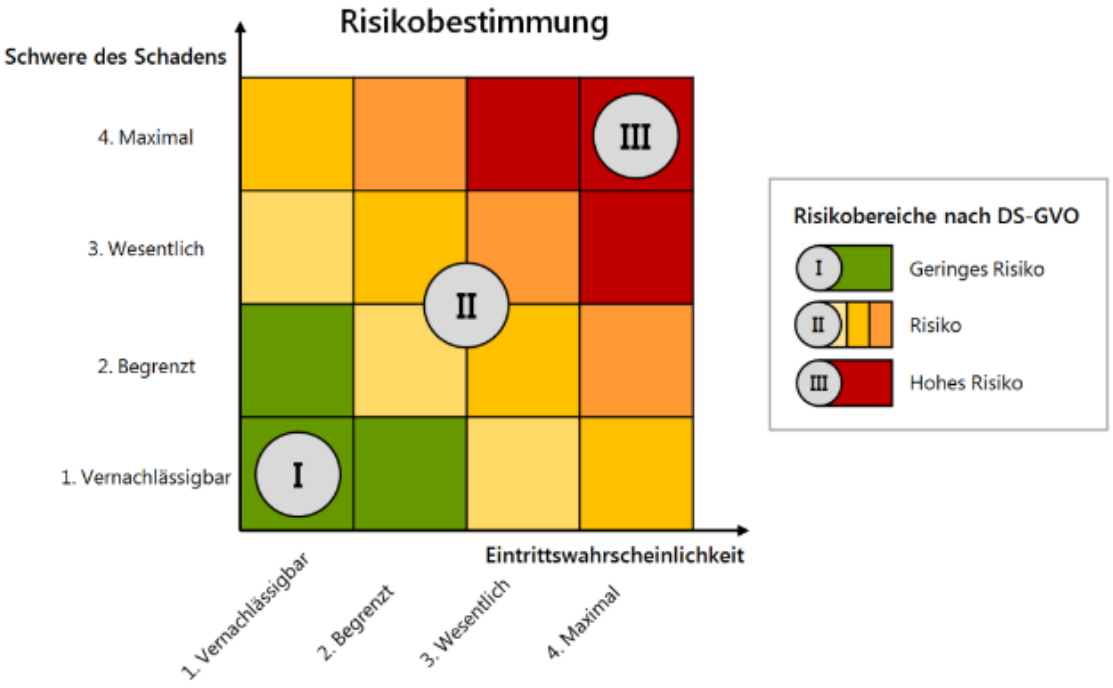

Abbildung 7: Allgemeine Matrix zur Risikobestimmung[48]

Nachfolgende beginnt die Risikobeurteilung oder auch Risikoanalyse. Anhand von Schadenskategorien (ErwGr. 75 DSGVO) kann die Schadenshöhe (Tabelle 5: Anhang: Bewertung Schadenshöhe) bestimmt werden. Die Eintrittswahrscheinlichkeit wird durch eine Trendbeurteilung der Zukunft und einen Blick in die Vergangenheit (Tabelle 6: Anhang: Bewertung Eintrittswahrscheinlichkeit) bestimmt. Die Formel zur Betrachtung ergibt sich somit aus den Faktoren „Schwere des Schadens“ und „Eintrittswahrscheinlichkeit“:

$$Risiko = Schwere\ des\ Schadens * Eintrittswahrscheinlichkeit$$

Als letzten Schritt werden geeignete Abhilfemaßnahmen auswählt. Ein geringes Risiko kann in den meistens Fällen vernachlässigt werden. Ein mittleres Risiko sollte geeignete

[48] [LDB] Risikobeurteilung, Kap. 4.2, S.18

technische und organisatorischen Maßnahmen zur Abhilfe bereitstellen. Bei einem hohen Risiko ist der Datenschutzbeauftragte zur Unterstützung hinzuzuziehen und eine Datenschutzfolgeabschätzung muss in Betracht gezogen werden.

4.2.4 Datenschutzfolgeabschätzung

Die Datenschutzfolgeabschätzung ist eine erweiterte ausführliche Risikoanalyse und benötigt die Hilfe der an der Verarbeitung beteiligten Personen. Es müssen nicht für alle im Verarbeitungsverzeichnis aufgeführten Verarbeitungstätigkeiten eine Datenschutzfolgeabschätzung durchgeführt werden. Die erste Voraussetzung ist ein durch das Risikomanagement bestimmtes hohes Risiko für die Betroffenen. Sollte dies vorhanden sein, schreitet der Verarbeitungsvorgang in eine Schwellenwertanalyse über.

Schwellenwertanalyse

Grundsätzlich ist eine Datenschutzfolgeabschätzung für folgende Szenarien notwendig:

1. Die Verarbeitung, insbesondere der Einsatz von neuerer Technologie, hat in der Art, dem Umfang, der Umstände und der Zwecke der Verarbeitung ein sehr hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge.[49]
2. Die Verarbeitung fällt unter ein Regelbeispiel der in der Datenschutzgrundverordnung[50] ausgeführten Verarbeitungsvorgängen:
    a. eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.
    b. eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
    c. eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
3. Die Verarbeitung befindet sich auf einer von der zuständigen Aufsichtsbehörde veröffentlichten Liste zur Durchführung einer Datenschutzfolgeabschätzung, auch DSFA Blacklist genannt.

Kann mindestens einer der vorstehenden Punkte mit „Ja“ beantwortet werden, ist eine Datenschutzfolgeabschätzung durchzuführen. Ist keine Datenschutzfolgeabschätzung durchzuführen, ist dies wiederrum auch zu dokumentieren.

[49] [DSGVO] Vgl. Datenschutzfolgeabschätzung, Art.35 Abs. 1

[50] [DSGVO] Datenschutzfolgeabschätzung, Art.35 Abs.3

Durchführung der Datenschutzfolgeabschätzung

Bei der Durchführung der Datenschutzfolgeabschätzung stellt der Datenschutzbeauftragte zu Beginn ein Datenschutzfolge-Team zusammen. Dieses analysiert den Verarbeitungsvorgang in Hinsicht auf Datenflüsse, Akteure, betroffene Personen, Auftragsdatenverarbeiter und Rechtsquellen.
Nachfolgend werden alle möglichen Risikoquellen und Risikoszenarien bestimmt und eine neue Risikoanalyse durchgeführt. Die Risikobehandlung kann entweder minimiert, eliminiert, übertragen oder akzeptiert werden. Die Akzeptanz und der Übertrag sollten jedoch bei einer Datenschutzfolgeabschätzung vermieden werden, da sonst das Risiko besteht, dass der Verarbeitungsvorgang nicht durchgeführt werden darf. Infolgedessen werden die bestimmten Abhilfemaßnahmen umgesetzt und eine weitere Risikoanalyse folgt. Bei erfolgreicher Minderung oder Eliminierung des Risikos kann die Datenschutzfolgeabschätzung abgeschlossen werden. Sollte weiterhin ein hohes Risiko bestehen ist die zuständige Aufsichtsbehörde zu informieren. Diese kann einerseits den Verarbeitungsvorgang dennoch erlauben oder den Vorgang sperren bzw. verbieten.

Gemäß PDCA-Zyklus ist die Datenschutzfolgeabschätzung regelmäßig zu überprüfen und gegebenfalls zu wiederholen. Bei der E-Tech GmbH wurde eine Praxisbeispiel (Anhang 8: Datenschutzfolgeabschätzung) zur Ortung von Kraftfahrzeugen umgesetzt.

4.2.5 Handhabung Datenschutzverletzung

Die Handhabung bei Datenschutzverletzungen wurde bereits im Praxisprojekt dargestellt und hier erneut aufgeführt:

Kommt es zu einer Sicherheitsverletzung bzw. Datenpanne, sollte schnell reagiert werden. Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Von der Entdeckung eines Sicherheitsverstoßes bis zur Übermittlung an den Vorgesetzen, Verantwortlichen und Datenschutzbeauftragten, welche die notwendigen Formalitäten erledigen, ist der Zeitraum sehr eng. Gegebenenfalls müssen auch die Betroffenen direkt kontaktiert werden.

Jede Sicherheitsverletzung sollte an den Verantwortlichen weitergeleitet werden. Im Einzelfall ist zu entscheiden, ob ein Verstoß meldepflichtig ist oder nicht. Beispiele für meldepflichtige Vorfällen sind die Preisgabe von Kunden oder Mitarbeiterdaten, Verlust von mobilen Datenträgern oder Systemen mit sensiblen Daten, Diebstahl oder auch der Angriff auf Kunden-, Mitarbeiter-, oder Mitgliedsdatenbanken.[51]

[51] [ICH] Verhalten bei Datenpannen, Kap. 2.2.6, S.14

Folgende Vorgehensweise bei einer Datenpanne bei der E-Tech GmbH wurde eingeführt:

Schritt 1: Kontakt zum Datenschutzbeauftragten aufnehmen

Der erste Ansprechpartner bei einer voraussichtlichen Datenpanne ist der Datenschutzbeauftragte. Dieser muss den Schaden einschätzen und die weiteren Schritte einleiten. Sollte kein Datenschutzbeauftragter zu erreichen sein, kann auch der zuständige Landesbeauftragte für Datenschutz um Rat gebeten werden.

Schritt 2: Überprüfung des Falls

Nicht jeder Schadensfall muss an die Aufsichtsbehörde weitergeleitet werden. Eine Einstufung des Risikos für die Rechte und Freiheiten der Betroffenen muss vorgenommen werden.

Ein geringes Risiko kann der Verlust eines Speichermediums darstellen, welches verschlüsselt und durch ein Passwort gesichert ist. Unbefugte können somit nicht an die Daten gelangen.

Ein mittleres Risiko zeichnet sich beispielsweise durch den Verlust und die Veröffentlichung von E-Mail-Adresslisten ab. Der Personenkreis ist zwar umfangreicher, doch sind E-Mail-Adressen weniger heikel als die Preisgabe von Kontakt- oder Adressdaten.

Ein hohes Risiko stell beispielsweise den Verlust von Bankverbindungen oder medizinischen Diagnosen dar. Diese Informationen gehören zu den sensiblen Informationen und die Betroffenen könnten umfangreiche Nachteile erlangen.

Generell gilt zu überprüfen, welche konkreten Daten verloren gegangen und wie viele Personen betroffen sind. Je höher die Anzahl an Betroffenen und Daten, desto größer das Risiko.

Schritt 3: Sofortige Gegenmaßnahmen ergreifen

Geeignete Gegenmaßnahmen werden sofort umgesetzt und getestet, ob das Risiko vermindert wurde.

Schritt 4: Meldung an die Aufsichtsbehörde

Bei mittleren und hohen Risiken erfolgt die Meldung an die Aufsichtsbehörde. Diese erfolgt in einem Zeitraum von 72 Stunden und beinhaltet Informationen über die Datenpanne, Anzahl der Personen, Art der Daten und welche Gegenmaßnahmen ergriffen wurden. Bei einer Verzögerung muss zusätzlich eine Begründung der Verzögerung dem Dokument beigefügt werden.

Schritt 5: Meldung an Betroffene

Bei einem hohen Risiko müssen zudem die Betroffenen über die Datenpanne informiert werden. Diese Benachrichtigung erfolgt, wenn hohe Risiken für die individuelle Freiheit oder persönlichen Rechte der Betroffenen bestehen. Bei geringem Risiko oder bei mittlerem Risiko durch Milderung geeignete Abhilfemaßnahmen entfällt die Pflicht.

Schritt 6: In Zukunft vorbeugen

Ein wichtiger Schritt nach der Datenpanne ist die genauere Analyse des Vorfalls und die Klärung, welche Vorkehrungen in Zukunft einen Vorfall vermeiden könnten. Je nach Vorfall können in Zukunft weitere Sicherheitsmaßnahmen umgesetzt oder die Schulungen der Beschäftigten erhöht werden.

4.3 Auftragsverarbeitung

Analyse

Die Kooperation mit anderen Unternehmen ist ein wichtiger Bestandteil der täglichen Arbeit eines Unternehmens. Für verschiedenste Zwecke werden andere Dienstleister beauftragt und benötigt. Um alle Auftragsdatenverarbeiter bzw. Dritte zu identifizieren, ist es notwendig, eine Aufstellung über alle Kooperation mit anderen Unternehmen oder Dienstleister zu bekommen. In welchem Format die Auflistung vorliegt, ist nicht wichtig. Es sollte nur eine allgemeine Auflistung mit möglichen Kontaktdaten und Aufgabenbereiche vorliegen.

In Falle der E-Tech GmbH konnten folgende Kooperationen identifiziert werden:

Dienstleister	**Auftragsverarbeitung liegt vor?**	**Begründung**
Externer Sicherheitsdienst	Ja	Verarbeitung durch Personenkontrollen
Hosting der Webseite	Ja	Verarbeitung von z.B. IP-Adresse
Cloud Systeme zur Kunden- und Personalverwaltung	Ja	Personenbezogene Daten liegen beim externen Dienstleister
Aktenvernichtung	Ja	Abfuhrdienstleister vernichtet sensible Daten
Marketingagentur zur Auswertung der Webseitenanalyse	Ja	Analyse von Benutzerverhalten
Anwalt	Nein	Fremde Fachleistung
Bankinstitut	Nein	Fremde Fachleistung
Externer EDV-Techniker	Ja	Ja, da der Zugriff auf personenbezogene Daten möglich ist.
Steuerberater	Nein	Fremde Fachleistung
Postdienst	Nein	Fremde Fachleistung
Personenbeförderung	Nein	Nein, da im Kern keine beauftragte Verarbeitung personenbezogener Daten, sondern der Auftrag zielt auf eine andere Tätigkeit.
Warenlieferung	Nein	Keine Verarbeitung von personenbezogenen Daten
Reinigungsdienstleister	Nein	Nein, da im Kern keine beauftragte Verarbeitung personenbezogener Daten, sondern der Auftrag zielt auf eine andere Tätigkeit.

