FERDINAND PORSCHE
FERN FH

Nutzung von Cloud-Services bei KMUs unter Berücksichtigung der DSGVO

Masterarbeit

eingereicht von: **Andreas Kaufmann, BA**
Matrikelnummer: 00760798

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH GmbH

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Thomas Krabina, M.Sc.

Zweitgutachten: DI Thomas Györgyfalvay

Wiener Neustadt, Mai 2019

EHRENWÖRTLICHE ERKLÄRUNG

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.

2. dass ich diese Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Sankt Stefan, Mai 2019

Unterschrift

DANKSAGUNG

An dieser Stelle möchte ich mich bei meinem Betreuer Thomas Krabina, M.Sc., bedanken. Er stand mir jederzeit mit seinem Feedback und neuen Anregungen zur Seite. Des Weiteren möchte ich mich bei meinem Zweitbetreuer DI Thomas Györgyfalvay für die Betreuung und sein konstruktives Feedback bedanken.

Ein großer Dank gilt allen Teilnehmerinnen und Teilnehmern, die die Umfrage unterstützt und geteilt haben. Insbesondere möchte ich mich bei der Wirtschaftskammer Österreich für die Unterstützung bei der Umfrage bedanken. Nur durch diese große Unterstützung konnte die Forschungsfrage beantwortet werden.

Des Weiteren möchte ich mich an dieser Stelle bei Ingo Hasewend für die grammatikalische und ganzheitliche Durchsicht der Arbeit bedanken.

Schließlich möchte ich mich noch bei meiner Familie sowie besonders bei meiner Frau bedanken, die mich während meines Studiums immer unterstützt haben.

KURZFASSUNG

Nutzung von Cloud-Services bei KMUs unter Berücksichtigung der DSGVO

Diese Arbeit hat sich das Ziel gesetzt, die Nutzung von Cloud-Services bei KMUs vor und nach dem Inkrafttreten der Datenschutz-Grundverordnung zu untersuchen. Dabei wird der Fokus auf die veränderte Cloud-Service-Nutzung von KMUs nach dem Inkrafttreten der Datenschutz-Grundverordnung gelegt.

Die Untersuchung erfolgt mittels einer empirischen Forschungsmethode unter Verwendung eines standardisierten Onlinefragebogens. Zusätzlich werden die gesammelten Forschungsergebnisse der empirischen Studie durch theoretische Grundlagen gestützt.

Im ersten Teil dieser Arbeit werden die theoretischen Grundlagen zur Beantwortung der Forschungsfrage erläutert. Der Fokus der theoretischen Grundlagen wird dabei auf die Themen „Cloud-Computing", „Datenschutz-Grundverordnung" sowie auf zusammenhängende Themengebiete gelegt.

Im zweiten Teil dieser Arbeit wird die Forschungsmethodik beschrieben und zur praktischen Anwendung gebracht. Die gewonnenen Forschungsergebnisse werden analysiert und interpretiert. Abschließend wird anhand dieser Ergebnisse die Forschungsfrage beantwortet.

Schlagwörter

DSGVO; Datenschutz-Grundverordnung; Cloud-Computing; Cloud-Services; Cloud-Security; Cloud-Compliance; Informationssicherheit; kleine und mittelständische Unternehmen; KMUs

ABSTRACT

Cloud service usage among SMEs in consideration of GDPR

The aim of this paper is to examine the use of cloud services by SMEs before and after GDPR came into effect, with a special focus on the change in cloud service usage after its commencement.

We examined this through empirical research methods, i.e. a standardised online questionnaire. Additionally, the collated results are supported by established theories.

The first part of this paper will explain the theoretical foundations that answer the research question, focussing on cloud computing, GDPR and related topics.

The second part of the paper describes and puts into practice our research methodology. The results are analysed and interpreted and finally, the research question is answered based on these results.

Keywords

GPRD; General Data Protection Regulation; Cloud-Computing; Cloud-Services; Cloud-Security; Cloud-Compliance, Information-Security; small and medium-sized Enterprises; SMEs

INHALTSVERZEICHNIS

I. ABKÜRZUNGSVERZEICHNIS 1

1. EINLEITUNG 3

1.1 Zielsetzung und Motivation 6

1.2 Forschungsfrage 7

1.3 Aufbau und Methodik der Arbeit 8

1.4 Abgrenzung 11

2. GRUNDLAGEN 12

2.1 Cloud-Computing 12

2.1.1 Begriffsdefinition 13

2.1.2 Was ist Cloud-Computing? 15

2.1.3 Service-Modelle 20

2.1.4 Betriebsmodelle 23

2.1.5 Übersicht von Cloud-Services-Kriterien 25

2.1.6 Anwendungsbereiche von Cloud-Services 28

2.1.7 Pro und Contra von Cloud-Services 33

2.1.8 Zusammenfassung 36

2.2 Datenschutz-Grundverordnung (DSGVO) 36

2.2.1 Begriffsdefinitionen 37

2.2.2 Geschichtlicher Hintergrund der DSGVO 39

2.2.3 Kernziele der DSGVO 40

2.2.4 Anwendungsbereiche der DSGVO 42

2.2.5 Fundament der EU-Datenschutz-Grundverordnung 43

2.2.6 Rechte und Pflichten 47

2.2.7 Technische und organisatorische Maßnahmen (TOMs) 50

2.2.8 Die Datenschutzbehörde 57

2.2.9 Strafrahmen 58

2.2.10 Zusammenfassung 59

2.3 Kleine und mittelständische Unternehmen (KMUs) 59

2.3.1 Begriffsdefinition 60

2.3.2 Verteilung der KMUs in Österreich 60

2.3.3 Zusammenfassung 61

3. CLOUD-COMPLIANCE 62
3.1 Vertragliche Rahmenbedingungen 63
3.2 IT-Service-Management 64
3.3 Informationssicherheit 66
3.3.1 Planungsphase 67
3.3.2 Umsetzungs- und Migrationsphase 68
3.3.3 Betriebsphase 69
3.3.4 Beendigung (Exit) 69
3.4 Datenschutz 69
3.5 Bedrohungen von Cloud-Services 71
3.5.1 Cloud-Provider-Infrastruktur 71
3.5.2 Nutzung von Cloud-Services 73
3.5.3 Einführung von Cloud-Services 75
3.6 Empfehlungen und mögliche Maßnahmen 78
3.6.1 Organisatorische Maßnahmen 78
3.6.2 Technische Maßnahmen 87
3.7 Zusammenfassung 91
4. EMPIRISCHE STUDIE 93
4.1 Methodik 93
4.2 Fragebogendesign 95
4.2.1 Allgemein 95
4.2.2 Cloud-Computing 96
4.2.3 Datenschutz-Grundverordnung 97
4.2.4 Nutzungsverhalten 97
4.3 Analyse und Interpretation 98
4.3.1 Allgemein 99
4.3.2 Cloud-Computing 102
4.3.3 Datenschutz-Grundverordnung 109
4.3.4 Nutzungsverhalten 116
4.4 Zusammenfassung 123
5. FAZIT 124
5.1 Beantwortung der Forschungsfrage 124
5.2 Ausblick und Nutzen 128
5.3 Zusammenfassung 130

II. ANHANG **135**
III. ABBILDUNGSVERZEICHNIS **141**
IV. TABELLENVERZEINIS **144**
V. LITERATURVERZEICHNIS **145**

I. ABKÜRZUNGSVERZEICHNIS

ADFS	Microsoft Active Directory Federation Services
ATAWAD	Anytime, Anywhere, Anydevice
AWS	Amazon Web Service
BCM	Business Continuity Management
BITKOM	Bundesverband für Informationswirtschaft, Telekomunikation und neue Medien
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Cloud-Computing
CSIRT	Computer Emergency Response Team
CSP	Cloud-Service-Provider
DaaS	Desktop-as-a-Service
DBaaS	Database-as-a-Service
DDoS	Distributed-Denial-of-Service
DLP	Data Loss Prevention
DSFA	Datenschutzfolgeabschätzung
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
ENISA	Europäische Agentur für Netz- und Informationssicherheit
EU	Europäische Union
Eurostat	Statistische Amt der Europäischen Union
GCP	Google Cloud Platform
HuaaS	Humans-as-a-Service
IaaS	Infrastructure-as-a-Service
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITK	Informations- und Kommunikationstechnik
ITSM	IT-Service-Management
KMUs	Kleine und mittlere Unternehmen
KVP	Kontinuierlicher Verbesserungsprozess
MFA	Multi-Faktor-Authentisierung
NIST	National Institute of Standards and Technology
PaaS	Platform-as-a-Service
PDCA	Plan-Do-Check-Act

SaaS	Software-as-a-Service
SLA	Service-Level-Agreement
StaaS	Storage-as-a-Service
TOMs	Technische und organisatorische Maßnahmen
XaaS	Everything-as-a-Service

1. EINLEITUNG

Das Thema „Cloud-Computing“ ist nicht mehr als utopisch anzusehen. Cloud-Computing ist schon längst in vielen Unternehmen beziehungsweise in der Informationstechnologie etabliert. Cloud-Computing bringt ganz neue Möglichkeiten. IT-Infrastrukturen und Applikationen können skalierbar und kosteneffizient genutzt werden. Cloud-Computing bietet zahlreiche Einsatzmöglichkeiten und damit verbundene Vor- und Nachteile. Diese werden in den folgenden Abschnitten der Arbeit im Detail erläutert. [VHH13, S. 2]

Der Trend „Cloud-Computing“ beherrscht in den vergangenen Jahren wie kaum ein anderer Trend die Medien und Unternehmensstrategien. Cloud-Computing wird aktuell von allen führenden IT-Analysten als einer der Top-5-IT-Trends dargestellt. Die Unternehmen evaluieren nicht mehr, ob Cloud-Computing eine praktikable Lösung für ihr Unternehmen ist, sondern viel mehr, wie man diese Technologie mit größtmöglichem Nutzen und möglichst hohen Sicherheitsstandards im Unternehmen implementieren kann. [MPR15, S. 1f.]