Tabelle 1: Identifizierung Auftragsverarbeiter

Wie in der Tabelle (Tabelle 1: Identifizierung Auftragsverarbeiter) analysiert, sind nicht alle Kooperationen und Dienstleister direkte Auftragsverarbeiter. Wenn keine Auftragsverarbeitung vorliegt, muss das externe Unternehmen bei der Verwaltung von Auftragsdatenverarbeitungsverträgen auch nicht berücksichtigt werden. Steuerberater, Rechtsanwälte, Betriebsärzte, Postdienste und einige weitere Berufsgruppen zählen zu den fremden Fachleistungen. Sie sind selbst für die Daten verantwortlich und benötigen somit keinen Auftragsverarbeitungsvertrag. Personenbeförderung, Reinigungsdienstleister und Spediteure verarbeiten in der Beauftragung im Kern keine personenbezogenen Daten, sondern der Auftrag zielt auf eine Tätigkeit.[52]

Auftragsdatenverarbeitungsvertrag

Der Auftragsdatenverarbeitungsvertrag wird von der Seite des Auftragnehmers bereitgestellt. Allerdings liegt die Pflicht zum Abschluss eines datenschutzkonformen Auftragsverarbeitungsvertrags gleichermaßen beim Auftraggeber und Auftragnehmer. Somit sollte der Auftraggeber, auch wenn er selbst keinen Auftragsdatenverarbeitungsvertrag bereitstellen muss, ebenfalls Erfahrungen im Umgang mit den Verträgen nachweisen.

In einem Auftragsdatenverarbeitungsvertrag sind laut Datenschutzgrundverordnung[53] folgende Aspekte vertraglich zu regeln:

1. Der Gegenstand, die Dauer, die Art und der Zweck der Verarbeitung
2. Welche Arten und Kategorien personenbezogenen Daten werden verarbeitet
3. Welche Rechte und Pflichten dem Verantwortlichen zustehen
4. Der Umfang der Weisungsbefugnis beim Auftragnehmer
5. Ausstellung von Vertraulichkeitsverpflichtung für die befugten Personen
6. Angaben zu den technisch- organisatorischen Maßnahmen des Auftragsnehmers
7. Angaben über mögliche Subunternehmer oder Transfer in Drittstaaten
8. Unterstützung bei Anfragen von Betroffenen, der Sicherheit der Verarbeitung und bei Meldepflichtigen Datenschutzverletzungen, sowie Datenschutzfolgeabschätzungen
9. Regelung zur Löschung und/oder Rückgabe der personenbezogenen Daten nach Beendigung des Auftragsverhältnisses
10. Informationen zur Einhaltung des Datenschutzrechts bei Datenschutzverstößen
11. Regelung zum Nachweis der Einhaltung der genannten Pflichten

Die E-Tech GmbH ist grundsätzlich nicht dazu verpflichtet, einen eigenen Auftragsverarbeitungsvertrag zu erstellen, da sie keine Dienstleistungen für Dritte erbringt. Dennoch wird der E-Tech GmbH ein Auftragsverarbeitungsvertrag (Anhang 12: Auftragsdatenverarbeitungsvertrag) zur Verfügung gestellt, um die Auftragsverarbeitungsverträge kontrollieren zu können.

[52] [FHD] Vgl. Vereinbarung der Auftragsverarbeitung, S.611-618

[53] [DSGVO] Vgl. Art.28, Abs. 3

4.4 Kunden- und Mitarbeiterdatenschutz

4.4.1 Kundendatenschutz

Der Kundendatenschutz ist ein spezieller Prozess zur Sicherstellung der Betroffenenrechte natürlicher Personen. Immer mehr Kunden machen von ihren Betroffenenrechten Gebrauch. Eine korrekte und schnelle Beantwortung dieser Anfragen schreibt die Datenschutzgrundverordnung vor. Mindestens innerhalb eines Monats ist eine Betroffenenanfrage zu beantworten. Eine klare Richtlinie bzw. Handlungsempfehlung zum Verhalten bei Betroffenenanfragen kann eine schnellere Lösung vorsehen. Das Ziel bei der Entwicklung von Handlungsempfehlungen laut PDCA-Zyklus sind die Reduktion von Risiken für das Unternehmen und die Einhaltung von Vorschriften gemäß Datenschutzgrundverordnung.

Folgende Betroffenenanfragen[54] müssen behandelt werden, wobei das Verarbeitungsverzeichnis hierbei ein guter Anhaltspunkt zur Ermittlung der Datenverläufe ist:

Das Recht auf transparente Informationen sollte bereits durch Datenschutzhinweise oder einer Datenschutzerklärung beim Abschluss eines Vertrages mitgeliefert werden. Bei elektronischen Abschlüssen, beispielhaft bei der E-Tech GmbH durch ein Kontaktformular oder durch den Besuch des Onlineshops, besteht bereits eine Pflicht zur Führung einer Datenschutzerklärung.

Das Auskunftsrecht erfordert die Aufmerksamkeit des Datenschutzbeauftragten bzw. des Datenschutzkoordinators. Alle gespeicherten Daten des Kunden müssen ausgelesen und anschließend dem Kunden mitgeteilt werden.

Beim Recht auf Berichtigung werden die gespeicherten Daten korrekt geändert und dem Kunden anschließend eine Bestätigung zugesandt. Elektronische Angaben kann der Kunde bereits selbst im Onlineshop ändern.

Das Recht auf Datenübertragbarkeit wird häufig zum Wechseln von Vertragspartnern angefragt. Alle gespeicherten Daten werden in einem leicht verständlichen Format dem Kunden oder bei Anfrage dem neuen Vertragspartner mittgeteilt. Eine tabellarische Aufstellung hat sich in der Praxis bewährt.

Das Recht auf Widerspruch und das Recht auf Löschung können aus unterschiedlichen Gründen gebraucht werden. Somit ist eine individuelle Betrachtung der Anfrage notwendig. Bei einem Widerspruch ist der Zweck der Verarbeitung zu sperren. Bei einer Löschung müssen alle gespeicherten Daten, vorausgesetzt sie müssen nicht aufgrund anderer Gesetzesregelungen gesichert werden, umgehend gelöscht werden.

Für das Recht auf Einschränkung werden sogenannte Blacklists verwendet. Somit kann bei Werbeangeboten sichergestellt werden, dass ein Kunde bei Widerspruch oder Löschung nicht erneut kontaktiert wird.

[54] [DSGVO] Vgl. Rechte der betroffenen Personen, Kap. 3

Bei der Bearbeitung von Betroffenenanfragen ist immer sicherzustellen, dass der Kunde ausreichend informiert ist, da dieser eine Beschwerderecht bei der zuständigen Aufsichtsbehörde besitzt.

4.4.2 Arbeitnehmerdatenschutz

Arbeitnehmer gehören zur Gruppe der natürlichen Personen. Aus diesem Grunde gelten für sie die gleichen Rechte wie die oben beschriebenen Kundenrechte. Ferner sind Arbeitnehmer jedoch auch die größte Schwachstelle im Datenschutz. Aus diesem Grunde muss ein weitgehendes Datenschutzbewusstsein im Unternehmen geschaffen werden, indem alle Arbeiternehmer miteinbezogen werden.

Datenschutzschulung

Um das Datenschutzbewusstsein zu erhöhen, können verschieden Maßnahmen umgesetzt werden. Arbeitnehmer sollten sensibilisiert, geschult und anschließend auf die datenschutzkonforme Verarbeitung trainiert werden. Die Aufmerksamkeit kann durch geeignet Sensibilisierungen, wie Aushänge oder interne Informationen, erhöht werden. Geeignete Lösungen werden in Form einer jährlich angebotenen Datenschutzschulung vermittelt. Anschließend werden die Lösungen durch verschiedene Trainings geübt. Ein gutes Mittel zur Erhöhung des Datenschutzbewusstseins sind E-Learning-Systeme. Wie bereits im Praxisprojekt[55] entwickelt und analysiert, lässt sich der Lernerfolg durch selbstständiges Lernen und einer anschließenden Abfrage des erlernten Wissens deutlich erhöhen. Weiterhin stellen die ausgestellten Zertifikate einen Nachweis gegenüber der Aufsichtsbehörde da.

Vertraulichkeitserklärungen

In manchen sozialen Berufen gehört die Schweigepflicht zum Alltag. Auch Arbeitgeber in anderen Branchen können und sollten sich diese zum Nutzen machen. Personenbezogene Daten werden oft durch Arbeitnehmer ins persönliche Umfeld getragen. Dies kann einem Unternehmen erheblich schaden und eine Datenschutzverletzung zur Folge haben. In unserem Beispielunternehmen der E-Tech GmbH würde es einen erheblichen finanziellen Verlust verursachen, wenn aus der Forschung Daten veröffentlicht werden. Somit sind alle Arbeitnehmer zur Verschwiegenheit schriftlich (siehe Anhang 13: Verschwiegenheitserklärung) zu verpflichten.

Richtlinien und Leitlinien

Richtlinien und Leitlinien sind ein gutes Instrument zur Erhöhung des Datenschutzes im Unternehmen. Zum einen gehören sie bereits zu den in der Datenschutzgrundverordnung geforderten organisatorischen Maßnahmen. Zum anderen werden klare Handlungshilfen für die Arbeitnehmer bereitgestellt und der Arbeitgeber kann sich zusätzlich absichern.

[55] [ICH] Entwicklung eines elektronisch unterstützten Schulungssystems für die Sensibilisierung zum Thema Datenschutz

Folgende „Richtlinien“[56] haben sich bewährt und werden in der E-Tech GmbH eingeführt:

1. Richtlinie zum Datenschutz für Beschäftigte
2. Richtlinie zur Umsetzung von Datenschutzmaßnahmen
3. Richtlinie für die Umsetzung von Betroffenenrechte
4. IT-Richtlinien für Nutzer
5. Richtlinie für Speicherorte
6. Richtlinie für die Nutzung mobiler IT-Systeme
7. Richtlinie für die Nutzung mobiler Datenträger
8. Richtlinie Regelungen für Lieferanten und sonstige Auftragnehmer
9. Richtlinie für Störungen und Ausfälle
10. Richtlinie für Sicherheitsvorfälle
11. Notfallplan

Eine beispielhafte Richtlinie (Anhang 9: IT-Richtlinie) und dessen Aufbau wurde der E-Tech GmbH zu Verfügung gestellt. Diese kann angepasst und für weitere Unternehmen und Richtlinien verwendet werden.

Einwilligung

Ein weiterer Streitpunkt bei der Verarbeitung personenbezogener Daten von Arbeitnehmern ist die Fragestellung, zu welchen Zwecken eine Einwilligung durch den Arbeitnehmer erfolgen muss. Zusätzlich ist der Gesichtspunkt der Freiwilligkeit einer Einwilligung zu berücksichtigen, da Arbeitnehmer generell eher eine Einwilligung unterzeichnen, um keine negativen Auswirkungen auf ihr Arbeitsverhältnis zu riskieren. Grundsätzlich darf der Arbeitgeber alle geschäftsrelevanten Informationen über seinen Beschäftigten veröffentlichen. Hierzu gehören geschäftliche Kontaktdaten, wie Namen, Emailadressen oder auch Visitenkarten. Dagegen benötigen Fotographien (beispielweise für die firmeninterne Webseite oder Nutzung auf Visitenkarten) und persönliche Kontaktdaten, wie mobile Rufnummer oder private Adressdaten, die explizite Einwilligung der betroffenen Person.

4.4.3 Bewerberinformationen

Ein oft vernachlässigter Punkt im Datenschutz ist die Verarbeitung personenbezogener Daten bei potenziellen neuen Beschäftigten bzw. Bewerbern im Unternehmen. Eingereichte Daten der Bewerber gehören zu den personenbezogenen Daten und müssen entsprechend sensible und korrekt behandelt werden. Nur den zuständigen Personen ist der Zugriff auf die eingereichten Unterlagen vorbehalten.

Bewerberunterlagen von eingestellten Arbeitnehmern dürfen in der Personalakte aufgenommen werden. Unterlagen von abgelehnten Bewerbern gehören im Normalfall unver-

[56] [DBH] Richtlinien Datenschutzmanagementsystem, Kap. 41, S. 264

züglich gelöscht. Jedoch sollten sich Arbeitgeber durch eine Einwilligung über eine Speicherdauer von maximal sechs Monaten absichern, da Bewerbern das Recht auf eine Klage nach dem Allgemeinen Gleichbehandlungsgesetz vorbehalten bleibt.

Auch das beliebte Mittel der Recherche über Bewerber in sozialen Medien, sogenanntes Social Monitoring, sollte mit Vorsicht genossen werden. Auch wenn die verfügbaren Informationen öffentlich zugänglich sind, dürfen diese nur zur Entscheidungsfindung genutzt werden, wenn kein schutzwürdiges Interesse des Bewerbers entgegensteht. Spezielle geschäftliche sozialen Medien dürfen wiederrum ungehindert benutzt werden.

4.5 Technisch-Organisatorische Maßnahmen

4.5.1 Sicherheitsmanagement

Die technisch-organisatorischen Maßnahmen sind ein großer Teil in der Verteidigung gegen den Datenmissbrauch. Inwieweit eingesetzte technische und organisatorische Maßnahmen ausreichend sind, hängt von dem Schutzniveau der zu verarbeitenden Daten ab. Grundsätzlich müssen die eingesetzten Maßnahmen angemessen sein und sollten nicht den Kosten-Nutzen-Faktor überschreiten. Das Paretoprinzip, in dem mit 20% der umgesetzten Maßnahmen bereits 80% des Schutzniveaus erreicht werden kann, ist ein gutes Beispiel bei der Umsetzung.

Die Schutzziele im Datenschutz entsprechen den klassischen IT-Sicherheitsziele. Die Vertraulichkeit ist hierbei das am höchsten angestrebte Ziel. Personenbezogene Daten müssen zu jeder Zeit vor unbefugter und unbeabsichtigter Preisgabe geschützt werden. Dies schließt interne, externe Angreifer und die strukturelle Gefährdung, z.B. ungeschulte Mitarbeiter oder den Mangel an der Datenschutzorganisation, mit ein. Das zweite Schutzziel ist die Integrität. Personenbezogene Daten sind vollständig und richtig bereitzustellen. Eine unbefugte Änderung dieser Daten ist zu erkennen und ein Verfahren zur Berichtigung bereitzustellen. Das letzte Schutzziel ist die Verfügbarkeit. Personenbezogene Daten müssen zur Verfügung stehen, wenn sie gebraucht werden. Bei unbeabsichtigtem Verlust oder Zerstörung der Daten ist eine Wiederherstellung vorgeschrieben.

Die Datensicherheitsrisiken im Datenschutzsicherheitsmanagement können in fünf übergeordnete Punkte zusammengefasst werden: Vernichtung, Verlust, Veränderung personenbezogener Daten und der unbefugten Offenlegung bzw. der unbefugte Zugang zu personenbezogenen Daten. Die folgende Tabelle stellt den Zusammenhang von Datensicherheitsrisiken und Schutzzielen grafisch dar:

Risiken	**Schutzziele**		
	Vertraulichkeit	**Integrität**	**Verfügbarkeit**
Vernichtung			✔
Verlust	✔		✔
Veränderung		✔	
Unbefugte Offenlegung	✔		
Unbefugter Zugang	✔		

Tabelle 2: Datensicherheitsrisiken und Schutzziele[57]

Die technisch-organisatorischen Maßnahmen sind in einem eigenen Datenschutzdokument zu sichern und der Aufsichtsbehörde bei Anfrage vorzulegen.

Bei der E-Tech GmbH wurden diese Maßnahmen in den folgenden Kapiteln analysiert und folglich dokumentiert (Anhang 14: TOM-Dokument).

4.5.2 Technische Maßnahmen

Analyse

Der erste Schritt in der Analyse und Implementierung von technischen Maßnahmen ist die Analyse des Unternehmensnetzwerkes. Als technische Maßnahmen werden alle physisch umsetzbaren Maßnahmen, wie Alarmanlagen oder eine Firewall, bezeichnet. Bereits durch den für die E-Tech GmbH erstellten Netzwerkplan (Abbildung 9: Anhang: Netzwerkdiagramm) können geeignet technische Maßnahmen analysiert werden. Für die besonders geschützten Daten, z.B. der Daten der Forschung, ist grundsätzlich die IT-Sicherheit zuständig. Für den Datenschutz sind nur die Sicherung und die Verarbeitung personenbezogener Daten zu betrachten.

Technische Schutzmaßnahmen

In der angefertigten Netzwerkdokumentation (Anhang 4: Netzwerkdokumentation E-Tech GmbH) der E-Tech GmbH lassen sich zum einen aktive technische Maßnahmen, wie der Einsatz einer Firewall oder die getrennte Datenverarbeitung der jeweiligen Abteilungen finden. Anderseits werden passive technische Maßnahmen beschrieben, wie das IT-Sicherheitsmanagementsystem, die Passwortkomplexität, IT-Protokolle, die technische Benutzerverwaltung oder auch die eingesetzte Software, wie der Virenschutz.

Neben den informationstechnischen Maßnahmen, welche in der IT-Dokumentation zu finden sind, finden sich auch Gebäudesicherungsaspekte in den technischen Schutzmaßnahmen wieder. Einige Beispiele sind die eingesetzte Alarmanlage, Fenster- und Türsicherungen oder auch Zäune und andere bauliche Absicherungen von Geländen und Gebäuden.

Privacy by Default und Privacy by Design

Privacy by Default bzw. Datenschutz durch datenschutzfreundliche Voreinstellung ist ein weiteres Instrument der technischen Maßnahmen. Folglich sind die Werkseinstellungen in Programmen, Apps und sonstigen Anwendungen so gestaltet, dass Nutzer keine weiteren Einstellungen vornehmen müssen, um den Datenschutz zu erhöhen. In erworbener Software ist diese Einstellung meist bereits aktiv, sollte jedoch erneut durch die EDV-Abteilung überprüft werden. Bei eigens entwickelter Software, beispielsweise den Onlineshop der E-Tech GmbH, ist drauf zu achten, Voreinstellungen zu definieren die diesen Grundsatz aufweisen.

[57] [DCD] In Anlehnung: Datenschutzkonforme Datenverarbeitung, Kap. 5.1, S. 69

Das Privacy by Design Prinzip bzw. der Datenschutz durch Technikgestaltung verfolgt den Grundsatz, dass Software bereits bei der Entwicklung auf die Konformität des Datenschutzes geprüft wird. Funktionen der Software sollen der Zweckbindung entsprechen und Massenspeicherung verhindert werden.

Geeignete Maßnahmen sind die Pseudonymisierung und Anonymisierung der Nutzerdaten und die Minimierung von Datenweitergaben (z.B. IP-Adressen Speicherung). Bei der Pseudonymisierung werden die persönlichen Daten keiner Person, sondern nur einem Pseudonym zugeordnet. Bei der Anonymisierung fällt diese zuordnen komplett weg und die Daten können frei verwendet werden, z.B. zur Analyse des Kaufverhaltens. Verschiedene Zertifizierungsstellen bieten bereits Zertifizierungen für das Privacy by Default und Design Prinzip bei eigens entwickelter Software an.

4.5.3 Organisatorische Maßnahmen

Als organisatorische Maßnahmen werden Handlungsanweisungen, sowie Vorgehens- und Verfahrensweisen für Arbeitnehmern bezeichnet, um auf organisatorischer Ebene den Schutz bei der Verarbeitung personenbezogener Daten zu gewährleisten. Wie bereits im Kapitel zum Arbeitnehmerdatenschutz (siehe 4.4.2 Arbeitnehmerdatenschutz) erwähnt, gehören Schulungskonzepte und die ausgewählten Anweisungen, Richtlinien und die Verschwiegenheitserklärung zu den organisatorischen Maßnahmen. Ein sehr beliebtes Mittel in den organisatorischen Maßnahmen ist das Vier-Augen-Prinzip. Nach diesem Prinzip dürfen alle wichtigen Entscheidungen nur von zwei gleichgestellten Personen durchgeführt werden. Somit liegt eine präventive Kontrolle bei der Umsetzung der Datenschutzgrundverordnung vor. Weitere organisatorische Maßnahmen sind der Abschluss und die Handhabung von Auftragsdatenverarbeitungsverträgen (siehe 4.3 Auftragsverarbeitung) oder der im Unternehmen eingesetzten datenschutzkonformen Entsorgung von sensiblen Daten.

4.6 Bestellung Datenschutzbeauftragter

4.6.1 Bestellung und Tätigkeiten

Die Tätigkeiten des Datenschutzbeauftragten sind seit der Einführung der Datenschutzgrundverordnung um ein Vielfaches gewachsen. Wann ein Datenschutzbeauftragter zu bestellen ist, ist in den Anforderungen der Datenschutzgrundverordnung geregelt.[58] Sollte eine Pflicht zur Bestellung bestehen, kann entweder ein interner oder externer Datenschutzbeauftragter bestellt werden. Ein wichtiger Aspekt hierbei ist die Erreichbarkeit des Datenschutzbeauftragten, da er bei Berufung der zuständigen Aufsichtsbehörde zu melden ist.

Die Tätigkeiten des Datenschutzbeauftragten bringen gewissen Vorzüge mit sich. Der Datenschutzbeauftragte ist weisungsfrei, ihm stehen erforderliche Ressourcen und Wei-

[58] [DSGVO] Vgl. Datenschutzbeauftragter, Art. 37

terbildungen zur Verfügung, er muss die Aufgabe nicht als Vollzeit-Datenschutzbeauftragter wahrnehmen, er darf in keiner Weise benachteiligt werden, er besitzt einen speziellen Kündigungsschutz und das Unternehmen muss ihm unterstützend zur Seite stehen. Neben den Vorzügen bringt die Aufgabe aber auch Pflichten mit sich. Er steht immer als erster Ansprechpartner zur Verfügung und unterliegt der besonderer Geheimhaltungs- und Vertraulichkeitspflicht. Zusätzlich ist er dazu verpflichtet einen Tätigkeitsbericht (Anhang 3: Tätigkeitsbericht) zu erstellen.

Grundsätzlich sind dem Datenschutzbeauftragten laut Datenschutzgrundverordnung[59] folgende fünf Aufgaben zugeteilt:

1. Unterrichtung und Beratung des Verantwortlichen, des Auftragsverarbeiters und der Beschäftigten hinsichtlich ihrer Pflichten, die Verarbeitung personenbezogener Daten datenschutzkonform zu gestalten.
2. Überwachung der Einhaltung der Datenschutzgrundverordnung und anderer Datenschutzvorschriften, sowie der Datenschutzstrategien des Verantwortlichen und Auftragsverarbeiter, die Zuweisung von Zuständigkeiten, die Sensibilisierung und Schulung von Beschäftigten und die anschließende Überprüfung.
3. Beratende Tätigkeiten im Zusammenhang mit der Datenschutzfolgeabschätzung und Überwachung ihrer Durchführung.
4. Die Zusammenarbeit mit der Aufsichtsbehörde.
5. Erster Ansprechpartner für die Aufsichtsbehörde.

4.6.2 Audit

Eine weitere Tätigkeit des Datenschutzbeauftragten ist die jährliche Kontrolle bzw. die Durchführung eines Audits. *„Ein Audit ist ein ... systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind.“*[60] Die Durchführung einer Auditierung findet sich im PDCA-Zyklus in der Stufe der Überprüfung (Check) wieder. Demgemäß soll regelmäßig geprüft werden, ob die an das Datenschutzmanagement gestellten Anforderungen eingehalten bzw. die in Form einer Checkliste definierten Auditkriterien erfüllt werden. Zur Einführung eines oder mehrerer Audits sind vorab die folgenden Fragestellungen zu klären:

- Information über Auditziele, -umfang, -methoden und -team
- Zugang zu den erforderlichen Informationen
- Planung des Audits

Anschließend ist ein konkrete Auditcheckliste (siehe Anhang 15: Audits) zu erstellen. Dieser sollte die nachkommenden Inhalte beschreiben:

- Auditziele
- Auditumfang

[59] [DSGVO] Vgl. Aufgaben des Datenschutzbeauftragten, Art. 39, Abs. 1

[60] [AZM] Definition Audit, Kap. 2.1, S. 3

- Auditkriterien
- zu prüfende Referenzdokumente
- zu prüfende Standorte
- Auditmethoden

Ein Audit gilt als beendet bzw. abgeschlossen, wenn alle in der Auditcheckliste festgelegten Aspekte durchgeführt oder das Audit unplanmäßig beendet wurde.

4.7 Dokumentation der Aufwendungen

4.7.1 Datenschutzdokumentation

Die Erstellung einer Datenschutzdokumentation ist das praktisch zu erreichende Ziel eines Datenschutzmanagements und dieser Bachelorarbeit. Die Datenschutzdokumentation stellt den Ausgangspunkt eines Datenschutzstrategie des Unternehmens dar. Als Anlaufstelle für die Aufsichtsbehörde kann das Dokument den Datenschutz im Unternehmen nachweisen und eventuelle Strafen bei Datenschutzverstößen deutlich verringern.

Abbildung 8: Dokumentenpyramide[61]

Der Aufbau der Dokumentation kann wie in der oben beschriebenen Abbildung (siehe Abbildung 8: Dokumentenpyramide) erstellt werden. Die oberen Dokumente in der Pyramide, beispielsweise die Datenschutzleitlinie, beinhalten eine starke Stabilität, dafür jedoch wenig Spezialisierung. Im Gegensatz dazu beinhalten die unteren Dokumente der Pyramide eine hohe Spezialisierung, werden dafür häufiger angepasst.