Durch die Digitalisierungsstrategien der Unternehmen wurden in beinahe allen Branchen neue Geschäftsmodelle entwickelt. Diese Geschäftsmodelle, ob in Dienstleistungsbereichen oder auch in Produktionsbereichen (Industrie 4.0), tragen zur Weiterentwicklung sowie auch zur Förderung von Cloud-Computing bei. Internet der Dinge (kurz IoT) und Industrie 4.0 sind die besten Beispiele für den Vormarsch von Cloud-Computing. Trotz dieser Digitalisierungsoffensive und des voranschreitenden Fortschritt treten weiterhin Herausforderungen auf. [BI14, S. 45f.]

Zum einen trat am 25. Mai 2018 die EU-Datenschutz-Grundverordnung (kurz DSGVO) in Kraft. Bis spätestens dahin mussten die europäischen Unternehmen ihre Compliance in Hinsicht auf den Schutz personenbezogener Daten sicherstellen. Um diese Compliance zu erreichen, müssen die Unternehmen

prinzipiell einen genauen Überblick über alle bearbeitenden Daten haben. Des Weiteren müssen klare technische und organisatorische Maßnahmen (TOMs) getroffen werden, um den technischen Schutz und den organisatorischen Umgang der Daten zu gewährleisten. Wenn Unternehmen mit der Verarbeitung der Daten ihr Kerngeschäft bestreiten, dann ist es zwingend notwendig einen Datenschutzbeauftragen zu bestellen. Seit dem 25. Mai 2018 wird die Compliance der Unternehmen von der Datenschutzbehörde (vormals Datenschutzkommission) überprüft. Die Datenschutzbehörde kann Verwarnungen und auch hohe Geldstrafen ausstellen. [La18]

Ist die Vereinbarung von Datenschutz und Cloud-Computing überhaupt möglich? Die Speicherung und Verarbeitung von personenbezogenen Daten natürlicher Personen in der Cloud ist ein spezieller Fall. Die Verantwortung für personenbezogene Daten an Cloudanbieter beziehungsweise Cloud-Service-Provider abzugeben, ist nicht zur Gänze möglich. Eine Restverantwortung bleibt immer beim Cloud-Nutzer, da die Datenschutz-Grundverordnung zwischen dem Datenverarbeiter (Cloud-Anbieter) und dem Datenverantwortlichen (Cloud-Nutzer) unterscheidet. Beide Teilnehmer müssen sicherstellen, dass sie die Compliance hinsichtlich der Speicherung und Verarbeitung personenbezogener Daten einhalten. [Be18, S. 315f.]

Zum anderen haben die Unternehmen Angst, die Kontrolle über ihre Daten zu verlieren. Der Verlust kann auf falscher Handhabe von Mitarbeitern (unabsichtliches Löschen der Daten) oder auch auf Cyberangriffen beruhen. Letzteres hat in den vergangenen Jahren enorme wirtschaftliche Schäden verursacht. Zudem hat eine durchgeführte Studie des Frauenhofer-Instituts für „Sichere Informationssicherheit“ bei den großen Cloud-Anbieter, einige grobe Sicherheitsmängel festgestellt. [He12, S. 1ff.]

Des Weiteren wurde vom „Bundesverband für Informationswirtschaft, Telekomunikation und neue Medien“ – kurz Bitkom – durch eine Umfrage

erläutert, dass in den vergangenen zwei Jahren bereits ein Drittel der Unternehmen Opfer eines Cyberangriffs wurden. [AK18]

Damit ist belegt, dass die Cloud-Computing-Anbieter noch einiges an Aufholbedarf im Bereich Informationssicherheit haben. Aber nicht nur die Cloud-Computing-Anbieter haben Aufholbedarf, auch Unternehmen - insbesondere KMUs - leiden unter organisatorischen Problemen hinsichtlich der Informationssicherheit. Aufgrund der Unternehmensgröße verzichten KMUs meist auf eigene Rechenzentren und lagern diese Kompetenzen an Dritte aus. KMUs müssen sich auf ihre Kernkompetenzen konzentrieren, um wirtschaftlichen Erfolg zu erzielen. [MRV11, S. 180f.]

Deshalb entscheiden sich viele Unternehmen für den Weg in die digitale Transformation und letztendlich in die Cloud. Um die Transformation erfolgreich umzusetzen, ist eine Digitale-Cloud-Strategie unumgänglich. Ohne eine Strategie kann es zu folgeschweren Fehlern in der Umsetzung kommen. Dies wiederrum führt dazu, dass die Unternehmen den Wettbewerbsvorteil gegenüber der Konkurrenz verlieren. [WZ14, S. 142ff.]

Der digitalen Transformation können sich Unternehmen - speziell KMUs - nicht entziehen, da KMUs mit immer mehr strukturierten Daten sowie auch unstrukturierten Datenmengen (Big Data) zu kämpfen haben. Die Datenmengen entstehen aus internen und aus externe Datenquelle, die durch den Support von Datenmanagement-Lösungen erfolgreich verarbeitet werden können. In Zukunft müssen diese Datenmengen strukturiert erfasst und dokumentiert werden. Hinsichtlich dieser Umstände sind sich einige Unternehmen unsicher und verfolgen den Weg in die Cloud beziehungsweise auch wieder aus der Cloud heraus. [VHH13, S. 13ff.]

In den Kapitelabschnitten des ersten Kapitels wird die Zielsetzung der Arbeit sowie die Motivation zum Forschungsthema beschrieben. Des Weiteren wird die Forschungsfrage genauer erläutert und der Aufbau der Arbeit geschildert.

1.1 Zielsetzung und Motivation

Eine zukunftssichere Informationstechnologie (kurz IT) stellt Unternehmen heutzutage auf ganz besondere Herausforderungen. Die IT muss den Unternehmen neue Märkte eröffnen und gleichzeitig sicher, zuverlässig und kosteneffizient sein. Cloud-Computing glänzt mit Eigenschaften wie schnell, funktionell, kosteneffizient, sicher und zuverlässig. Somit sind Cloud-Anbieter eine realistische Alternative zum Eigenbetrieb oder dem klassischen Outsourcing. [MPR15, S. 3f.]

Seit Jahren werben die führenden Cloud-Anbieter wie Amazon, Microsoft aber auch Google mit Ihren Cloud-Services. Die Cloud-Services zeichnen sich durch hohe Skalierbarkeit und durch einen hohen Grad an Kostenkontrolle aus. Des Weiteren wird der Umstieg durch einfache Migrationsszenarien sowie durch kostenlose Migrationsworkshops schmackhaft gemacht. Laut einer Studie des „Statistischen Amt der Europäischen Union“ (kurz Eurostat) nutzten 2014 rund zwölf Prozent der österreichischen Unternehmen Cloud-Services. [BGS14, S. 1ff.]

Im Jahr 2016 kamen die österreichischen Unternehmen bereits auf einen Nutzungsgrad von rund 18 Prozent. Betrachtet man den EU-Durchschnitt mit einem Nutzungsgrad von Rund 21 Prozent im Jahr 2016, dann befindet sich Österreich demnach unter dem EU-Durchschnitt. [St16]

Man kann davon ausgehen, dass der Nutzungsgrad der österreichischen Unternehmen weiter steigen wird und somit immer mehr österreichische Unternehmen Cloud-Services von Cloud-Anbietern beziehen werden. Aber wie verändert sich die Cloud-Service-Nutzung der kleinen und mittelständischen Unternehmen nachdem die EU-Datenschutz-Grundverordnung (kurz DSGVO) in Kraft getreten ist? Das herauszufinden, ist das Kernziel dieser Arbeit.

Ein weiteres Ziel dieser Arbeit ist es, die datenschutzrechtlichen Faktoren hinsichtlich der Datenschutz-Grundverordnung und des Cloud-Computing zu erläutern und die Abhängigkeit zwischen den beiden Faktoren darzustellen.

Verändert sich der Nutzungsgrad von Cloud-Services durch das Inkrafttreten der DSGVO oder hat dies keinerlei Auswirkung auf die Nutzung von Cloud-Services. Anhand von österreichischen KMUs soll die Forschungsfrage, die im nächsten Kapitelabschnitt erläutert wird, beantwortet werden.

1.2 Forschungsfrage

Wie in den vorausgegangenen Kapitelabschnitten beschrieben, beschäftigt sich die Arbeit mit der Nutzung des Cloud-Computing insbesondere bei KMUs und nach dem Inkrafttreten der Datenschutz-Grundverordnung. Diese Arbeit soll eine mögliche Abhängigkeit dieser beiden Faktoren darstellen. Gibt es eine mögliche Abhängigkeit zwischen dem Inkrafttreten der Datenschutz-Grundverordnung und den Cloud-Services? Wird der Trend „Cloud-Computing" durch die neuen rechtlichen Aspekte wieder verblassen, oder verstärkt sich der Trend sogar?

Die Forschungsfrage lautet daher:

„Wie hoch ist die Bereitschaft zur Cloud-Service-Nutzung bei KMUs vor und nach Inkrafttreten der DSGVO?"

Aus der Sicht des Autors erhöht sich der Nutzungsgrad von Cloud-Services auch nach dem 25. Mai 2018 weiterhin. Durch die immer weiter steigende Komplexität im Bereich der Informationstechnologie sowie durch die immer weiter steigende Flexibilität werden immer mehr Unternehmen auf Cloud-Services setzen. Durch die Datenschutz-Grundverordnung muss jedoch ein Umdenken erfolgen. Viele Unternehmen werden ihre Prozesse dokumentieren und nachweisen müssen beziehungsweise praktizieren dies bereits freiwillig. Ohne die beschriebenen Grundvoraussetzungen müssen Unternehmen mit hohen Geldstrafen rechnen.