[61] [DCD] In Anlehnung an: Dokumentenpyramide, Kap. 7.2, S. 163, Abb. 62

In der E-Tech GmbH wird die Dokumentation (siehe Anhang 1: Datenschutzdokumentation E-Tech GmbH) gemäß dem folgenden Ablauf dargestellt:

Datenschutzleitlinie (siehe Anhang 2: Datenschutzleitlinie)
Datenschutzhandbuch

- Auflagen aus Normen und Standards
  - Tätigkeitsbericht des Datenschutzbeauftragten
    (siehe Anhang 3: Tätigkeitsbericht)
  - Softwareregister und Netzwerkplan
    (siehe Anhang 4: Netzwerkdokumentation E-Tech GmbH)
- Organisation
  - Datenschutz-Governance Struktur
    (siehe Anhang 5: Datenschutz-Governance-Struktur)
  - Prozessbeschreibung
    (siehe Anhang 6: Prozessbeschreibung)
  - Verarbeitungsverzeichnis
    (siehe Anhang 7: Verarbeitungsverzeichnis)
  - Datenschutzfolgeabschätzungen
    (siehe Anhang 8: Datenschutzfolgeabschätzung)
- Richtlinien / Arbeitsanweisungen
  - Handlungsempfehlungen / Arbeitsanweisungen
    (siehe Anhang 9: IT-Richtlinie)
- Verwaltung
  - Risikoregister
    (siehe Anhang 10: Risikoregister)
  - Maßnahmenplan
    (siehe Anhang 11: Maßnahmenplan)
- Verträge und Vertragsbestandteile
  - Auftragsdatenverarbeitungsvertrag
    (siehe Anhang 12: Auftragsdatenverarbeitungsvertrag)
  - Verschwiegenheitserklärung
    (siehe Anhang 13: Verschwiegenheitserklärung)
- Technisch-Organisatorische Maßnahmen
  - TOM Dokument
    (siehe Anhang 14: TOM-Dokument)
- Audits und Reviews
  - Auditprogramm / Auditcheckliste (siehe Anhang 15: Audits)

4.7.2 Kostendokumentation

Bei der Durchführung eines Datenschutzprojektes entstehen unterschiedliche Aufwände und Kosten. Einerseits müssen tiefergehende Kenntnisse im Bereich des Datenschutzes durch die Ausbildung eines Datenschutzbeauftragten und Datenschutzkoordinator erlangt werden. Anderseits entstehen durch die Planung und Entwicklung des Datenschutzmanagements und die im Praxisprojekt entwickelter Software einmalige Kosten. Im Folgenden befindet sich eine tabellarische Auflistung der zu erwartenden Aufwendungen bei der Durchführung der Datenschutzstrategie bei der E-Tech GmbH:

Position	Bezeichnung	Menge	Einzel brutto	Gesamt brutto
1	Datenschutz-schulung incl. Prüfungskosten (TÜV)	2	2.747,71 €	5.495,42 €
2	Fachliteratur Datenschutz	Pauschal	500,00 €	500,00 €
3	Kalkulatorische Entwicklungskosten eigenes E-Learning, extern (Praxisprojekt)	240 h	90,00 €	21.600,00 €
4	Kalkulatorische Entwicklungskosten Ersterstellung Datenschutzstrategie, extern (Bachelorarbeit)	360 h	90,00 €	32.400,00 €
Zwischensumme einmalige Kosten				59.995,42 €
6	Datenschutzbeauftragter & Datenschutzkoordinator	2, monatlich	3.000,00 €	6.000,00 €
Zwischensumme monatliche Kosten				4000,00 €
Gesamt brutto				**65.995,42 €**

Tabelle 3: Aufwendungen

5 Diskussion und Fazit

Das primäre Ziel dieser Bachelorarbeit ist es am Beispiel eines mittelständischen Unternehmens ein Datenschutzmanagement zu realisieren. Mit dem geplanten Datenschutzmanagement lassen sich alle Anforderungen und Pflichten, die die Datenschutzgrundverordnung an ein Unternehmen stellt, erfüllen. Die Durchführung des Projektes konnte weitgehend wie geplant realisiert und die angestrebten Ziele erreicht werden. Die hier angewandten Methoden der GAP-Analyse und des PDCA-Zyklus stellten sich als optimale Lösungen zur Umsetzung des Projektes heraus. Die GAP-Analyse konnte den IST-Zustand des Unternehmens aufdecken und der PDCA-Zyklus kann, aufgrund seiner kontinuierlichen Verbesserung, ideal zur Durchführung und Kontrolle des Datenschutzes eingesetzten werden. Auch hat der Gesetzgeber mit seiner Einbeziehung der technisch-organisatorischen Maßnahmen eine gute Förderung hinsichtlich der Steigerung der Informationssicherheit in Unternehmen geleistet. Insgesamt schafft die in der Bachelorarbeit erzeugte Dokumentation mit ihren Beispielen einen guten Überblick und zeigt Handlungsempfehlung über alle umzusetzenden Maßnahmen auf. Das erforderliche Wissen kann sich daher gut angeeignet und die Vorgaben strukturiert umgesetzt werden.

Trotz der im allgemeinen positiv verlaufenden Realisierung, konnten einige sekundäre Themengebiete nicht wie geplant umgesetzt werden. Da es sich bei dem Thema Datenschutz um ein sehr umfangreiches Aufgabengebiet handelt, konnten nur die notwendigsten Punkte aus der Datenschutzgrundverordnung dargestellt werden. Andere Gesetze wie das seit kurzem veröffentlichte Telekommunikation-Telemedien-Datenschutzgesetz wurden somit leider nicht mitberücksichtigt. Weiterhin ist die vorliegende Dokumentation hauptsätzlich für Unternehmen, Selbstständige oder Zuständige für den Datenschutz geeignet, da die erläuterten Themen die Anforderungen zur Umsetzung an ein Unternehmen darstellen. Geeignete Fachthemen, welche in Hinsicht für Betroffenen interessant sind, wurden bereits im Praxisprojekt erläutert. Zu beachten ist auch, dass ein Datenschutzmanagement keinen umfassenden Schutz zur Sicherheit des Datenschutzes gewährleistet. Es bildet lediglich die benötigten Prozesse ab, welche durch die Beschäftigten umzusetzen und einzuhalten sind. Denn wie auch in der IT-Sicherheit, ist im Datenschutz der Mensch das größte Sicherheitsrisiko.

Für die Zukunft des Datenschutzes und dem hier geplanten Datenschutzmanagement sind vom Gesetzgeber noch weitere Anpassungen und Änderungen geplant. Weiterhin erhöhen die Aufsichtsbehörden und Kontrollorgane im Datenschutz bereits ihr Personal. Infolgedessen werden mehr Unternehmen kontrolliert und das Thema Datenschutz wird allgemein präsenter. Abschließend lässt sich sagen, dass der Datenschutz bekanntermaßen einen kontinuierlichen Prozess darstellt und immer weiterentwickelt werden kann. Somit wird das Thema auch in Zukunft aktuell bleiben und an Bedeutung weiter zunehmen.

Literaturverzeichnis

[ADP] Aichinger, Matthias, Dolezal, Andreas, Datenschutz in der Praxis, myMorawa, Salzburg, 2018

[AEM] UN-Vollversammlung, Allgemeine Erklärung der Menschenrechte, 217 [III] A, Paris

[AWP] European Commission, Article 29 Data Protection Working Party, The Future of Privacy (WP 168), Brüssel, 2009

[AZM] Brauweiler, Jana, Markus Will, Anke Zenker-Hoffmann, Auditierung und Zertifizierung von Managementsystemen: Grundwissen für Praktiker, 1. Auflage, Springer Fachmedien, Wiesbaden, 20151

[BBH] Bundesministerium des Inneren für Bau und Heimat, Referat 01, Handbuch für Organisationsuntersuchungen und Personalbedarf, Köln, Februar 2018

[BDSG] Bundesrepublik Deutschland, Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680(Datenschutz-Anpassungs- und -Umsetzungsgesetz EU–DSAnpUG-EU), Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 44, Bonn, 05. Juli 2017

[BDSGA] Bundesrepublik Deutschland, Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG), Bundesgesetzblatt Jahrgang 1977 Teil I Nr. 7, Bonn, 01. Februar 1977

[BPM] Josef Ludwig Straud, Geschäftsprozesse und ihre Modellierung mit der Methode Business Process Model and Notation (BMPN 2.0), tredition GmbH, Hamburg, 2011

[CEU] Europäisches Parlament, Charta der Grundrechte der Europäischen Union (2000/C 364/10), Amtsblatt der Europäischen Gemeinschaften vom 18.12.2000, Brüssel, 18. Dezember 2000

[BFDI] Prof. Kelber, Ulrich, Winkler, Luca, Weick, Coletta, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, abgerufen am 21 September 2021 https://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html, (o. D.)

[DBH] Stephan Hansen-Oest, Datenschutzbeauftragte – Einsteigerlektüre für Anfänger, Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main, 2020

[DCD] Thomas Kranig, Andreas Sachs, Markus Gierschmann, Datenschutz-Compliance nach der DS-GVO, Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden, Bundesanzeiger Verlag GmbH, Köln, 2019

[DED] Proliance GmbH, Alexander Ingelheim, Dominik Fünker, Definition Datenschutzmanagement, abgerufen am 21. September 2021 von https://www.datenschutzexperte.de/datenschutzmanagement/, München, (o. D.)

[DEG] Europäisches Parlament, 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 Nr. L 281 vom 23/11/1995, Brüssel, 23.November 1995

[DHS] Spiros Simitis, Hessisches Datenschutzgesetz (GHDSG), A. Bernecker Verlag GmbH, Wiesbaden, 1970

[DSGVO] Europäische Union, 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), Amtsblatt der Europäischen Union, Brüssel, 04. Mai 2016

[EMG] Susanne Koch, Einführung in das Management von Geschäftsprozessen: Six Sigma, Kaizen und TQM, Springer, Berlin, 2011

[EMK] Europarat, Convention for the Protection of Human Rights and Fundamental Freedoms, Den Haag, 4. November 1950

[FHD] Ansgar Koreng, Matthias Lachenmann, Formularhandbuch Datenschutz,2. Auflage, C.H. Beck oHG, München, 2018

[HAU] Prof. Dr. Coris Paal, Anwendungsbereich der DSGVO, abgerufen am 21 September 2021 von https://www.haufe.de/compliance/recht-politik/datenschutz-grundverordnung/anwendungsbereich-der-dsgvo_230132_517854.html ,Universität Freiburg, 09.06.2020

[ICH] Marco Nentwig, Praxisprojekt, Entwicklung eines elektronisch unterstützten Schulungssystems für die Sensibilisierung zum Thema Datenschutz, abrufbar unter https://epb.bibl.th-koeln.de/frontdoor/deliver/index/docId/1664/file/Nentwig_Marco_Praxisprojekt.pdf , TH-Köln, Gummersbach, 01.02.2021

[ICS] intersoft consulting services AG, abgerufen am 21. September 2021 von https://dsgvo-gesetz.de/themen/verzeichnis-von-verarbeitungstaetigkeiten/ , (o. D.)

[IHK] IHK Ulm, Sebastian Kuhn, Dokumentationspflichten nach der EU-Datenschutz-Grundverordnung, abgerufen am 06. September 2021 von https://www.ulm.ihk24.de/recht-und-fair-play/wirtschaft-und-recht/datenschutz/eu-dsgvo/dokumentationspflichten-3869466 , Ulm, Oktober 2019

[LDI] Block, Helga, Landesbeauftragte für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen, abgerufen am 21. September 2021 von https://www.ldi.nrw.de/mainmenu_Datenschutz/Inhalt/Datenschutz/Datenschutz.php, (o. D.)

[LDB] Bayerisches Landesamt für Datenschutzaufsicht, Durchführung einer Datenschutz-Folge-Abschätzung nach Art.35 DS-GVO in Anlehnung an die ISO/ICE 29134 abgerufen am 21. September 2021 von https://www.lda.bayern.de/media/03_dsfa_fallbeispiel_baylda_iso29134.pdf ,2017

[OMG] Object Management Group, BPMN2, abgerufen am 06. September 2021 von https://www.bpmn.org/ , (o.D)

[PA] 93rd United States Congress, Privacy Act of 1974, Washington, 1974,

[PSD] Ronald Petrlic, Christoph Sorge, Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, Springer Vieweg, Wiesbaden, 2017

[SCB] Buchholz, Liane, Strategisches Controlling: Grundlagen-Instrumente-Konzepte, 3. Auflage, Springer Fachmedien Wiesbaden, Wiesbaden, 2019

[SWL] Samuel Warren, Louis Brandeis, The Right of Privacy, Harvard Law Review, Cambridge, 1890

[TÜV] TÜV Rheinland, GAP-Analyse, abgerufen am 21. September 2021 von https://www.tuv.com/germany/de/dsgvo-gap-analyse.html, (o.D)

Anhang

Anhang 1: Datenschutzdokumentation E-Tech GmbH

Das nachfolgende Dokument beschreibt die beispielhafte Datenschutzdokumentation der E-Tech GmbH.

Anhang 2: Datenschutzleitlinie

Leitlinie zu Datenschutz und Informationssicherheit

1. Einleitung

Die E-Tech GmbH verabschiedet hiermit diese Leitlinie zu Datenschutz und Informationssicherheit in unserem Unternehmen.

Als Unternehmen verarbeiten wir eine Vielzahl von Daten, um unsere Aufgaben und Pflichten gegenüber unseren Kunden, Vertragspartnern, Dienstleistern, öffentlichen Stellen und sonstigen Dritten zu erfüllen.

Dabei verarbeiten wir Daten mit unterschiedlichen Schutzbedarf. Die Sicherheit der Informationen und der Schutz von personenbezogen Daten spielt eine wesentliche Rolle in unserem Unternehmen. Diese Leitlinie soll die Strategie, die Organisation und die Ziele von Datenschutz und Informationssicherheit in unserem Unternehmen in übersichtlicher Form darstellen.

2. Geltungsbereich

Diese Leitlinie gilt für die E-Tech GmbH. Sie erstreckt sich auf alle Standorte und Abteilungen der E-Tech GmbH. Die Leitlinie ist für alle Beschäftigten der E-Tech GmbH verbindlich und wird in entsprechend geltender Fassung den Beschäftigten zur Verfügung gestellt.

3. Ziele

Ziel dieser Leitlinie ist es, Datenschutz und Informationssicherheit im Unternehmen zu gewährleisten. Für diesen Zweck wird das Unternehmen bei der Planung, Einführung und während des Ablaufs von Verarbeitungsvorgängen nachfolgende Ziele berücksichtigen:

- Schaffung und Erhaltung von Vertrauen und Respekt vor den Erwartungen des Einzelnen zum Thema Datenschutz
- Einhaltung der Zweckbindung und der Richtigkeit für die vom Kunden zur Verfügung gestellten Daten
- Verhinderung von Verletzung der Privatsphäre
- Alle nationalen und internationalen Vorschriften werden eingehalten
- Gesetzliche Vorgaben haben Vorrang vor betrieblichen Entscheidungen

Diese Ziele werden durch gesonderte Richtlinien konkretisiert.

Bei der konkreten Umsetzung der Ziele müssen die getroffenen Schutzmaßnahmen in einem wirtschaftlichen vertretbaren Verhältnis zum Schutzbedarf der verarbeiteten Daten und Informationen stehen.

4. Organisation von Datenschutz und Informationssicherheit

Datenschutz-Governance-Struktur

Verantwortlich für die Sicherheitsorganisation ist die Unternehmensführung.

Zur Erreichung der Ziele dieser Leitlinie wird eine Datenschutz-Governance-Struktur (DGS) gebildet.

Diese besteht aus dem Datenschutzbeauftragten, einem Datenschutzkoordinator, einem Verantwortlichen aus der Geschäftsführung, einer Person aus der EDV-Abteilung sowie ggf. weiteren Personen, die von der E-Tech GmbH benannt werden können. Weitere Mitglieder wird die Unternehmensleitung im Einvernehmen mit den jeweiligen Personen bestimmen.

Die DGS wird die Planung, Umsetzung und Evaluierung von Datenschutz und Informationssicherheit in der E-Tech GmbH begleiten und unterstützen.

Die DGS wird die für die Umsetzung der Ziele dieser Leitlinie erforderlichen Richtlinien planen, mit der Unternehmensleitung abstimmen und regelmäßig auf ihre Wirksamkeit hin überprüfen und erforderliche Anpassungen vornehmen.

Für den Fall, dass die DGS in Fragen der Planung, Umsetzung, Evaluierung oder Anpassung von Richtlinien oder bei der Beurteilung von Sach- oder Rechtsfragen uneinig ist, wird die DGS dies der Unternehmensleitung vortragen. Die Unternehmensleitung wird dann entscheiden und die erforderlichen Maßnahmen veranlassen.

Die Richtlinie zur Umsetzung von Datenschutz und Informationssicherheit wird von der Unternehmensleitung verbindlich gemacht, so dass sie von den jeweiligen Adressaten der Richtlinie einzuhalten ist und Verstöße ggf. sanktioniert werden können.

Die DGS berichtet direkt an die Unternehmensleitung.

Die DGS berät über Sachfragen und wird der Unternehmensleitung über das Ergebnis der Erörterung berichten. Sollte die DGS keine einheitliche Meinung zu einer Sachfrage haben, wird der Meinungsstand offen an die Unternehmensleitung berichtet.

Die Unternehmensleitung kann Entscheidungen an die DGS durch Weisungen in Textform delegieren. Bei dieser Delegierung hat die Unternehmensleitung zu bestimmen, ob für eine Entscheidung der DGS ein einheitlicher Beschluss der DGS oder eine Mehrheitsentscheidung ausreichend ist.

Die DGS wird sich mindestens zweimal jährlich treffen, um die getroffenen Maßnahmen zu Datenschutz und Informationssicherheit im Hinblick auf ihre Wirksamkeit zu überprüfen und Anpassungen vorzunehmen.

Die DGS wird sich ansonsten anlassbezogen im Hinblick auf Treffen oder Entscheidungsfindung koordinieren, um anstehende Sachfragen zu erörtern und zu entscheiden. Maßnahmen und Entscheidungen können auch telefonisch oder in Textform erörtert werden.

Die DGS kann selbst eigene Aufgaben an Mitglieder verteilen. Dennoch wirkt die DGS gemeinschaftlich und die Mitglieder unterstützen sich gegenseitig bei der Erfüllung ihrer Aufgaben.

Der DGS können Aufgaben und Befugnisse von der Unternehmensleitung übertragen werden.

Aufgabe der DGS ist es auch, das Wissen im Bereich Datenschutz und Informationssicherheit aufzubauen und aufrechtzuerhalten. Die DGS pflegt hierzu Kontakt zu geeigneten Arbeitskreisen, Gremien und Verbänden.

Die DGS ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheits- und datenschutzrelevante Aspekte zu berücksichtigen.

Die aktuellen Mitglieder der DGS finden Sie in einem separaten Dokument und entsprechende Aushängen. Zur Vereinfachung wurde eine Sammel-E-Mail-Adresse unter datenschutz@e-tech.com erstellt.

<u>Datenschutzbeauftragter</u>

Die E-Tech GmbH hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte ist Ansprechpartner für das Thema Datenschutz im Unternehmen. Er berät, kontrolliert und unterstützt die Unternehmensleitung und Beschäftigte hinsichtlich der Verarbeitung von personenbezogen Daten im Unternehmen.

Weitere Aufgabe ergeben sich vor allem aus Art. 39 DSGVO.

Im Bereich der Verarbeitung von personenbezogenen Daten ist Sorge dafür zu tragen, dass eine frühe Einbindung des Datenschutzbeauftragten bei der Planung und Einführung von neuen Verarbeitungsvorgängen, in deren Zusammenhang auch personenbezogenen Daten verarbeitet werden, erfolgt.

Gleiches gilt für Änderungen an bestehenden Verarbeitungsvorgängen. Die Einbindung des Datenschutzbeauftragten kann auch im Zusammenhang mit der Einbindung der Datenschutz-Governance-Struktur erfolgen.

Im Unternehmen wird für den Bereich der Informationssicherheit und des Datenschutzes ein Management aufgebaut. Hierfür wird im Unternehmen ein Prozess der kontinuierlichen Verbesserung mit dem Ziel implementiert, die einzelnen Maßnahmen im Bereich Datenschutz und Informationssicherheit so zu koordinieren, dass die Ziele dieser Leitlinie erreicht werden.

5. Maßnahmen

Die Maßnahmen zur Umsetzung dieser Leitlinie können in Form von technischen und organisatorischen Maßnahmen erfolgen. Dazu gehören auch Richtlinien, betriebliche

Regelungen oder betriebliche Anweisungen. Diese sind von den Beschäftigten zu befolgen.

Die Umsetzung der Richtlinien, sowie die technisch-organisatorischen Maßnahmen erfolgt durch ein separates Dokument.

6. *Sanktionen*

Die auf Grundlage dieser Leitlinie getroffenen Richtlinien zu Datenschutz und Datensicherheit sind verpflichtend für alle Beschäftigten. Verstöße gegen Richtlinien können eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.[62]

Auflagen aus Normen und Standards

Anhang 3: Tätigkeitsbericht des Datenschutzbeauftragten

Vorwort:

Der Tätigkeitsbericht umfasst den halbjährlichen Zeitraum vom 01.01.2021 bis 01.07.2021. Die Datenschutzstruktur wurde in diesem Zeitraum in der E-Tech GmbH erstmalig aufgebaut. Aus diesem Grunde umfasst der Bericht nur die bisher aufgenommenen Zahlen und Fakten.

Zahlen und Fakten

In diesem Berichtszeitraum wurden folgende schriftliche Eingaben eingereicht. Telefonische Anfragen werden nicht berücksichtigt.

- 0 Beschwerden
- 0 Anfragen
- 0 Beratungsanfragen
- 0 Datenschutzvorfälle
- 1 Datenschutzfolgeabschätzung

Erläuterung zu den Vorfällen:

- Keine Beschwerden wurden eingereicht.
- Keine Anfragen lagen vor.
- Es gab keine relevanten Datenschutzvorfälle. Kein Datenschutzvorfall wurde an die Aufsichtsbehörde weitergeleitet.
- Eine Datenschutzfolgeabschätzung zum Thema „Ortung von Fahrzeugen“ wurde durchgeführt. Die Risiken wurden gemindert und das Verfahren kann wie geplant gestartet werden.

[62] [DBH] Leitlinie zu Datenschutz und Informationssicherheit, Kap. 41.2, S.247-252

Anhang 4: Netzwerkdokumentation E-Tech GmbH

Im Folgenden wird ein einfacher Netzwerkplan der E-Tech GmbH gezeigt. Unter realen Bedingungen sollten Raumpläne mit der Zuweisung der IP-Adresse, den Geräten und Informationen über den jeweiligen Nutzer erstellt werden. Zusätzlich ist eine Dokumentation über alle eingesetzten Netzwerkgeräte zu führen.

Netzwerkdiagramm

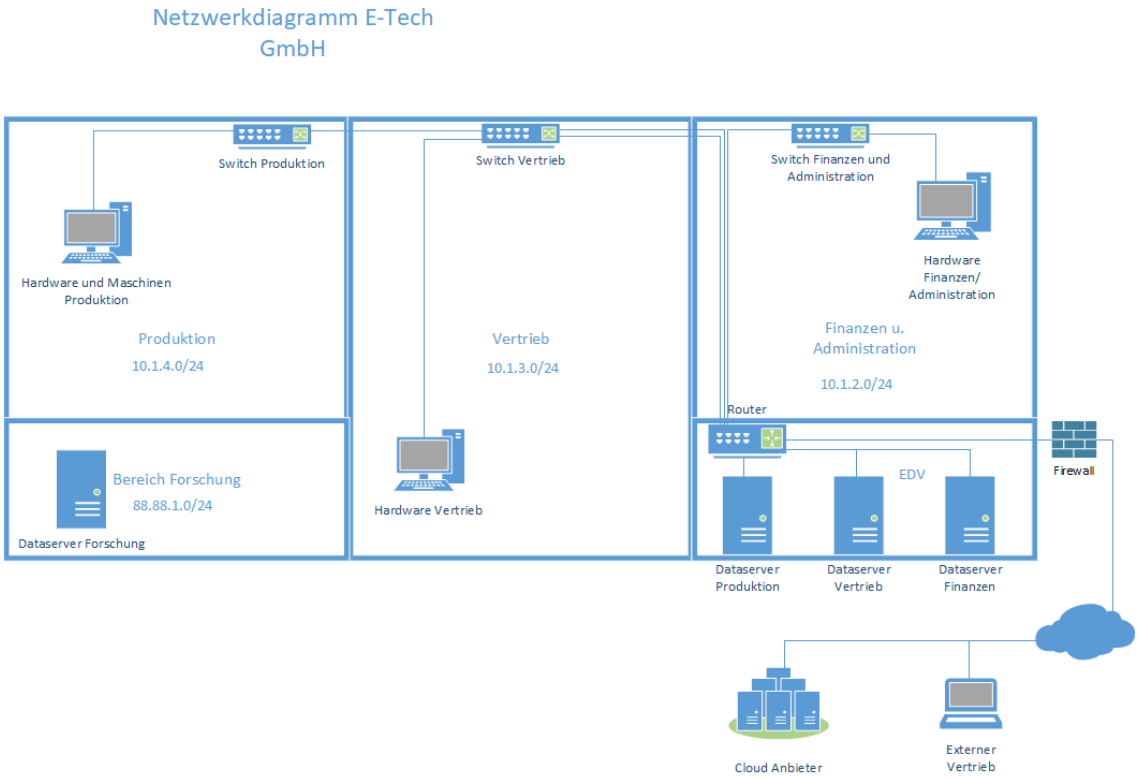

Abbildung 9: Anhang: Netzwerkdiagramm

Dokumentation

Anschließend folgt eine einfach Netzwerkdokumentation mit Softwareregister und Berechtigungskonzept:

Topologie:	sternförmig	
Domänen:	Intern: etech.local	Extern: etech.de
Öffentliche IP-Adresse:	93.158.148.x	
IP-Kreise:	Local: 10.1.x.x / 24 VPN: 10.10.10.x /24	Forschung: 88.88.1.x /24 WAN: 192.168.2.x /24
Server:	Dataserver Forschung	IP: 88.88.1.10
	Dataserver Produktion	IP: 10.1.4.10
	Dataserver Vertrieb	IP: 10.1.3.10
	Dataserver Finanzen	IP: 10.1.2.10

	Backup-System	IP:10.1.1.10
	Webserver extern	IP: 231.132.123.123
	Online-Shop	IP: 213.123.123.233
	Firewall:	IP: 123.123.123.132
Sonstige Geräte:	WLAN, TK-Anlage, Firewall, Drucker	
Softwareregister:	Windows Server 2016	
	Windows 10	
	Linux (verschiedene Distributionen)	
	Cloud-Software	
	Virenschutz	
	IT-Sicherheitsmanagement	
	SAP	
	Online-Shop	
	CRM-Software	
	Produktions-Software	
	….	

Berechtigungskonzept:

Das Berechtigungskonzept zeigt, welche Daten von welchen Abteilungen verarbeitet werden dürfen:

Daten Forschung:	Forschung, Geschäftsführung
Daten Vertrieb:	Vertrieb, Finanzen, Geschäftsführung
Daten Produktion:	Produktion, Finanzen, Vertrieb, Geschäftsführung
Daten Finanzen:	Finanzen, Geschäftsführung

Organisation

Anhang 5: Datenschutz-Governance-Struktur

Die Datenschutz-Governance-Struktur der E-Tech GmbH umfasst zurzeit folgende Mitglieder:

Verantwortlicher:	Herr Müller, Geschäftsführung CFO
Datenschutzbeauftragter:	Herr Fischer, Abteilung Forschung und Entwicklung
Datenschutzkoordinator:	Frau Soll, Abteilung Verwaltung
Weitere Mitglieder:	Herr Bäcker, Abteilung EDV
	Frau Schmitz, Abteilung Vertrieb

Erläuterung:

Herr Müller steht als Verantwortlicher der Geschäftsführung zu Verfügung. Der Datenschutzbeauftragte Herr Fischer aus der Abteilung Forschung und Entwicklung übernimmt die Aufgaben des Datenschutzbeauftragten im 40% Arbeitszeit-Modell. Als Vertretung wurde die Datenschutzkoordinatorin Frau Soll berufen, alle Betroffenenanfragen wird sie im Namen von Herrn Fischer bearbeiten. Bei sonstigen Fragen und Beratungen rund um den Datenschutz ist als erster Ansprechpartner Herr Fischer hinzuzuziehen. Weitere Mitglieder der Datenschutz-Governance-Struktur sind Herr Bäcker aus der EDV-Abteilung und Frau Schmitz aus dem Vertrieb. Herr Bäcker ist zusätzlich für den Datenschutz für IT-Systeme zuständig. Frau Schmitz unterstützt die Struktur im Rahmen von Meetings.