Die beschriebene Forschungsfrage soll mittels einer empirischen Studie beantwortet werden. Um eine hohe Aussagekraft zu erreichen, entschied sich der Autor dieser Arbeit für eine quantitative Befragung mittels einem Online-Fragenbogen. Als Vorteil der quantitativen Online-Befragung können die niedrigen Erhebungs- und Auswertungskosten sowie die Anonymität der Probanden genannt werden. Durch diese Anonymität kann mit ehrlicheren Antworten der Probanden gerechnet werden. Des Weiteren können die erhobenen Antworten mit dieser Methode schnell und effizient ausgewertet und miteinander vergleichen werden. Diese Forschungsmethode weißt neben den beschriebenen Vorteilen auch Nachteile auf. Durch die starre Struktur des Online-Fragebogens können keine zusätzlichen Fragen oder Antworten generiert werden. Des Weiteren kann die Richtigkeit der Antworten, durch die Anonymität der Probanden, nicht überprüft werden. Als Zielgruppe der quantitativen Befragung mittels Online-Fragenbogen wurden österreichische KMUs definiert. [Ko07, S. 34]

Im nächsten Kapitel wird der Aufbau der Arbeit und die Methodik der Arbeit beschrieben. Des Weiteren wird die Arbeit in zwei Teile gegliedert.

1.3 Aufbau und Methodik der Arbeit

Die Kapitel eins bis fünf enthalten die relevanten Forschungsinhalte der Arbeit. Die Kapitel I bis V enthalten den Anhang sowie das Literatur-, Abbildungs-, Tabellen- und das Abkürzungsverzeichnis.

Die Arbeit startet mit dem **Kapitel I** indem das Abkürzungsverzeichnis dargestellt wurde. Das **Kapitel 1** beschreibt die Zielsetzung und Motivation dieser Arbeit. Zudem wird im ersten Kapitel die Forschungsfrage erläutert und der Aufbau dieser Arbeit detailliert beschrieben und dargestellt. Im **Kapitel 2** werden die Grundlagen des Cloud-Computing, der Datenschutz-Grundverordnung (DSGVO), den kleinen und mittelständischen Unternehmen und weiterer

grundlegender Begriffe dieser Arbeit beschrieben. Das **Kapitel 3** beschäftigt sich mit der Cloud-Compliance. Die Cloud-Compliance wird gemäß des Cloud-Kompass erläutert. In diesem Kapitel werden mögliche Cloud-Service-Szenarien und Empfehlungen für mögliche technische und organisatorische Maßnahmen beschrieben. Im **Kapitel 4** wird die empirische Studie behandelt. Wie schon vorab beschrieben handelt es sich bei der empirischen Studie um eine quantitative Onlinebefragung. Dabei werden das Vorgehensmodell und der benötigte Fragebogen erarbeitet und erläutert. Die Daten für die Studie wurden mittels einer Umfrage erhoben. Anschließend werden im vierten Kapitel die Analyse und die Interpretation der erhaltenen Daten durchgeführt. Das **Kapitel 5** schließt die Arbeit mit einer Zusammenfassung und mit der Beantwortung der Forschungsfrage ab. Im anschließenden **Kapitel II** werden alle relevanten Anhänge dargestellt. In diesem Kapitel wurde ein Auszug des Onlinefragebogens, der für die quantitative Online-Befragung herangezogen wurde, dargestellt. Zudem werden das Abbildungsverzeichnis und Tabellenverzeichnis im **Kapitel III** sowie im **Kapitel IV** dargestellt. Die für die Arbeit herangezogene Literatur wird im **Kapitel V** in einem Literaturverzeichnis zusammengefasst.

In der Abbildung 1 wird die Gliederung der Arbeit grafisch dargestellt und in einen Theorieteil und einen Praxisteil unterteilt. Im Theorieteil werden die Grundlagen des Cloud-Computing und der vorherrschenden rechtlichen Situationen gemäß der Datenschutz-Grundverordnung erläutert. Des Weiteren werden die kleinen und mittelständischen Unternehmen genauer erläutert. Der Theorieteil schließt mit einer ausführlichen Bearbeitung des Themas „Cloud-Compliance“ und der dazugehörigen Bedrohungsszenarien und Schutzmaßnahmen, hinsichtlich der Nutzung von Cloud-Services, ab.

Der Praxisteil der Arbeit beschreibt die Forschungsmethoden der empirischen Studie und die daraus gewonnen Ergebnisse der durchgeführten Befragung. Des Weiteren werden im Praxisteil die aus der Befragung gewonnen Daten analysiert und interpretiert. Abschließend wird die Arbeit zusammengefasst und mit der Beantwortung der Forschungsfrage abgeschlossen.

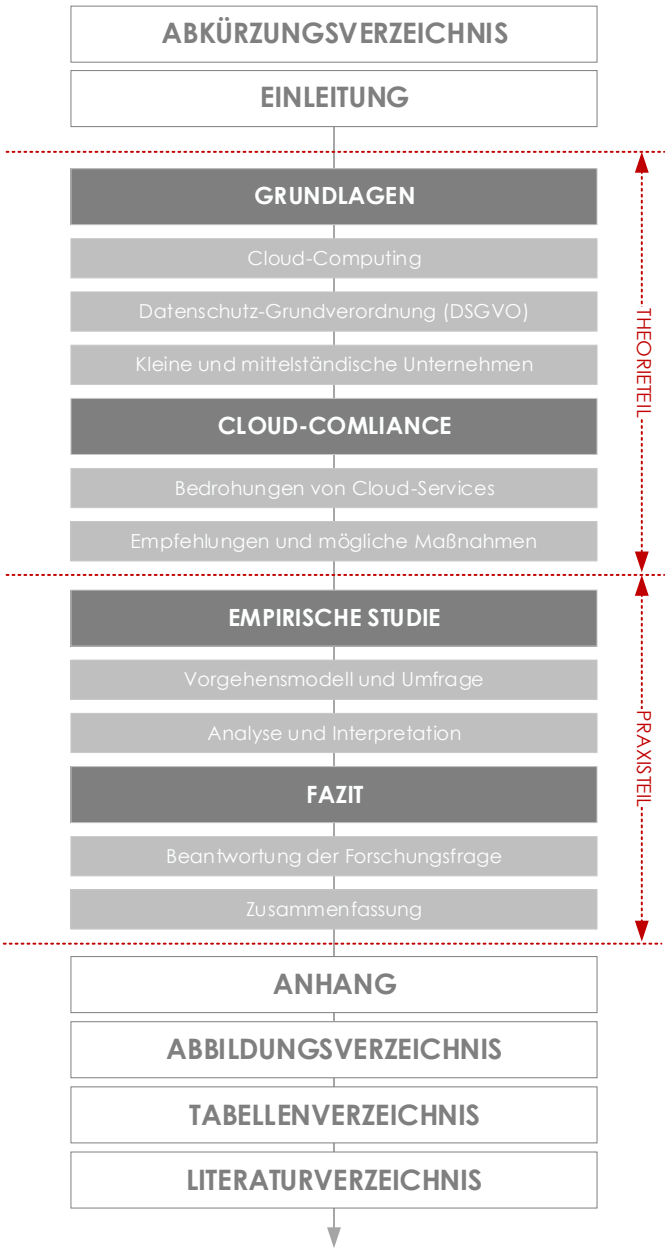


Abbildung 1 - Grafische Gliederung der Arbeit

1.4 Abgrenzung

Der Theorieteil dokumentiert die Grundlagen der wichtigsten Aspekte (Cloud-Computing, Datenschutz-Grundverordnung und KMUs) dieser Arbeit und deckt diese vollumfänglich ab. Bei diesen Aspekten handelt es sich um Informationsgrundlagen zur Beantwortung der Forschungsfrage.

Die gelisteten Cloud-Anbieter haben keinen Anspruch auf Vollständigkeit, da diese Auflistung nur jene Anbieter beinhaltet, die innerhalb des Recherchezeitraums identifiziert werden konnten.

Die möglichen Cloud-Szenarien sind Beispielszenarien, die den Cloud-Computing-Kriterien entsprechen und für KMUs ausgelegt sind. Die Cloud-Szenarien haben keinen Anspruch auf Vollständigkeit.

Die beschriebenen Empfehlungen und Rückschlüsse basieren auf den beschriebenen theoretischen Grundlagen und aus den erhobenen Werten der empirischen Studie. Des Weiteren beziehen sich diese Empfehlungen und Ergebnisse auf KMUs. Großunternehmen werden nicht berücksichtigt.

2. GRUNDLAGEN

Das zweite Kapitel dieser Arbeit gliedert sich in drei Kapitelabschnitte. Diese Kapitelabschnitte: Cloud-Computing, Datenschutz-Grundverordnung sowie kleine und mittelständische Unternehmen (kurz KMU) bilden zugleich die einzelnen Themenschwerpunkte dieser Arbeit. Neben allgemeinen Begriffsdefinitionen zu den einzelnen Themenschwerpunkten werden im Kapitelabschnitt „Cloud-Computing" die Grundlagen des Cloud-Computing erläutert. Anschließend werden die möglichen Service- und Betriebsmodelle mit den wichtigsten Merkmalen und Eigenschaften beschrieben. Am Ende des Kapitelabschnittes werden die Anwendungsbereiche und die Pro- und Contra-Argumente von Cloud-Computing abgeleitet.

Im Kapitelabschnitt „Datenschutz-Grundverordnung (DSGVO)" wird ein besonderes Augenmerk auf die Kernziele der Datenschutz-Grundverordnung gelegt. Anschließend werden die Rechte und Pflichten der Verantwortlichen, die technischen und organisatorischen Maßnahmen (kurz TOMs) sowie die Aufgaben der Datenschutzbehörde im Detail erläutert.

Abschließend wird im letzten Kapitelabschnitt des zweiten Kapitels der letzte Themenschwerpunkt „kleine und mittelständische Unternehmen" beschrieben. Dieser Kapitelabschnitt beschäftig sich mit der Differenzierung der KMUs zu anderen Unternehmensgrößen und beschreibt die Verteilung der KMUs innerhalb Österreichs.

2.1 Cloud-Computing

In diesem Kapitelabschnitt wird der Begriff „Cloud-Computing" detailliert erläutert und beschrieben. Neben der Begriffsdefinition werden verschiedene Cloud-Computing-Modelle, die Anwendungsbereiche von Cloud-Computing-Modellen und die Cloud-Anbieter sowie ihre Vor- und Nachteile beschrieben.