Anhang 6: Prozessbeschreibung

Alle Prozesse wurden durch die jeweiligen Abteilungen grafisch durch BMPN2 dargestellt. Da die Prozesse der jeweiligen Abteilungen der E-Tech GmbH den Rahmen des Dokumentes sprengen würden, befinden sie sich in einem separaten Dokument und werden hier nur zur Richtigkeit aufgenommen. Nachfolgend findet sich ein Beispiel für den Verarbeitungsvorgang Auftragsbearbeitung:

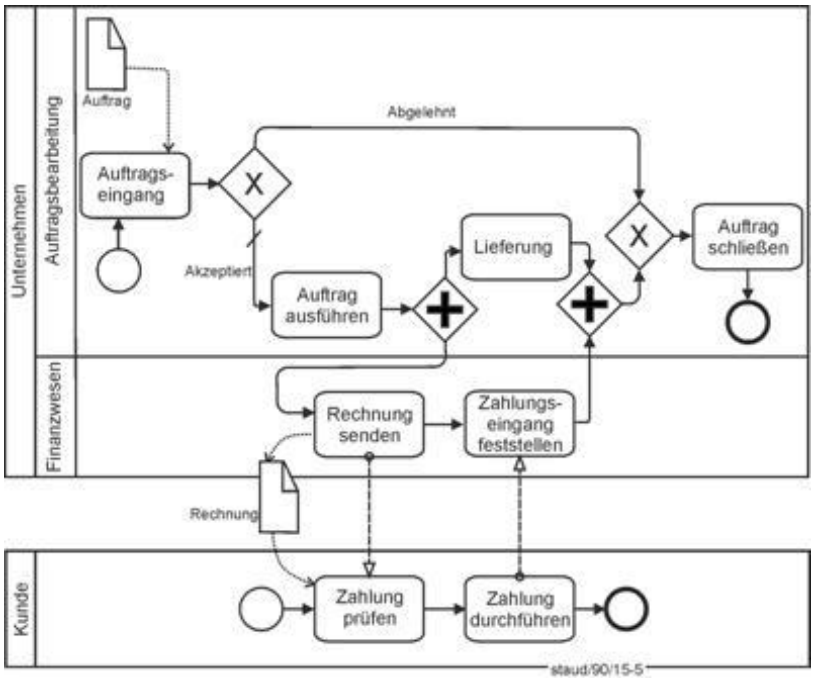

Abbildung 10: Anhang: Beispiel BPMN2[63]

[63] [BPM] BPMN2 Auftragsabwicklung S. 269, Figur 10.85

Anhang 7: Verarbeitungsverzeichnis

Alle Verarbeitungen im Verarbeitungsverzeichnis werden nach folgendem Beispiel aufgebaut:

Muster zur Verarbeitungstätigkeit „Auftrag entgegennehmen“

1. *Bezeichnung der Verarbeitung mit fortlaufender Nummerierung*
   Auftrag entgegennehmen, Verkauf von Waren, Nr.1
2. *Zwecke der Verarbeitung*
   Verkauf und Vertrieb von Waren und Dienstleistungen
3. *Beschreibung der Kategorien personenbezogener Daten*
   Vorname, Nachname, Titel, Name des Unternehmens, Anschrift (privat, geschäftlich), Rechnungsanschrift, E-Mail-Adresse, Telefonnummer, Kundennummer, Kundenart, Kontaktdaten, Kontakthistorie, Termindaten, Bankverbindung, Umsatzsteueridentifikationsnummer, Daten zu gekauften Waren oder Dienstleistungen, Vertragsdaten, Umsatzdaten
4. *Beschreibung der Kategorien betroffener Personen*
   Kunden, Geschäftspartner
5. *Kategorien von Empfänger, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden*
   Logistikunternehmen, Finanzwesen
6. *Übermittlung an Drittländern oder internationalen Organisationen*
   Keine
7. *Vorgesehene Fristen zur Löschung der verschiedenen Datenkategorien*
   10 Jahre, da buchungsrelevante Daten nach § 147 Abs.4 AO aufzuheben sind.
8. *Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen*
   Siehe technisch-organisatorische Maßnahmen

Anhang 8: Datenschutzfolgeabschätzung

Als Beispieldatenschutzfolgeabschätzung wurde der Prozess „Ortung von Kraftfahrzeugen“ ausgewählt und im nachfolgendem dargestellt:

Sachverhalt:

Die E-Tech GmbH möchte zur Sicherung ihres Eigentums eine Ortung der dienstlich genutzten Kraftfahrzeuge veranlassen. Hierbei soll eine neue Technologie eingesetzt werden, welche den Standort der Fahrzeuge über eine mobile Sim-Karte an ein Cloud-Dienstleister vermittelt. Die Abtastfrequenz eines Datensatzes beträgt eine Sekunde. Die Daten werden verschlüsselt über die Mobilfunkverbindung zum Cloudanbieter geschickt und liegen im Anschluss der E-Tech GmbH entschlüsselt vor. Die Rohdaten aus den Kraftfahrzeugen werden drei Jahre lang aufbewahrt. Rechtlich soll der Datenumgang durch einen Auftragsverarbeitungsvertrag mit den Cloud-Dienstleister und einer Einwilligung der Beschäftigten geregelt werden.

Schwellenwertanalyse

Die Schwellenwertanalyse hat folgende Tatbestände im vorliegenden Fall ermittelt:

Eine große Menge an Daten wird mit einer neuen Technologie verarbeitet. Des Weiteren können die Standortdaten den einzelnen Fahrern bzw. Beschäftigten zugeordnet werden. Somit können durch die Daten Rückschlüsse über die Lebensweise und den Aufenthaltsort des Fahrzeugführers gebildet werden.

Folgende Punkte treffen zu:

Systematische Überwachung, Sensitive Daten, Umfangreiche Datenverarbeitung, Neue Technologie

Aus der Zusammenschau dieser Tatbestände wird abgeschätzt, dass wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen beifolgendem Sachverhalt entstehen: Es werden eine große Menge an Daten, zum Teil auch sensible Daten, erhoben, welche eine systematische Überwachung der Beschäftigten zur Folge haben.

Zusammenstellung des DSFA-Teams

Das DSFA-Team besteht in diesem Falle aus der Datenschutz-Governance Struktur einschließlich der Projektleitung des umzusetzenden Projektes und der zuständigen Betreuerin des Software- und Cloud-Anbieters.

Analyse des Sachverhalts

Folgende Komponenten und Datenflüsse können ermittelt werden:

Die Sim-Karte erstellt Daten zu Fahrgestellnummer, GPS-Position, Uhrzeit, Fahrer und sonstigen KFZ-Merkmalen. Diese übermittelt sie an eine Datenbank des Cloud-Anbieters, welcher durch die Rohdaten die Fahrroute, Geschwindigkeit, Datum und Fahrverhalten ermittelt. Im Anschluss werden diese Daten in einem Backupsystem gespeichert.

Akteure

Verantwortlicher: E-Tech GmbH

Auftragsverarbeiter: Cloud-Anbieter

Betroffene: Beschäftigte, Anderweitige Fahrer des KFZ

Rechtsgrundlage

Die Rechtsgrundlage für die Erhebung und Verarbeitung der Daten der Beschäftigten soll durch eine Einwilligung gemäß DSGVO Art. 6a erfolgen. Der Vertrag zwischen der E-Tech GmbH und dem Cloud-Anbieter wird durch einen Auftragsverarbeitungsvertrag gemäß DSGVO Art. 28 abgeschlossen.

Modellierung der Risikoquellen

Folgende Risikoquellen wurden ermittelt:

Art der Quelle	Extern/Intern	Unbeabsichtigt / Vorsätzlich	Akteur / Risikoquelle
Menschlich	Intern	Unbeabsichtigt	Mitarbeiter
Menschlich	Intern	Vorsätzlich	Mitarbeiter
Menschlich	Extern	Unbeabsichtigt	Mitarbeiter (Dienstleister), sonst. Dritte
Menschlich	Extern	Vorsätzlich	Dienstleister, Cyberkriminelle, Staatliche Institute, sonst. Dritte
Nichtmenschlich	Intern	/	Hardwaredefekte, Softwarefehler
Nichtmenschlich	Extern	/	Hardwaredefekte, Softwarefehler, Umwelteinflüsse, Gesetzesänderungen, Netzstörungen

Tabelle 4: Anhang: Risikoquellen

Risikoanalyse

Die Risikoanalyse erfolgt in einem separaten Dokument. Die Verarbeitungsgrundsätze werden mit den Risikoquellen, den möglichen Schäden, Schadenskategorien, Eintrittswahrscheinlichkeit und Schwere des Schadens zusammengefasst und eine Risikobewertung folgt.

	Risikobeurteilung (gemäß ISO 31000)							
	I. Risikoidentifikation			II. Risikoanalyse				III. Risikobewertung
Risiko ID	Verarbeitungsgrundsatz (nach Art. 5 DS-GVO)	Risikoquelle	Risikobeschreibung	Möglicher Schaden	Schadenskategorie (nach ErwGr. 75)	Eintrittswahrscheinlichkeit	Schwere des Schadens	Ergebnis
1	Verfügbarkeit	Externer Mitarbeiter - USA	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	Risiko (4)
2	Verfügbarkeit	Cyberkrimineller (Hacker/Schadsoftv	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
3	Verfügbarkeit	Softwarefehler	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	Risiko (4)
4	Verfügbarkeit	Hardwaredefekt (physikalisch)	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
5	Verfügbarkeit	Umwelteinflüsse (Naturgewalt)	Löschung der Backups der Rohdaten in den USA be	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
6	Verfügbarkeit	Externer Mitarbeiter - Bangladesch	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
7	Verfügbarkeit	Cyberkrimineller (Hacker/Schadsoftv	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Wesentlich (3)	Begrenzt (2)	Risiko (5)
8	Verfügbarkeit	Umwelteinflüsse (Naturgewalt)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
9	Verfügbarkeit	Softwarefehler	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Begrenzt (2)	Begrenzt (2)	geringes Risiko (2-3)
10	Verfügbarkeit	Hardwaredefekt (physikalisch)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
11	Verfügbarkeit	Versicherter (Kfz-Fahrer)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
12	Verfügbarkeit	Dritter (anderer Kfz-Fahrer)	Löschung der Rohdaten in Bangladesch bei Bengali	Einschränkungen beim Auskun	Hinderung der Kontrolle der Betroffe	Vernachlässigbar (1)	Begrenzt (2)	geringes Risiko (2-3)
13	Integrität und Vertraulichkeit	Externer Mitarbeiter - Bangladesch	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
14	Integrität und Vertraulichkeit	Versicherter (Kfz-Fahrer)	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Begrenzt (2)	Begrenzt (2)	Risiko (4)
15	Integrität und Vertraulichkeit	Dritter (anderer Kfz-Fahrer)	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Begrenzt (2)	Wesentlich (3)	Risiko (5)
16	Integrität und Vertraulichkeit	Cyberkrimineller (Hacker/Schadsoftv	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
17	Integrität und Vertraulichkeit	Interner Mitarbeiter - Insight AG	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Wesentlich (3)	Maximal (4)	hohes Risiko (7-8)
18	Integrität und Vertraulichkeit	Externer Mitarbeiter - USA	Unbefugte Entwendung der Rohdaten vom Fahrzeu	Rufschädigung, Diskriminierur	Rufschädigung	Begrenzt (2)	Maximal (4)	Risiko (6)

Abbildung 11: Anhang: Auszug aus der Risikobeurteilung[64]

Auswahl geeigneter Abhilfemaßnahmen

Folgende Abhilfemaßnahmen kommen zu den Tatbeständen in Frage:

Die Fahrzeugdaten, sowie die Daten zu Fahrer können pseudonymisiert oder auch anonymisiert werden. Somit entfällt der Rückschluss auf die Fahrweise des Beschäftigten.

Die Verkettbarkeit von Fahrzeugdaten und Fahrer kann aufgehoben werden. Somit werden keine personenbezogenen Daten erhoben.

Die Umsetzung eines Löschkonzeptes zur Datensparsamkeit.

[64] [LDB] Risikobeurteilung, S.19, Abb. 7 [online]

Einführung eines Monitorings des Zugriffs mittels Log-Dateien.

Weitere Maßnahmen zur Verschlüsselung.

Einbeziehung von externen Beratern und die Durchführung von Penetrationstests.

Umsetzung und Tests der Abhilfemaßnahmen

Die Umsetzung und Tests der Abhilfemaßnahmen erfolgten. Eine weitere Risikoanalyse ergab, dass durch die Pseudonymisierung der Fahrerdaten das Risiko minimiert wurde. Der Verarbeitungsvorgang kann wie geplant umgesetzt werden.

Richtlinien / Arbeitsanweisungen

Anhang 9: IT-Richtlinie

Der E-Tech GmbH wurde eine beispielhafte Richtlinie zur IT-Nutzung der Beschäftigten zur Verfügung gestellt. Weitere Richtlinie können den gleichen Aufbau und Form nutzen. Beispiele für weitere Richtlinien finden Sie im Kapitel 4.4.2 Arbeitnehmerdatenschutz.

IT-Richtlinie für Nutzer

1. *Einleitung*

Die E-Tech GmbH verfügt über eine IT-Infrastruktur, die den Beschäftigten im Zusammenhang mit ihrer Tätigkeit für die E-Tech GmbH als Arbeitsmittel zur Verfügung steht. Die IT-Infrastruktur ist unerlässlich für den Geschäftsbetrieb der E-Tech GmbH.

2. *Geltungsbereich*

Diese IT-Richtlinien gelten für die E-Tech GmbH. Sie gelten für alle Standorte und Abteilungen der E-Tech GmbH.

Dies IT-Richtlinien sind von allen Beschäftigten der E-Tech GmbH einzuhalten.

3. *Ziele*

Um die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme auf Dauer zu gewährleisten, sind die nachfolgenden IT-Richtlinien von allen Beschäftigten einzuhalten.

4. *Allgemeine Nutzungsrichtlinien für IT-Systeme*

Sofern nachfolgend von IT-Systemen die Rede ist, sind darunter ausnahmslos alle Geräte und Anwendungen zu verstehen, mit denen Informationen elektronisch verarbeitet oder übertragen werden können. Dazu gehören insbesondere Computer, Notebooks, Tablet PCs, Telefone, Server, Speichermedien, Netzwerktechnologien, Softwareprodukte und Drucker.

Die Nutzung der IT-Systeme und Applikationen in der E-Tech GmbH ist ausschließlich zu dienstlichen Zwecken und in jeweils erlaubtem Umfang zur Aufgabenerledigung zulässig. Abweichungen hiervon bedürfen der Erlaubnis des Arbeitgebers. Es darf nur die Software auf IT-Systemen des Unternehmens installiert werden, die vom Arbeitgeber oder der IT-Abteilung freigegeben worden ist.

Die Benutzung privater Hard- und Software zu dienstlichen Zwecken ohne Genehmigung ist nicht zulässig.

Die Nutzung von IT-Systemen bei der E-Tech GmbH erfolgt grundsätzlich nur für die beruflichen Zwecke. Eine private Nutzung von IT-Systemen der E-Tech GmbH ist grundsätzlich untersagt.

5. Einhaltung von Rechtsvorschriften

Bei der Benutzung von IT-Systemen und Applikationen bei der E-Tech GmbH sind von den Beschäftigten die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie sonstige Rechtsvorschriften und Unternehmensrichtlinien einzuhalten. Sollten Beschäftigte unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren Vorgesetzten zur Klärung zu wenden.

6. Schulungen

Das Unternehmen trägt Sorge dafür, dass die Beschäftigten die erforderlichen Schulungen und Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen erforderlich sind.

7. Vorgaben zu Gestaltung und des Arbeitsplatzes

Der Arbeitsplatz ist von den Beschäftigten so zu gestalten, dass Dritte keinen Zugang zu personenbezogenen Daten erhalten können.

Beim Verlassen des Arbeitsplatzes ist der Computer zu sperren oder der Benutzer abzumelden.

Informationen in Papierform sind so abzulegen, dass Dritte keine Kenntnis von den Daten erhalten können.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist komplex zu gestalten.

Die Nutzung der dienstlichen E-Mailadresse darf nur für dienstliche Zwecke erfolgen. Private E-Mails dürfen über einen entsprechenden Browser genutzt werden.

Die eingesetzte Virensoftware ist regelmäßig zu überprüfen.

Bei Verdacht auf Gefährdung des IT-Systems ist die IT-Abteilung zu informieren. Die Weisungen der IT-Abteilung im Bezug auf den Umgang mit IT-Systemen ist zu folgen.

8. Notfallplan

Falls es zu einem Notfall kommt, ist der Notfallplan anzuwenden. Die Meldung hat spätestens nach 24 Stunden zu erfolgen. Der Notfallplan befindet sich in einem separaten Dokument.

9. Protokollierung

Bei der IT-Infrastruktur werden verschiedene Informationen protokolliert um Störungen, Ausfälle und Sicherheitsvorfälle schneller zu identifizieren und beheben zu können. Dabei werden die datenschutzrechtlichen Bestimmungen eingehalten und die Persönlichkeitsrechte der Beschäftigten gewahrt.

10. Missbrauchskontrolle

Für das Erkennen von Störungen, Ausfällen und Sicherheitsvorfällen findet eine nichtpersonenbezogene Auswertung von Protokolldaten statt. Eine personenbezogene Auswertung erfolgt nur, wenn aufgrund einer Stichprobenkontrolle, einer Meldung oder anderen Verdachtsmomenten ein konkreter Verdacht auf eine missbräuchliche, unerlaubte oder strafbare Nutzung besteht.

11. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden. [65]

Verwaltung

Anhang 10: Risikoregister

Die Risikoanalyse setzt sich aus der Formel $Risiko = Schadenshöhe\ x\ Eintrittswahrscheinlichkeit$ zusammen.

Für die E-Tech GmbH wurden folgende Faktoren zur Ermittlung des Risikos benutzt:

Beispielhafte Bewertung Schadenshöhe

Schadenskategorien	**Vernachlässigbar**	**Begrenzt**	**Wesentlich**	**Maximal**
	Kleine Unannehmlichkeit	*Größere Unannehmlichkeit*	*Wesentliche Folgen*	*Wesentlichen und/oder irreversible Folgen*
Diskriminierung			Diskriminierung in einem Teilbereich des Lebens (z.B. Arbeit)	Diskriminierung des Betroffenen im gesamten Lebensumfeld
Identitätsdiebstahl				Identitätsdiebstahl
Finanzieller Verlust	Monatsgehalts	Mehrere Monatsgehälter	Jahresgehalt	Verlust des gesamten Vermögens
Rufschädigung			Rufschädigung in einem Teilbereich des Lebens	Rufschädigung im gesamten Lebensumfeld
Gesellschaftliche oder wirtschaftliche Nachteile	Keine oder sehr geringe Auswirkungen	Auswirkungen sind spürbar oder führen zu kleinen Einschränkungen	Nachteile im Lebensalltag	Große Auswirkungen auf das Leben im persönlichen Umfeld

[65] [DBH] IT-Richtlinie für Nutzer, Kap. 41.13, S.275-282

Kinderdaten			Kinderdaten werden geringfügig verarbeitet	Kinderdaten werden im großen Ausmaß verarbeitet
Große Menge personenbezogener Daten	50 Datensätze	100 Datensätze	500 Datensätze	1000 Datensätze
Große Menge von betroffenen Personen	50 Personen	100 Personen	500 Personen	1000 Personen
Scoring	Keine Nachteile	Leichte Nachteile durch automatisierte Verarbeitung	Nachteile durch automatisierte Verarbeitung	Nachteile im privaten Umfeld

Tabelle 5: Anhang: Bewertung Schadenshöhe

Bewertung Eintrittswahrscheinlichkeit

Eintrittswahrscheinlichkeit		**Schätzung für die Zukunft**	**Blick in die Vergangenheit**
Vernachlässigbar	*Fast unmöglich*	Frühstens in 7 Jahren	Vorfall bisher noch nie eingetreten
Begrenzt	*Mit gewissem Aufwand machbar*	Vorfall in den nächsten 4-7 Jahren geschätzt	Vorfall bereits einmal aufgetreten
Wesentlich	*Mit geringem Aufwand machbar*	Vorfall in den nächsten 1-3 Jahren geschätzt	Vorfall liegt bis zu 3 Jahren zurück
Maximal	*Einfach*	Vorfall könnte im nächsten Jahr auftreten	Vorfall im letzten Jahr aufgetreten

Tabelle 6: Anhang: Bewertung Eintrittswahrscheinlichkeit

Anhang 11: Maßnahmenplan

Dies ist ein zusammengefasster Maßnahmenplan der E-Tech GmbH. Die ausführlichere Darstellung befindet sich unter 4.2.5 Handhabung Datenschutzverletzung.

1. *„Datenschutzvergehen erkennen und schnell handeln:* Weiterleitung des Vorfalls vom Mitarbeiter an den Vorgesetzen, den Datenschutzkoordinator oder direkt an den Verantwortlichen für den Datenschutz.
2. *Bewertung***:** Durchführung einer Risikoanalyse durch den Verantwortlichen für Datenschutz, um das Ausmaß abschätzen zu können.
3. *Maßnahmen zur Abwendung / Eindämmung:* Maßnahmen ergreifen, um gegen das Datenleck vorzugehen.
4. *Entscheidung, ob eine Meldung erfolgen soll:* Anhand der Bewertung entscheidet der Verantwortliche für Datenschutz, ob eine Meldung bei der Behörde erfolgen soll und ob Betroffene in Kenntnis gesetzt werden müssen.
5. *Meldung an die Aufsichtsbehörde oder / und an die Betroffenen:* Der Verantwortliche für Datenschutz erstattet Meldung bei der zuständigen Behörde.“ [66]

[66] [ICH] Verhalten bei Datenpannen, Kap. 2.2.6, S.14

Verträge und Vertragsbestandteile

Anhang 12: Auftragsdatenverarbeitungsvertrag

Die E-Tech GmbH ist grundsätzlich nicht dazu verpflichtet einen eigenen Auftragsverarbeitungsvertrag zu erstellen, da keine Dienstleistungen für Dritte erfolgen. Dennoch wird der E-Tech GmbH ein Auftragsverarbeitungsvertrag zur Verfügung gestellt, um die Auftragsverarbeitungsverträge kontrollieren zu können.

Auftragsverarbeitungsvertrag Musterbeispiel

1. *Gegenstand und Dauer des Auftrags*

Gegenstand und Dauer des Auftrages bestimmen sich nach den jeweiligen Vertragsverhältnissen, welche durch den Auftragnehmer und Auftraggeber abgeschlossen wurden. Der Auftragnehmer verarbeitet dabei auf Grundlage dieses Auftrags personenbezogene Daten für den Auftraggeber nach Art. 28 und Art. 4 Abs. 2 DSGVO.

2. *Konkretisierung des Auftragsinhaltes*

Folgende Arten und Zwecke der Verarbeitung personenbezogener Daten durch den Auftragnehmer sind dabei:

- Personenstammdaten
- Kommunikationsdaten, Vertragsstammdaten, Protokolldaten
- Vertragsabrechnungs- und Zahlungsdaten

Der Umfang der Betroffenen umfasst hierbei:

- Kunden und Interessen des Auftragsgebers
- Mitarbeiter und Lieferanten des Auftragsgebers

Die Verarbeitung der vertraglichen Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union statt. Jede Verlagerung in ein Drittland bedarf der Zustimmung des Auftragsgebers und der besonderen Voraussetzung nach Art. 44ff. DSGVO.

3. *Technisch-organisatorische Maßnahmen*

Der Auftragnehmer hat die Durchführung der vorgegebenen technischen und organisatorischen Maßnahmen vor Auftragserteilung zu dokumentieren und dem Auftraggeber vor Aufnahme der Verarbeitung, insbesondere zur konkreten Vertragsdurchführung, zur Prüfung vorzulegen. Nimmt der Auftraggeber diese an, werden die aufgezeichneten Maßnahmen Grundlage des Auftrags. Ergibt die Prüfung des Auftraggebers ein Anpassungsbedarf, ist dieser einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit der personenbezogenen Daten gemäß Art. 28 und Art. 32 DSGVO in Verbindung mit Art. 5 DSGVO herzustellen. Die getroffenen Maßnahmen müssen dabei den Stand der Technik, die Implementierungskosten, die Art, der Umfang und die Zwecke der Verarbeitung, sowie die Eintrittswahrscheinlichkeit und

Schwere eines Risikos berücksichtigen. Die Maßnahmen müssen gewährleisten, dass die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit eingehalten werden.

Die technisch-organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diesbezüglich kann der Auftragnehmer alternative geeignete Maßnahmen ergreifen. Das Sicherheitsniveau der Maßnahmen darf hierbei nicht abgesenkt werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die im Auftrag verarbeiteten Daten nicht unbefugt, sondern nur nach den dokumentierten Weisungen des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Sollte sich eine betroffene Person diesbezüglich direkt an den Auftragnehmer wenden, wird der Auftragnehmer diese Anfrage unverzüglich an den Auftraggeber weiterleiten.

Falls im Leistungsumfang umfasst, sind Löschkonzepte, das Recht auf Vergessenwerden, Berichtigung und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsnehmers

Der Auftragnehmer ist zur Bestellung eines Datenschutzbeauftragten verpflichtet. Dieser ist dem Auftraggeber mitzuteilen.

Der Auftragnehmer hat alle Beschäftigte, welche bei der Durchführung von Verarbeitungsvorgängen des Auftraggebers mitwirken, zur Vertraulichkeit zu verpflichten.

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde zusammen.

Der Auftragnehmer kontrolliert regelmäßig die technisch-organisatorischen Maßnahmen, sowie die internen Prozesse, um das Datenschutzniveau zu gewährleisten.

6. Unterauftragsverhältnisse

Der Auftragnehmer darf nur nach vorheriger schriftlicher bzw. dokumentierter Vereinbarung Unterauftragnehmer beschäftigten. Der Auftraggeber stimmt der Beauftragung folgender Unterauftragnehmer zu: /

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Einverständnis mit dem Auftragnehmer, Überprüfungen durchzuführen bzw. durch geeignete Prüfer durchzuführen lassen. Diese Kontrollen sind rechtzeitig anzumelden. Für die Ermöglichung der Kontrollen kann der Auftragnehmer eine Vergütungspauschale geltend machen.

8. Mittelung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung von Pflichten zur Sicherheit personenbezogener Daten, Datenschutzfolgeabschätzung, Meldepflichten und Datenpannen. Bei Verstößen des Auftragnehmers ist unverzüglich der Auftraggeber zu informieren.

9. Weisungsbefugnis des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber in geeigneter Form. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstößt gegen geltende Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung auszusetzten, bis sie durch den Auftraggeber bestätigt wurde.