2.1.1 Begriffsdefinition

Die Begriffe Datenschutz, Datensicherheit und IT-Security werden in den nachfolgenden Kapiteln immer wieder verwendet. Durch die Überlappung der genannten Begriffe ist eine klare Abgrenzung nur schwer möglich. Aus diesem Grund werden nachfolgend die unterschiedlichen Ziele der drei Begrifflichkeiten definiert.

2.1.1.1 Datenschutz

Unter Datenschutz wird der Schutz der personenbezogenen Daten einer natürlichen Person verstanden. Datenschutz soll das Persönlichkeitsrecht einer natürlichen Person in Bezug auf seine personenbezogenen Daten vor einem Missbrauch schützen. Der Schutz der Daten bezieht sich im Folgenden auf die Verarbeitung, auf den unerwünschten Zugriff und den Verlust. Des Weiteren soll die Person vor den Folgen des unerwünschten Zugriffs beziehungsweise der Verarbeitung und des Verlustes geschützt werden. Die Geheimhaltung der personenbezogenen Daten ist ein weiterer zentraler Punkt des Datenschutzes. Datenschutz ist in § 1 Datenschutzgesetz (kurz DSG) als Grundrecht definiert. Dieses Grundrecht umfasst alle personenbezogenen Daten natürlicher Personen. Im Kapitelabschnitt 2.2 wird das Datenschutzgesetz im Speziellen und die EU-Datenschutz-Grundverordnung genauer erläutert. [VB18, S. 2f.]

2.1.1.2 Informationssicherheit

Der Begriff Informationssicherheit beschreibt den Schutz der Daten hinsichtlich der Schutzziele für Informationssicherheit „Vertraulichkeit, Verfügbarkeit und Integrität“ der Daten. Die Vertraulichkeit der Daten ist gegeben, wenn verhindert werden kann, dass eine nichtautorisierte Person auf die Daten zugreifen kann. Um die Verfügbarkeit der Daten sicherzustellen, müssen Datensicherungen und Zugriffsredundanzen bestehen. Die Integrität der Daten besteht, wenn die Daten in ihrer korrekten Form vorliegen und nicht missbräuchlich verändert

beziehungsweise manipuliert wurden. Informationssicherheit ist somit die Kombination aus Vertraulichkeit, Verfügbarkeit und Integrität von personenbezogenen Daten. Die EU-Datenschutz-Grundverordnung definiert im Artikel 32 Absatz 1, noch einen weiteres Schutzziel. Zu den drei genannten Schutzzielen wurde durch die DSGVO die Belastbarkeit als ein weiteres Ziel definiert. Unter Belastbarkeit versteht man die Robustheit beziehungsweise die Widerstandsfähigkeit eines IT-Systems. Die Belastbarkeit definiert, wie sicher die personenbezogenen Daten beziehungsweise die Verarbeitung der personenbezogenen Daten im Zuge auftretender Fehler oder herbeigeführter Störungen (DDoS-Attacken, etc.) eines IT-Systems sind. [Bu14, S. 70ff.]

Zusammengefasst bedeutet Informationssicherheit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme im Zusammenhang mit der Verarbeitung personenbezogener Daten sicherzustellen. [Mc18]

2.1.1.3 IT-Sicherheit

IT-Sicherheit beinhaltet technische und organisatorische Maßnahmen, um die Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit sicherzustellen. Durch den Einsatz von technischen und organisatorischen Maßnahmen soll das Risiko durch Bedrohungen auf ein angemessenes Maß reduziert werden. Des Weiteren schützt IT-Sicherheit Unternehmen und Personen vor wirtschaftlichen Schäden und Vertraulichkeitsverletzungen beziehungsweise Manipulationen. Umfassende IT-Sicherheit kann nicht durch einzelne Applikationen oder Maßnahmen erzielt werden, sondern nur durch einen Prozess, der stetig weiterentwickelt und verbessert wird. [Tr16, S. 17f.]

2.1.2 Was ist Cloud-Computing?

Der Begriff „Cloud-Computing“ ist aus der Weiterentwicklung im Bereich Hardware und Software entstanden. Cloud-Computing ist de facto nicht mehr aus der Informationstechnologie wegzudenken. Viele Unternehmen sowie private Haushalte nutzen bereits verschiedenste Formen von Cloud-Computing. Der Begriff Cloud-Computing wird vom „National Institute of Standards and Technology“ (kurz NIST) beschrieben: [Bu12, S. 14f.]

"Cloud-computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [MG11, S. 2]

Laut dieser Definition ist Cloud-Computing ein Modell, das einen bequemen, bedarfsgesteuerten Netzwerkzugriff (On-Demand Network Access) auf einen gemeinsam genutzten Pool konfigurierbarer Rechenressourcen (Ressource Pooling) möglich macht und der mit einem minimalen Aufwand durch den Cloud-Service-Provider bereitgestellt werden kann (Rapid Elasticity). Aus dieser Definition der NIST können fünf wesentliche Merkmale, die alle Cloud-Computing-Dienste gemeinsam haben, abgeleitet werden: [Ba11, S. 16]

- On-Demand Self-Service
  Nutzer können sich automatisiert Speicher- und Rechenleistungen provisionieren lassen, ohne das ein Service-Provider eingreifen muss. [Ba11, S. 16]
- Broad Network Access
  Die Funktionen sind über das Internet verfügbar und über Standardmechanismen zugänglich, die die Verwendung von heterogenen Thin- oder Thick-Client-Plattformen (z.B. Mobiltelefone, Laptops und persönliche digitale Assistenten) fördern. [Ba11, S. 17]

- Ressource Pooling

  Die zur Verfügung gestellten Ressourcen werden auf mehrere Nutzer aufgeteilt. Das bedeutet, dass die Ressourcenzuteilung der Cloud-Services nach dem aktuellen Bedarf des Nutzers erfolgen. Die Nutzer verfügen über keinerlei Informationen über die zugrunde liegenden Systeme beziehungsweise über die zugrunde liegende Hardware. [Ba11, S. 17]
- Rapid Elasticity

  Durch Cloud-Computing ist es möglich, schnell auf Ressourcenveränderungen zu reagieren. Das bedeutet, dass die zur Verfügung gestellten Ressourcen je nach Bedarf schnell nach oben oder nach unten skaliert werden können. Für den Verbraucher erscheinen die bereitgestellten Funktionen oft unbegrenzt und können in beliebiger Menge erworben werden. [Ba11, S. 17]
- Measured Service

  Cloud-Services verwalten und optimieren ihre Ressourcen anhand intelligenter Algorithmen automatisch. Somit werden anhand von Messungen Ressourcen automatisch optimiert und skaliert. [Ba11, S. 17]

NIST definiert Cloud-Computing nach den fünf wesentlichen Merkmalen, den drei Service-Modellen und den vier Betriebsmodellen. Die Abbildung 2 stellt die Definition des Cloud-Computing nach NIST grafisch dar.

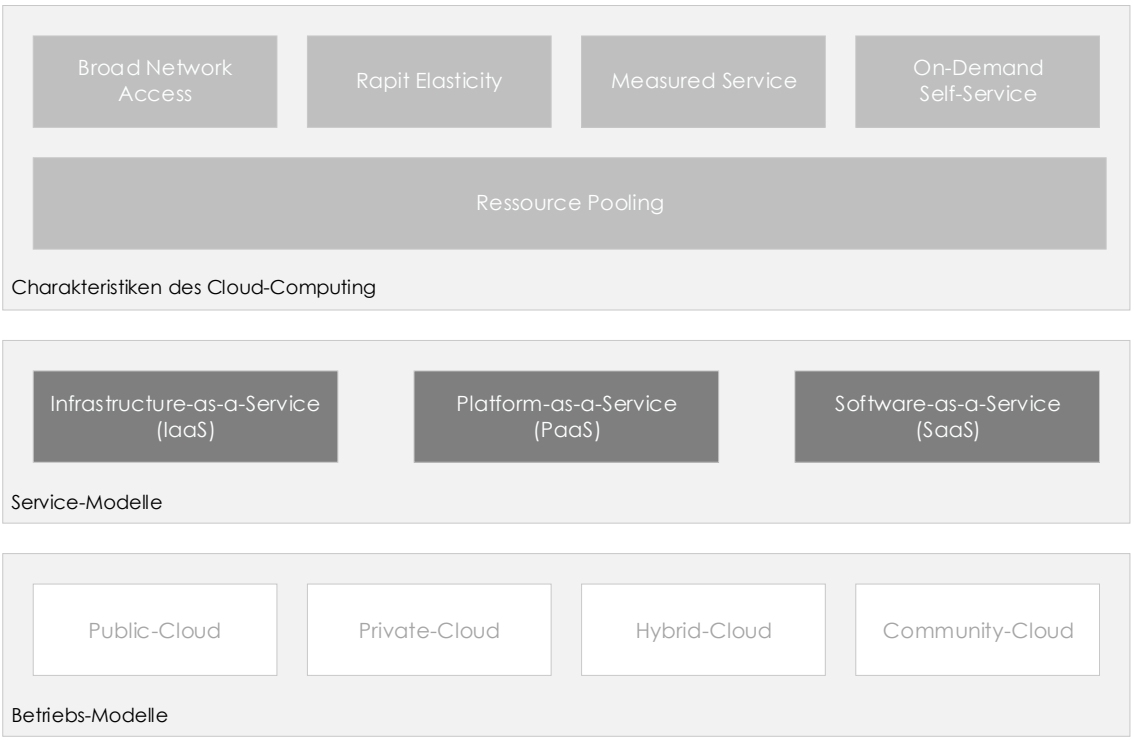


Abbildung 2 - NIST Definition Cloud-Computing [MG11, S. 2f.]

Die dargestellten Service-Modelle: Infrastrcture-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) werden im Kapitelabschnitt 2.1.3 genauer erläutert. Zudem werden nach NIST vier Betriebsmodelle unterschieden: Private-Clouds, Public-Clouds, Community-Clouds und Hybrid-Clouds. Diese Betriebsmodelle werden nachfolgend im Kapitelabschnitt 2.1.4 behandelt.