10. Löschung und Rückgabe von Daten

Der Auftragnehmer darf keine Kopien oder Duplikate ohne Wissen des Auftragnehmers anfertigen. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung des Datenschutzes. Nach Forderung des Auftraggebers oder nach Beendigung des Auftragsverhältnisses hat der Auftragnehmer die Pflicht, alle Daten dem Auftraggeber auszuhändigen oder nach Aufforderung zu Löschen. Hierbei ist ein Protokoll der Löschung zu erstellen und dem Auftraggeber auszuhändigen.

Ort, Datum, Unterschrift des Auftraggebers und Auftragnehmers

Anhang 13: Verschwiegenheitserklärung

Die folgende Vertraulichkeitserklärung wurde der E-Tech GmbH bereitgestellt:

Verpflichtung zu Wahrung der Vertraulichkeit zur Beachtung des Datenschutzes sowie ggf. zu Wahrung von Berufs- bzw. Privatgeheimnisses

Hinweis zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Im Rahmen Ihrer Tätigkeit sind Sie personenbezogenen Daten ausgesetzt. Daher verpflichtet die E-Tech GmbH Sie hiermit, die Datenschutzmaßnahmen, insbesondere die Vertraulichkeit im Unternehmen, einzuhalten. Sie verpflichten sich dazu personenbezogene Daten nicht unbefugt zu verarbeiten, diese Daten nicht an Dritte weiterzugeben oder diesen in anderer Art und Weise Zugriff zu gewähren. Sie sind insbesondere verpflichtet, die datenschutzrechtlichen Vorgaben und Weisungen des Unternehmens einzuhalten. Diese Verpflichtung gilt umfassend.

Die DSGVO definiert Verarbeitungen als jeden Verarbeitungsvorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, das Ordnen, das Bestellen, das Speichern, die Anpassung oder Änderung, das Auslesen, das Abfragen, das Übermitteln, das Verteilen oder jede andere Form des Bereitstellens, Vergleichens oder Verknüpfens, Einschränkens, Löschens oder Vernichtens der Nutzung und Offenlegung.

Personenbezogene Daten im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen. Eine Person gilt als identifizierbar durch

die Zuordnung von Kennungen wie Name, Identifikationsnummer, Standortdaten, Online-Kennung, physische, physiologische, genetische, psychologische, wirtschaftliche, kulturelle oder soziale Informationen.

Unter Geltung der DSGVO, BDSG und andere Strafgesetze und Vorschriften können Verstöße zum Datenschutz mit Freiheits- oder Geldstrafen geahndet werden. Verstöße gegen den Datenschutz können weiterhin einen Verstoß gegen arbeitsrechtliche oder dienstrechtliche Pflichten bedeuten und entsprechende Konsequenzen haben. Bei schweren Verstößen gegen den Datenschutz können dem Unternehmen zudem sehr hohe Bußgelder drohen, die zu Ansprüchen gegen Sie führen können.

Hinweise für Berufsgeheimnisträger

Im Laufe Ihrer Arbeit kommen Sie möglicherweise auch mit Privatgeheimnissen in Kontakt. Hierbei handelt es sich um Informationen, welche Ihnen im Rahmen der Berufsausübung anvertraut werden und an deren Geheimhaltung der Betroffene ein besonderes Interesse hat.

Unabhängig von der vorgenannten Datenschutzverpflichtung haben Sie diese Informationen streng vertraulich zu behandeln. Dies gilt auch, sofern Sie Zeuge in einem Zivil-, Straf- oder Verwaltungsverfahren sind. Ein Verstoß gegen diese Geheimhaltungspflicht ist strafbar nach Art. 203 des deutschen Strafgesetzbuches.

Diese Verpflichtung besteht ohne zeitliche Begrenzung und auch nach Beendigung Ihrer Tätigkeit im Unternehmen.

Über die Verpflichtung auf das Datengeheimnis und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung mit dem Abdruck der hier genannten Vorschriften habe ich erhalten.

Ort, Datum, Unterschrift des Verpflichteten

Anhang 14: TOM-Dokument

Technische und organisatorische Maßnahmen zur Datensicherheit

Bei der E-Tech GmbH sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit getroffen worden.

1. Vertraulichkeit

Zutrittskontrolle

Die Zugänge zur E-Tech GmbH und auch zu den dazugehörigen Büroräumen sind Tag und Nacht verschlossen. Zum einen wird der Zugang zum Unternehmen durch bauliche Zäune gesperrt. Zum anderen kommt ein elektronisches Schließsystem mit Transpondern zum Einsatz. Dieses wird von der Verwaltung der E-Tech GmbH verwaltet und entsprechend protokolliert. Bei der Vergabe von Berechtigungen wird nach dem Grundsatz der Erforderlichkeit gehandelt.

Weiterhin wird ein Alarmsystem eingesetzt, welches Fenster und Türen der E-Tech GmbH sichert. Dies wird durch eine Sicherheitsfirma erweitert, welches in den nächtlichen Stunden Rundgänge erledigt.

Jeder Besucher muss sich beim Empfang anmelden. Der Besucher wird im Anschluss von der Empfangsperson zum jeweiligen Ansprechpartner geleitet und in einem Besuchsbuch protokolliert. Besucher dürfen sich grundsätzlich nicht ohne Begleitung in den Büroräumen aufhalten.

Zugangskontrolle

Zum Zugang zu den IT-Systemen der E-Tech GmbH sind Benutzerberechtigungen vergeben. Der Benutzer enthält einen Benutzernamen mit einem komplexen Passwort. Das Passwort besteht aus 12 Zeichen und enthält eine komplexe Kombination aus Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern. Das Passwort wird jedes Quartal erneuert. Eine Passworthistorie ist hinterlegt, damit die 10 zuletzt gewählten Passwörter nicht erneut ausgewählt werden.

Fehlerhafte Anmeldungen der Benutzer werden dokumentiert und nach 3-maliger Falscheingabe das Konto gesperrt.

Alle Clients der E-Tech GmbH verfügen über eine Sicherheitssoftware, welche mit tagesaktuellen Sicherheitsupdates bespielt wird.

Alle Server sind zusätzlich mit Sicherheitssoftware und Firewall versorgt, welche regelmäßig gewartet wird.

Der VPN- Zugang der Mitarbeiter ist verschlüsselt und benötigt eine Zertifikatsbasierte Anmeldung.

Der Internetzugriff der Client und Server ist durch eine Firewall gesichert, welche als Content-Filter und Portkontrolle dient.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese unbeaufsichtigt verlassen.

Zugriffskontrolle

Die Berechtigungen für die IT-Systeme werden durch die Personalabteilung beauftragt und können nur durch die Administratoren vergeben werden. Es gibt ein rollenbasiertes Berechtigungssystem, welche die differenzierte Vergabe von Zugriffsberechtigung nach Rollen, Aufgabengebiet und Projekten ermöglicht.

Datenträger und Papiere werden durch einen Dienstleister nach DIN 66399 fachgerecht vernichtet.

Beschäftigten ist es untersagt, nicht genehmigte Software zu installieren oder zu verwenden.

Alle Clients und Server der E-Tech GmbH werden regelmäßig mit Updates aktualisiert.

Trennung

Alle von der E-Tech GmbH eingesetzten IT-Systeme sind mandantenfähig. Eine Trennung der Daten von verschieden Kunden ist vorgesehen.

Pseudonymisierung und Verschlüsselung

Der Zugriff von den Administratoren auf die Serversysteme erfolgt über eine verschlüsselte Verbindung.

Weiterhin enthalten die Clients und Server eine Verschlüsselungstechnik, welche alle Daten auf den Festplatten verschlüsselt.

2. Integrität

Eingabekontrolle

Die Beschäftigten sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Accounts dürfen nicht geteilt werden.

Eine Protokollierung der Eingabe, Löschung oder Änderung von personenbezogenen Daten erfolgt.

Weitergabekontrolle

Alle Mitarbeiter der E-Tech GmbH werden regelmäßig zu Datenschutz und Datensicherheit geschult. Eine Verschwiegenheitserklärung verpflichtet sie zu einem vertraulichen Umgang mit personenbezogenen Daten.

Die Weitergabe von personenbezogenen Daten wird mit dem Kunden stets abgestimmt und erfolgt nur zur Erbringung von vertraglichen Leistungen. Die Weitergabe erfolgt grundsätzlich verschlüsselt.

Die Nutzung von privaten Datenträgern der Beschäftigte ist gesperrt und untersagt.

3. Verfügbarkeit

Die Daten der E-Tech GmbH werden wöchentliche voll und täglich inkrementell gesichert. Die Backups befinden sich an einem physisch getrennten Ort und werden verschlüsselt. Das Einspielen der Backups wird regelmäßig getestet.

Im Serverraum befindet sich eine CO2-Löschanlage, welche die Server vor einem Brand schützen kann. Zusätzlich werden die Serverräume durch ein Monitoringsystem überwacht, das im Falle einer Störung die zuständigen Administratoren informiert.

Die IT-Systeme verfügen über ein Notstromsystem mit passender unterbrechungsfreier Stromversorgung.

Ein Notfallplan mit entsprechenden Wiederanlaufplan steht den Administratoren zur Verfügung und wird regelmäßig getestet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei der E-Tech GmbH ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie und entsprechende Richtlinie, die den Datenschutz und die Datensicherheit gewährleisten.

Ein Datenschutzbeauftragter und Datenschutzkoordinator mit Datenschutz-Governance Struktur wurden berufen. Diese Struktur plant, evaluiert und setzt alle Maßnahmen im Bereich Datenschutz um.

Datenschutzvorfälle werden dokumentiert und ausgewertet. Je nach Ermessen erfolgt eine Weiterleitung an die Aufsichtsbehörde und die jeweiligen Kunden werden informiert.

Ein jährliches Audit erfolgt, um alle geplanten technischen- und organisatorischen Maßnahmen zu kontrollieren.

Auftragskontrolle

Die Verarbeitung der Daten erfolgt ausschließlich in der Europäischen Union bzw. in Deutschland.

Externe Auftragsverarbeiter werden auf das Datengeheimnis verpflichtet und unterliegen einem Auftragsdatenverarbeitungsvertrag. Während des Vertragsverhältnisses und bei Abschluss eines neuen Auftragsverarbeiters erfolgt eine Auditierung über die Datensicherheit.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bei der Entwicklung der eingesetzten Software und dem Webshop der E-Tech GmbH wird auf den Grundsatz der Erforderlichkeit geachtet. Im Interface sind Formularfelder und Bildschirmmasken so gestaltet, dass erforderliche Eingaben verpflichtend sind oder deaktiviert werden können.

Die eingesetzte Software verfügt über eine Eingabekontrolle, um Fehler bei der Eingabe oder Veränderung der Daten zu vermeiden. Weiterhin verfügt die Standardeinstellung über datenschutzfreundliche Voreinstellungen. Die Berechtigungen der Software können flexibel gesetzt werden.

Anhang 15: Audits

Das Auditprogramm mit entsprechender Auditcheckliste legt die jährliche Überprüfung des Datenschutzes fest. Bei der Kontrolle der Aufsichtsbehörde kann das Auditreview vorgelegt werden.

Im Folgenden befindet sich eine exemplarische Übersicht über die kontrollierten Inhalte des Datenschutzkonzeptes der E-Tech GmbH:

Checkliste für Unternehmen	**Erledigt**
Organisationskontrolle	**Ja/Nein**
Datenschutzkonzept vorhanden?	Ja
Datenschutzbeauftragter / -Koordinator vorhanden und erreichbar?	Ja
Mitarbeiter zur Verschwiegenheit verpflichtet?	Ja
Mitarbeiter zum Thema Datenschutz geschult?	Ja
Zutrittskontrolle	**Ja/Nein**
Zutritt zum Gebäude beschränkt?	Ja
Zutritt zu Räumen beschränkt, in denen personenbezogenen Daten lagern?	Ja
Server gesichert?	Ja
Serverräume nur für befugtes Personal zugänglich?	Ja
Zugangskontrolle	**Ja/Nein**
Passwortkomplexität vorhanden?	Ja
Virenschutz vorhanden und aktuell?	Ja
Authentifizierung vorhanden?	Ja
Bildschirmsperren eingerichtet?	Ja
Firewall installiert und aktuell?	Ja
Zugriffskontrolle	**Ja/Nein**
Datenträger und Papiere werden sicher entsorgt?	Ja
Konzept zur Zugriffsberechtigung liegt vor?	Ja
Datenschutzverletzungen werden protokolliert?	Ja
Weitergabekontrolle	**Ja/Nein**
Regelmäßige Wartung und Prüfung der Systeme?	Ja
Verschlüsselung eingerichtet?	Ja
Beschränkung der Nutzung der IT-Systeme?	Ja
Eingabekontrolle	**Ja/Nein**
Protokollierung von Eingabe, Löschung und Änderung personenbezogener Daten?	Ja
Protokollierung von Zugriffen?	Ja
Auftragskontrolle	**Ja/Nein**
Auftragsdatenverarbeitungsverträge vorhanden?	Ja
Auditierung der Auftragnehmer durchgeführt?	Ja
Verfügbarkeitskontrolle	**Ja/Nein**
Sicherungskopien vorhanden?	Ja
Sicherung vor Schadsoftware vorhanden?	Ja
Daten gegen unbeabsichtigte Vernichtung oder Löschung geschützt?	Ja
Trennungsgebot	**Ja/Nein**
Systeme mandantenfähig?	Ja
Personenbezogene Daten getrennt verfügbar?	Ja
Gemeinsam erhobene Daten getrennt voneinander verfügbar?	Ja

Tabelle 7: Anhang: Auditcheckliste