Eine weitere Begriffsdefinition zum Thema Cloud-Computing liefert das „Bundesamt für Sicherheit in der Informationstechnik“ (kurz BSI). Das BSI hat folgende Definition zum Begriff Cloud-Computing festgelegt: [Bu14]

„Cloud-Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite, der im

Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.“ [Bu14]

Den geschichtlichen Hintergrund des Begriffs „Cloud-Computing“ prägte Eric Schmidt. Eric Schmidt erfand in den 1990er Jahren den Begriff „Cloud-Computing“. Er war zu der genannten Zeit der Chief Technology Officer von Sun Microsystems und prägte den Begriff „Computer in der Cloud“. Cloud-Computing ist somit, wie bereits erarbeitet, keine neue Technologie. [Ba14, S. 41]

Thomas Barton schreibt, dass Cloud-Computing aus vier Faktoren entstanden ist. Diese Faktoren setzen sich aus der Entwicklung der Informationstechnologie und aus den Erwartungen sowie Verhalten der Nutzer zusammen. In Abbildung 3 werden die vier Entstehungsfaktoren von Cloud-Computing grafisch dargestellt. [Ba14, S. 42]

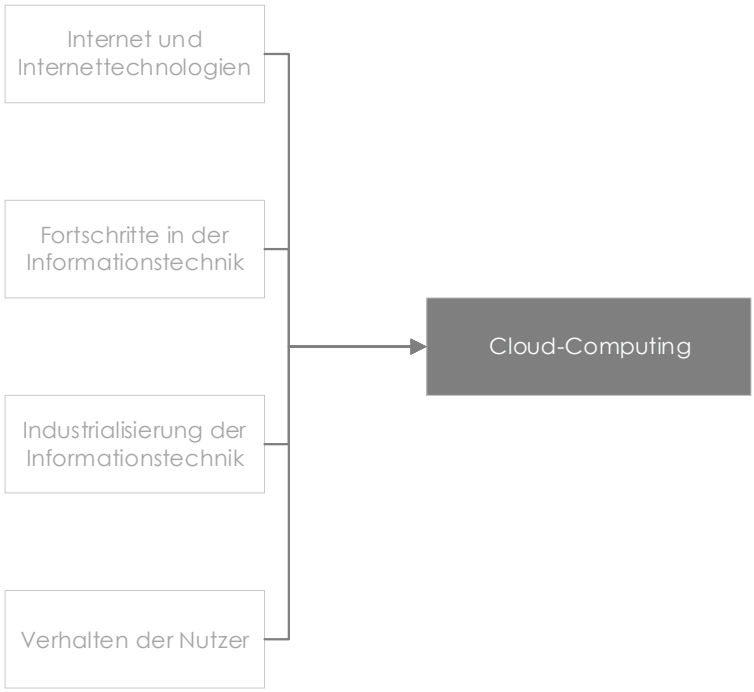


Abbildung 3 - Faktoren von Cloud-Computing [Ba14, S. 42]

Die vier Erfolgsfaktoren nach Thomas Barton werden folgend beschrieben: [Ba14, S. 42]

- Internet und Internettechnologien
  Ein wesentlicher Bestandteil von Cloud-Computing ist das Internet und die dazugehörige Internettechnologie. Durch die Internettechnologie kann das Internet als globales Kommunikationsmedium verwendet werden, Damit kann ein Zugriff auf die Informationstechnik aufgebaut werden.
- Fortschritte in der Informationstechnik
  Der kontinuierliche Fortschritt in der Informationstechnik hat dazu geführt, dass Infrastrukturkomponenten ein stetiges Leistungswachstum erfahren haben und zugleich die Preise der Komponenten gesunken sind.
- Industrialisierung der Informationstechnik
  Durch die Weiterentwicklung der Informationstechnik im Industriebereich wurde Cloud-Computing sehr stark beeinflusst. Besonders das Cloud-Service-Modell „Software-as-a-Service" wurde durch die Industrie sehr stark beeinflusst und weiterentwickelt. Die Weiterentwicklung und die daraus gewonnen Erkenntnisse aus der Industrie, insbesondere bei der Entwicklung und Bereitstellung von Software, hat Cloud-Computing sehr stark beeinflusst.
- Verhalten der Nutzer
  Einer der wichtigsten Erfolgsfaktoren von Cloud-Computing ist das Verhalten sowie die Erwartungen der Nutzer. Das Verhalten der Nutzer hat gezeigt, dass Sie von jedem Ort, zu jeder Zeit und von jedem Endgerät aus – anytime, anywhere, anydevice (kurz ATAWAD) – auf Ihre beruflichen und privaten Daten, Anwendungen oder Services zugreifen wollen.

Zusammengefasst kann der Begriff Cloud-Computing wie folgt beschrieben werden. Der Begriff wurde in den 1990er Jahren von Eric Schmidt erfunden und wurde durch die vier beschriebenen Entstehungsfaktoren weiterentwickelt. Durch die stetige Weiterentwicklung der Internet- und Informationstechnologien

und durch das Verhalten sowie die Erwartungen der Nutzer ist Cloud-Computing im beruflichen und privaten Umfeld allgegenwärtig. Cloud-Computing ist somit ein Modell, das einen allgegenwärtigen, bequemen und bedarfsgesteuerten Netzwerkzugriff auf einen gemeinsam genutzten Pool konfigurierbarer Rechenressourcen (z.B. Netzwerke, Server, Speicher, Anwendungen und Dienste) ermöglicht, der mit minimalem Verwaltungsaufwand schnell bereitgestellt ist. [Ba14, S. 42ff.]

Im nachfolgenden Kapitelabschnitt werden die Service-Modelle des Cloud-Computing aufgelistet und beschrieben.

2.1.3 Service-Modelle

Die Cloud-Service-Modelle werden in drei Hauptservices unterteilt. Diese dienen dazu, die Cloud-Services logisch zu trennen. Die Einteilung dieser Services erfolgt auf Basis der angebotenen Dienstleistungen, auf Basis der Anwendungen und auf Basis der Infrastruktur. Alle Cloud-Services bauen aufeinander auf und sind miteinander verknüpft. In der Regel wird nicht nur ein Service-Modell genutzt, sondern eine Kombination aus mindestens zwei Modellen. Alle Arten von Cloud-Service-Modellen werden unter dem Begriff „Everything-as-a-Service (XaaS) zusammengefasst. Unter XaaS kann jegliche Dienstleistung, Anwendung und Infrastruktur als Cloud-Service angeboten werden. [VHH13, S. 19]

2.1.3.1 Infrastructure-as-a-Service (IaaS)

Das Cloud-Service-Modell „Infrastructure-as-a-Service“ bietet dem Anwender die Nutzung der infrastrukturellen Dienste. Somit bekommt der Anwender die Möglichkeit, Speicher, Rechenleistung, Netzwerkbandbreite und auch weitere virtuelle Hardwareressourcen zu nutzen. Somit können vollwertige Infrastrukturen aus der Cloud bezogen werden, ohne physische Hardwareressourcen selbst zu betreiben. Zudem ist dieser Dienst mit einer sehr hohen Flexibilität verbunden. Diese Flexibilität hat den Vorteil, dass eine Aufrüstung von Rechnerleistung oder

Speicher jederzeit möglich ist. Details über die zugrunde liegenden Infrastrukturkomponenten bleiben dem Nutzer verborgen, darauf hat der Nutzer keinen Zugriff beziehungsweise keine Kontrolle. [Ba11, S. 17]

2.1.3.2 Platform-as-a-Service (PaaS)

Das Cloud-Service-Modell „Platform-as-a-Service" richtet sich an Nutzer, die ihre eigenen Applikationen entwickeln, betreiben und für weitere Nutzer bereitstellen möchten. Die Entwicklung und Bereitstellung der Anwendungen erfolgt mittels verschiedener Tools und Programmiersprachen und auf Basis der zugrunde liegenden virtuellen Infrastruktur. Im Gegensatz zu IaaS übernimmt hier der Nutzer die Kontrolle, die Bereitstellung und die Administration der virtuellen Intrastruktur, des Betriebssystems und der Anwendungen. [Ba11, S. 17]

2.1.3.3 Software-as-a-Service (SaaS)

Das Cloud-Service-Modell „Software-as-a-Service" bietet dem Nutzer Applikationen, die vom Anbieter entwickelt wurden, über die vom Anbieter bereitgestellte virtuelle Infrastruktur genutzt werden können. Der Nutzer hat dabei keinen Zugriff auf die darunterliegende Infrastruktur. Er hat lediglich die Möglichkeit, die Applikation beziehungsweise Software über vordefinierte Schnittstellen zu nutzen. Bekannte Beispiele sind Services wie Microsoft Office 365 und Google Docs. [Ba11, S. 9]

2.1.3.4 Everything-as-a-Service (XaaS)

Neben den drei Haupt-Service-Modellen existiert eine weiterer Cloud-Service. Das Cloud-Service-Modell „Everything-as-a-Service" beschreibt alle Dienste und Services, die im Zusammenhang mit dem zugrunde liegenden Grundgedanken „as-a-Service" stehen. Somit basiert dieses Modell nicht nur auf rein informationstechnologischen Service-Modellen, sondern allein auf der Idee des „Ressource Pooling". Als Beispiel kann „Human-as-a-Service" genannt werden.

Dieses Service-Modell beschreibt die menschliche Ressourcenbereitstellung. [Wi19b]

In der nachfolgenden Abbildung 4 wird eine grafische Darstellung der Cloud-Services-Architekturen zusammengefasst. In dieser Grafik werden die Verantwortlichkeiten des Nutzers und des Providers dargestellt.

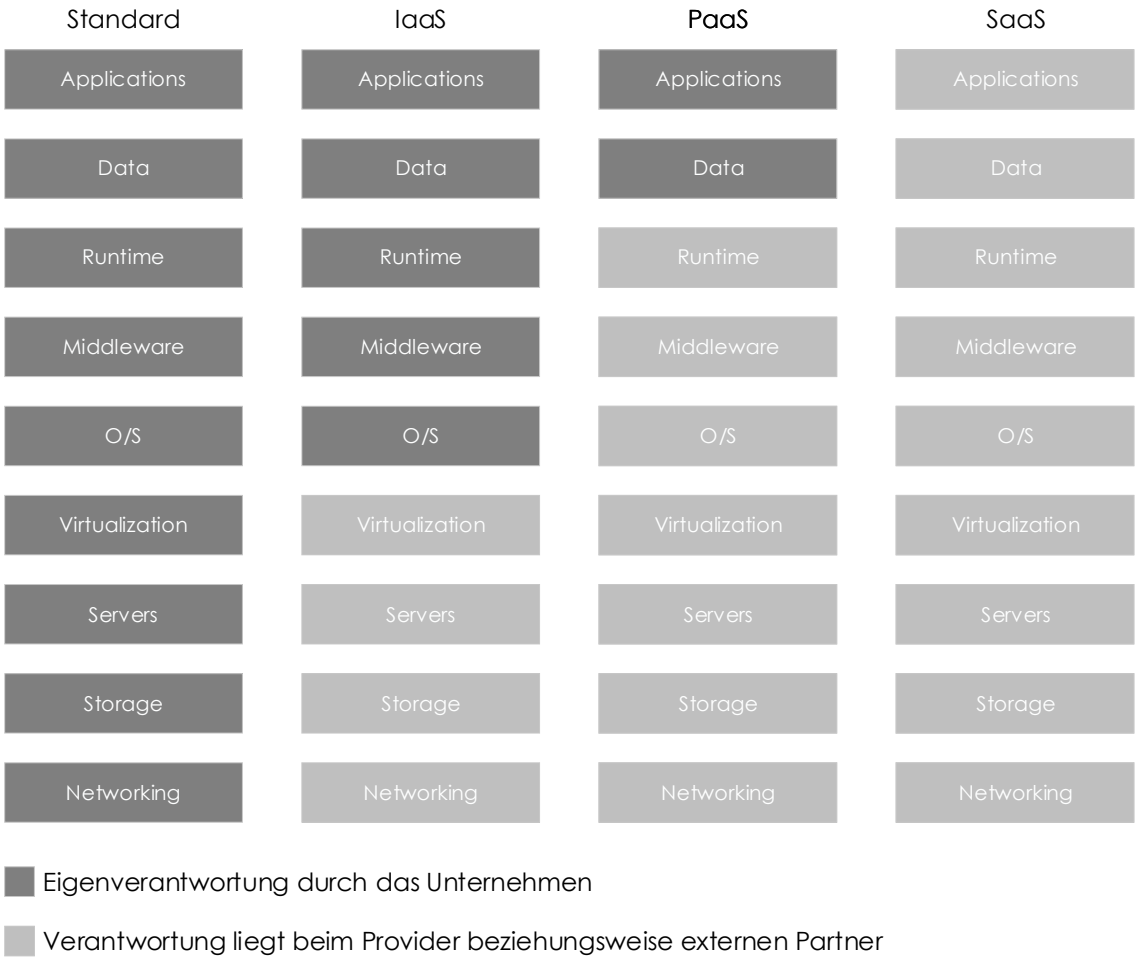


Abbildung 4 - Cloud-Service-Architektur [HY10, S. 11]

Nach der Erläuterung der Cloud-Service-Modelle in diesem Kapitelabschnitt folgt im nächsten Kapitelabschnitt die Aufzählung und Beschreibung der verschiedenen Betriebsmodelle.

2.1.4 Betriebsmodelle

Die Betriebsmodelle werden im Gegensatz zu den Service-Modellen aus der organisatorischen Sicht und nicht aus der technischen Sicht betrachtet. In diesem Kapitel werden die vier Betriebsmodelle nach NIST erläutert. Die Betriebsmodelle unterscheiden sich nach der Nutzungsform, dem Eigentum der zugrunde liegenden Infrastruktur oder auch der Integration von Services in bestehende Organisationsformen. Die Abbildung 5 stellt die vier Betriebsmodelle grafisch dar. Anschließend werden die vier Betriebsmodelle (Private-Cloud, Public-Cloud, Hybrid-Cloud und Community-Cloud) im Detail erläutert. [Ba14, S. 46]

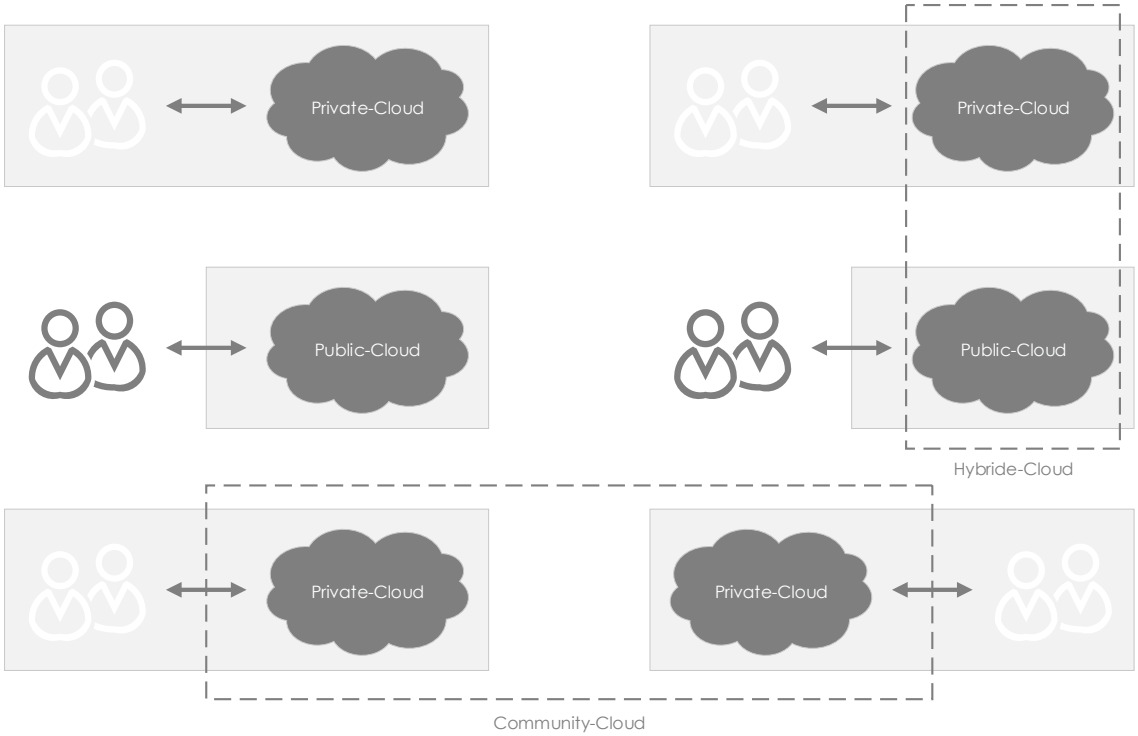


Abbildung 5 - Cloud-Service-Betriebsmodelle

2.1.4.1 Public-Cloud

Public-Cloud-Modelle, auch öffentliche Cloud genannt, können von der breiten Öffentlichkeit genutzt werden. Die Nutzer, die aus verschiedenen Nutzergruppen

bestehen können, teilen sich die zugrunde liegende Infrastruktur und nutzen die für sie bereitgestellten Services. Die Nutzung des Service wird vom Service-Provider über ein Berechtigungskonzept geregelt und gesteuert. Der Service-Provider ist für die Verwaltung, Administration und Sicherheit sowie die Verfügbarkeit des Service verantwortlich. Die Nutzer können rein über Service-Level-Agreements (kurz SLAs) das Service steuern. Die Anbindung der Cloud-Services erfolgt über das Public-Internet. [MPR15, S. 13f.]

2.1.4.2 Private-Cloud

Im Gegensatz zur Public-Cloud, besitzt bei einer Private-Cloud nur eine Organisation beziehungsweise ein Nutzer Zugriff auf die Cloud-Services. Der Zugang für die breite Öffentlichkeit bleibt bei diesem Modell verwehrt. In der Regel steht die zugrunde liegende Infrastruktur im Rechenzentrum des Unternehmens und wird auch vom Unternehmen selbst administriert und verwaltet. Natürlich kann das Service auch ausgelagert werden. Somit wird die Infrastruktur von einem Partner zur Verfügung gestellt und administriert. Die Steuerung des Partners kann mittels Service-Level-Agreements erfolgen. Im Gegensatz zur Public-Cloud kann eine Private-Cloud die vollen Potenziale der Skalierbarkeit nicht ausnutzen. Somit können dem Nutzer weniger Ressourcen zur Verfügung gestellt werden als bei Public-Cloud-Modellen. Aus der Sicht des Datenschutzes und der Datensicherheit werden Unternehmen das Private-Cloud-Modell bevorzugen. Bei Private-Cloud können die Sicherheitsfaktoren selbst bestimmt werden. Bei Public-Cloud-Modelle sind diese Faktoren vom Anbieter abhängig. [MPR15, S. 14]

2.1.4.3 Hybrid-Cloud

Das Hybrid-Cloud-Modell ist eine Mischform von Private-Cloud und Public-Cloud. Diese Form vereint die Vor- und Nachteile der oben beschriebenen Cloud-Modellen. Durch diese Form kann der beschriebene Nachteil der Private-Cloud behoben werden. Durch die Anbindung von Ressourcen einer Public-Cloud

können Lastspitzen leichter bewältigt werden. Die Skalierbarkeit der Public-Cloud kann die „Trägheit“ der Private-Cloud bei Lastspitzen ausgleichen. Auch die Datenschutzproblematik bei Public-Cloud-Modellen können durch Hybrid-Cloud-Modelle behoben werden. Ziel einer Hybrid-Cloud-Umgebung ist es, die Vorteile der einzelnen Modelle auszunutzen, um somit eine geeignete Umgebung für das Unternehmen aufzubauen. [MPR15, S. 14]

2.1.4.4 Community-Cloud

Bei Community-Clouds handelt es sich um einen Zusammenschluss von mehreren Private-Cloud-Umgebungen. Auf diese Umgebung haben definierte Unternehmen beziehungsweise Nutzer Zugriff, die dieselben Cloud-Services nutzen. Die Verwaltung kann durch die Unternehmen selbst, aber auch durch einen externen Dienstleister erfolgen. Diese Form wird meistens von KMUs genutzt, die zwar eine Private-Cloud wünschen oder fordern, aber aufgrund der Größe diese Anforderungen allein nicht erfüllen können. [Bu17, S. 8]

Jedes dieser vier Betriebsmodelle bietet Vor- und Nachteile in Bezug auf die Skalierbarkeit, Performance, Kosten und Sicherheit. Somit ist es für jedes Unternehmen zwingend notwendig, die Kriterien zu definieren. Im nächsten Kapitelabschnitt werden die Cloud-Service-Kriterien aufgelistet und beschrieben.

2.1.5 Übersicht von Cloud-Services-Kriterien

Die Auswahl des Cloud-Anbieters kann durch verschiedene Kriterien erfolgen. Um den Nutzern beziehungsweise den Unternehmen die Auswahl zu erleichtern, hat das „Trust Cloud Kompetenznetzwerk e.V.“ einen Cloud-Kriterienkatalog veröffentlicht. Dieser Katalog definiert Mindestanforderungen, die ein Cloud-Service erfüllen muss, um das „Trusted-Cloud-Label“ zu erlangen. Dieser Kriterienkatalog ist für die Nutzer transparent gestaltet und er ist geeignet für die Auswahl beziehungsweise den Vergleich von Cloud-Services in Bezug auf Datensicherheit, Datenschutz (DSGVO), Rechtskonformität, Integrierbarkeit und

Investitionssicherheit. Die aktuelle Version 2.0 - die am 30. Mai 2018 veröffentlicht wurde – verfügt über die datenschutzrechtlichen Aspekte der EU-Datenschutz-Grundverordnung in Bezug auf die Verarbeitung von personenbezogenen Daten. [Bu18, S. 2ff.]

Der Kriterienkatalog besteht aus zehn Hauptbereichen, die wiederum in mehrere Unterbereiche gegliedert wurden. Folgend werden die Ziele der Hauptbereiche und Unterbereiche des Kriterienkatalogs beschrieben: [Bu18, S. 12ff.]

2.1.5.1 Anbieter

Im ersten Bereich „Anbieter“ wird die Organisation geprüft. So werden die Rechtsform, die Gesellschafter und die Erfahrung des Anbieters in Bezug auf die Bereitstellung von Cloud-Services geprüft. Des Weiteren wird die Auditierbarkeit des Anbieters geprüft.

2.1.5.2 Service

Die funktionalen Anforderungen an das Service werden im zweiten Bereich „Service“ untersucht. In diesem Bereich wird zudem der Reifegrad des Service, die Referenzen, die Ansprechpartner und die Umsetzungsszenarien geprüft. Des Weiteren wird in diesem Bereich die Art der zu verarbeitenden Daten definiert.

2.1.5.3 Subunternehmer und Rechenzentren

Im dritten Bereich „Subunternehmer und Rechenzentren“ wird das Unternehmensprofil erläutert. Angaben zu der Unternehmensgröße, zur Anzahl der Mitarbeiter, zu den Hauptgeschäftsfeldern und den Standorten der Rechenzentren sowie eventuelle Subunternehmen werden aufgezeigt.

2.1.5.4 Zertifikate

Der Bereich „Zertifikate“ listet alle Zertifikate/Gütesiegel des Anbieters, des Subunternehmers, der Rechenzentren und des Services auf.

2.1.5.5 Vertrag

Allgemeine Vertragsbedingungen, Rechts- und Gerichtsstand, Angaben zu Service-Level-Agreements, Preismodell, Angaben zu Change-Management und auch Angaben zu Urheber- und Nutzungsrechten werden im fünften Bereich „Vertrag“ festgelegt.

2.1.5.6 Sicherheit

Der Bereich „Sicherheit“ prüft die Effizienz des Anbieters beziehungsweise des Service in Bezug auf das Management von Sicherheitsvorfällen. Des Weiteren wird der Nachweis von Sicherheitszertifikaten und IT-Sicherheitsmaßnahmen (BSI-Grundschutz, ISO/IEC 27001, etc.) geprüft. Die Umsetzung von Verschlüsselungsverfahren und von Identity- und Accessmanagement sind ein weiterer Punkt im Bereich „Sicherheit“.

2.1.5.7 Datenschutz

Im Bereich Datenschutz werden die technischen und organisatorischen Maßnahmen (kurz TOMs), die formalen Datenschutzanforderungen sowie die Nachweispflichten gemäß der EU-Datenschutz-Grundverordnung geprüft. Ein weiteres Hauptaugenmerk wird auf die Lokalisierung der Datenhaltung, die Umsetzung der Betroffenenrechte und die Ausbildung und Zertifizierung der Mitarbeiter gelegt. Die Begrifflichkeiten der EU-Datenschutz-Grundverordnung werden im Kapitelabschnitt 2.2 detailliert erläutert.

2.1.5.8 Operative Prozesse

Der Bereich „Operative Prozesse“ prüft den Nachweis auf ein effizientes Service-Management zur Gewährleistung der definierten Servicequalität sowie die Angaben zu Backups, zur Provisionierung des Services und den Support-Leistungen.

2.1.5.9 Interoperabilität und Portabilität

Die Darstellung der technischen Standards, der Zugriffs- und Exportverfahren der Daten, der Integration des Cloud-Services auf die bestehende IT-Infrastruktur und die technische und organisatorische Nutzung des Cloud-Services wird im Bereich „Interoperabilität und Portabilität“ geprüft.

2.1.5.10 Architektur

Im anschließenden Bereich „Architektur“ werden die Maßnahmen zur technischen und organisatorischen Isolation über Mandantenfähigkeit des Cloud-Service geprüft. Des Weiteren wird das Augenmerk auf die technische Skalierbarkeit des Service gelegt.

Zusammenfassend können folgende Ziele beschrieben werden: [Bu18, S. 12ff.]

- Darstellung des Anbieters, der zugehörigen Beteiligungsverhältnisse und des Bereitstellungs-Knowhows in Bezug auf Cloud-Services.
- Eine vollständige funktionale Beschreibung des Cloud-Service.
- Die Definition der Service-Erbringung.
- Nachweis der Zertifikate/Gütesiegel sowie aller relevanten Vertragsbedingungen der Anbieter und Subunternehmer.
- Darstellung aller technischen und organisatorischen Maßnahmen in Bezug auf die IT-Sicherheit und den Datenschutz.
- Definition und Darstellung der operativen Prozesse und der dazugehörigen Service-Level-Agreements (SLAs).
- Die Maßnahmen zur Migration und Nutzung des Services und die Definition und Beschreibung der zugrundeliegenden Infrastruktur.

2.1.6 Anwendungsbereiche von Cloud-Services

Die Nutzungsmöglichkeiten und Anwendungsbereiche von Cloud-Computing-Services sind sowohl im privaten als auch im beruflichen Bereichen vielzählig.

Besonders für Unternehmen und Organisationen weisen Cloud-Services ein breites Spektrum an neuen Möglichkeiten auf. Die Grundlage dafür bieten die im Kapitelabschnitt 2.1.3 beschriebenen Cloud-Service-Modelle. In den nachfolgenden Kapitelabschnitten werden die Anwendungsbereiche der im Kapitelabschnitt 2.1.3 beschriebenen Service-Modelle IaaS, PaaS, SaaS und XaaS erläutert.

2.1.6.1 Anwendungsbereiche von „Infrastructure-as-a-Service (IaaS)"

Durch die Anschaffung und den Betrieb von IT-Infrastrukturen fallen bei Unternehmen sehr hohe Fixkosten an. Das betrifft alle Unternehmensgrößen, jedoch sind die Kosten je nach Größe des Unternehmens unterschiedlich. Viele Start-ups und KMUs investieren nicht mehr in eigene IT-Infrastrukturen, sondern lagern diese über IT-Outsourcing an einen Cloud-Service-Provider aus. Das hat den Vorteil, dass die Investitionskosten verringert werden und die Kosten dadurch variabilisiert werden. Des Weiteren können durch den Bezug von IaaS Lastspitzen einfacher abgedeckt werden, als es mit der eigenen Infrastruktur der Fall ist. IaaS zeichnet sich nicht nur durch Investitionsersparnisse und die ressourceneffiziente Nutzung der IT-Infrastruktur aus, sondern auch durch weitere Kostenersparnisse in den Bereichen Betreuungsressourcen (Personal), Wartungskosten und Infrastrukturkosten wie Strom und Miete. Zu diesen direkten Ersparnissen kommen noch die indirekten Ersparnisse, die sich durch die Konzentration und Intensivierung auf das Kerngeschäft des Unternehmens ergeben. Zusammengefasst wird bei einer Nutzung von IaaS der Betrieb sowie die Betreuung der IT-Infrastruktur von einem externen Cloud-Service-Provider übernommen und die benötigten Services werden über ein Pay-Per-Use-Model von dem externen Cloud-Service-Provider bezogen. Das Unternehmen kann somit auf hohe Investitionen im Bereich IT-Infrastruktur verzichten und sich auf sein Kerngeschäft konzentrieren. [MPR15, S. 10]

Die Top-3 Anbieter im IaaS-Bereich sind Amazon Web Service (AWS), Microsoft Azure und Google Cloud Platform (GCP). [Wi19b]

2.1.6.2 Anwendungsbereiche von „Platform-as-a-Service (PaaS)“

Plattform-as-a-Service bietet speziell Unternehmen die Möglichkeit, eigene Applikationen rasch und einfach zu veröffentlichen. Zudem besteht die Möglichkeit, Anwendungen als Software-as-a-Service den eigenen Kunden zur Verfügung zu stellen. PaaS zeichnet sich durch seine schnelle und unkomplizierte Aktualisierbarkeit aus. Durch eine im Hintergrund einheitliche IT-Infrastruktur und Laufzeitumgebung müssen keine zusätzlichen Anpassungen vor der Veröffentlichung vorgenommen werden. Unternehmen können mittels PaaS schnell und unkompliziert eigene Applikationen veröffentlichen und durch Kombination mit SaaS diese Applikationen den Kunden bereitstellen, ohne Rücksicht auf die zugrunde liegende IT-Infrastruktur zu legen, die mittels IaaS bereitgestellt wird. [MPR15, S. 10]

Die bekanntesten Beispiele für Plattform-as-a-Service sind Microsoft Azure, Google App Engine und SAP Cloud Plattform. [Wi19b]

2.1.6.3 Anwendungsbereiche von „Software-as-a-Service (SaaS)“

Software-as-a-Service wird sehr stark durch das Verhalten der Nutzer beeinflusst. Der „Arbeitsplatz der Zukunft“ basiert auf dem Prinzip „anywhere, anytime, anydevice“. An jedem Ort, zu jeder Zeit und mit jedem Gerät auf die gewünschten Daten und Applikationen zugreifen zu können, bieten Software-as-a-Service-Lösungen. Die Nutzung von SaaS bringt Kostenersparnisse durch effiziente Lizenznutzung (Pay-Per-Use-Modell) und durch weniger lokale Installationen auf den Endgeräten. SaaS wird von Cloud-Service-Providern über definierte Schnittstellen dem Nutzer bereitgestellt. Durch Dienste wie „Microsoft Active Directory Federation Services (ADFS)“ können Schnittstellen zu Cloud-

Diensten kontrolliert aufgebaut und gesteuert werden. Die Benutzerverwaltung der Software-Dienste erfolgt über die definierten Benutzerrechte. [MPR15, S. 11]

Der Zugang zu den Applikationen erfolgt in der Regel über einen Webbrowser. In der Tabelle 1 wurden die bekanntesten SaaS-Bereiche und die dazugehörigen Anbieter dargestellt:

Bereich	Anbieter / Lösung
Collaboration	Cisco WebEx, Google Meet
Office	Microsoft Office 365, GoogleDocs
E-Mail	Microsoft Outlook Online, GoogleMail
Security	Sophos Central, Ikarus
Content Management	WordPress
CRM-Systeme	SAP HANA, Microsoft Dynamics

Tabelle 1 – SaaS-Bereiche und -Anbieter

2.1.6.4 Anwendungsbereiche von „Everything-as-a-Service (XaaS)“

Wie schon im Kapitelabschnitt 2.1.3.4 beschrieben, handelt es sich bei XaaS um Dienste, die nicht nur Cloud-Services zugeordnet werden. Für Unternehmen ergeben sich durch Everything-as-a-Service zahlreiche Anwendungsbereiche. Einige Anwendungsbereiche werden in dieser Arbeit näher dargestellt. [Wi19b]

- Backup-as-a-Service
  Bei Backup-as-a-Service handelt es sich um einen Backupdienst aus der Cloud. Damit haben Unternehmen und private Nutzer die Möglichkeit, Backups nicht mehr nur auf der lokalen Infrastruktur zu sichern, sondern auch zusätzlich oder ausschließlich auf einem Cloud-Speicher zu sichern. Diese Möglichkeit bietet einen zusätzlichen Sicherheitsfaktor für besonders wichtige Daten und auch einen Kostenvorteil für die Nutzer. Die Verrechnung erfolgt durch Pay-Per-Use. Das bedeutet, dass nur belegter

Speicher verrechnet wird. Außerdem können interne Ressourcen eingespart werden. Den Betrieb und die Wartung übernimmt der Cloud-Service-Provider. [Ta14]

- Desktop-as-a-Service (DaaS)
  Hierbei handelt es sich um eine kostengünstige Alternative zu den Fat-Clients. Durch das Desktop-as-a-Service-Modell ist es möglich, Desktops über eine virtuelle Umgebung schnell und effizient den Nutzern zur Verfügung zu stellen. Diese Methode empfiehlt sich für große und standardisierte Unternehmen mit einem leistungsfähigen Netzwerk. Da die Daten und die Systeme nicht mehr lokal auf der Peripherie gespeichert werden, müssen sämtliche Daten über das Netzwerk übertragen werden. Damit kann das Netzwerk auch zum „Show-Stopper" werden. Wenn das Netzwerk beziehungsweise die Internetverbindung nicht verfügbar ist, dann kann der virtuelle Desktop nicht aufgerufen und genutzt werden. [He16]
- Database-as-a-Service (DBaaS)
  Datenbankserver benötigen viel Speicher und eine hohe Rechenleistung. Durch DBaaS können Datenbanken in die Cloud ausgelagert werden und müssen Unternehmen Datenbankserver nicht mehr selbst betreiben. [Wi19a]
- Humans as a Service (HuaaS)
  Darunter versteht man die menschliche Intelligenz, die über einen Webservice genutzt werden kann. So werden kleine Aufgaben von Menschen über das Internet organisiert und erledigt. [Wi19b]
- Storage-as-a-Service (StaaS)
  Um Spitzen im Speicherbereich abzudecken, setzten Unternehmen auf StaaS. Zusätzlicher Speicherbedarf kann durch dieses Cloud-Service schnell und effizient abgedeckt werden. Des Weiteren kann das Service für neue Unternehmen beziehungsweise Start-ups interessant sein. Diese

Unternehmen befinden sich im Aufbau und können den Speicherbedarf nur schwer abschätzen. [Ro16]

Die Anwendungsmöglichkeiten von Cloud-Computing sind für private Nutzer, besonders aber für Unternehmen vielfältig. In diesem Kapitelabschnitt wurden einige Anwendungsbereiche und dazugehörige Vor- und Nachteile erläutert. Im nächsten Kapitelabschnitt werden die Pro und Contra von Cloud-Computing im Detail aufgelistet.

2.1.7 Pro und Contra von Cloud-Services

Durch Cloud-Services gehen nicht nur Vorteile einher, die Nutzung von Cloud-Services ist auch mit einigen Nachteilen behaftet. In diesem Kapitelabschnitt werden die Pro und Contra von Cloud-Computing zusammengefasst und erläutert.

2.1.7.1 Pro-Argumente von Cloud-Services

- Direkter Kostenvorteil
  Wie schon in den vorhergehenden Kapitelabschnitten erläutert, spielt der Kostenvorteil eine sehr große Rolle bei Cloud-Services. Eine effiziente Nutzung von Cloud-Produkten kann zu einer signifikanten Ersparnis in der IT-Infrastruktur führen. Somit können Unternehmen durch den Wegfall von Ressourcen (Mitarbeiter), Räumlichkeiten und Stromverbrauch, erhebliche Kosten einsparen. Des Weiteren entfallen hohe Investitionskosten und Wartungskosten. Diese Kosten werden wiederum in variable Kosten umgewandelt und entfallen somit nicht gänzlich. [Mü09, S. 44]
- Indirekter Kostenvorteil
  Diese Kostenvorteile ergeben sich durch eine kurz- oder langfristige Nutzung von Cloud-Services und sind nicht direkt zu beziffern. Diese Vorteile ergeben sich aus der Organisation. Durch den Wegfall der IT-

Infrastruktur kann sich das Unternehmen auf das Kerngeschäft konzentrieren und die Schwerpunkte innerhalb der Organisation auf das Wesentliche verlagern. Dies ist speziell für Unternehmen relevant, die sich nicht vorrangig in der ITK-Branche befinden. [Mü09, S. 44]

- Verfügbarkeit
  Cloud-Services können über das Netzwerk beziehungsweise das Internet von jedem Ort aus erreicht und genutzt werden. Das bedeutet eine ständige Verfügbarkeit der Dienste für den Nutzer. Durch SLAs wird vom Cloud-Service-Provider die Verfügbarkeit des Service festgelegt. [Mü09, S. 41]
- Risikotransfer
  Durch die Auslagerung der IT-Infrastruktur an den Cloud-Service-Provider entfällt nicht nur der administrative Aufwand sondern auch das Risiko. Das Risiko für Ausfälle, Angriffe oder weitere technische Probleme wird an den Provider ausgelagert. [Mü09, S. 49]
- Aktualität
  Die Aktualität speziell bei Softwareanwendungen kann durch SaaS bedeutend verbessert werden. Updates und Neuerungen werden über eine zentrale Stelle eingespielt und durchgeführt. Somit können Sicherheitslücken schnell und effizient geschlossen werden. [Mü09, S. 67]
- Skalierbarkeit
  Durch die Skalierbarkeit bei Cloud-Services können Spitzenauslastungen schnell und flexibel abgedeckt werden. Es sind keine Investitionen oder zusätzliche Hardware-Komponenten notwendig. [Mü09, S. 50]

2.1.7.2 Contra-Argumente von Cloud-Services

- Anbieterauswahl
  Die Anbieterauswahl gestaltet sich durch fehlende Standards und Normen sehr schwierig und aufwändig. Durch den beschriebenen Kriterienkatalog von „Trusted Cloud“, der bereits im Kapitelabschnitt 2.1.5

beschrieben wurde, kann man mittels eines definierten Ablaufs die Anbieter vergleichen und auswählen. Durch diesen Kriterienkatalog bekommt man einen guten Überblick über die evaluierten Cloud-Service-Provider. [MÜ09, S. 50]

- Rechtslage und Sicherheit

  Die Rechtslage ist aufgrund vielzähliger rechtlicher Faktoren und im Zusammenhang mit der Lokalität der Datenablage sehr unübersichtlich. Das Vertragsrecht von Cloud-Diensten lässt sich oftmals nur sehr schwer einordnen. Man unterscheidet zwischen Werkvertrag und Mietvertrag. Es gibt aber auch eine Mischung aus beide. Unternehmen haben je nach Vertrag nur begrenzten Einfluss auf Erfüllung oder Kompensation der vertraglichen Verpflichtungen. Durch die internationale Ausrichtung der Cloud-Provider stellt sich die Frage des Datenschutzes und der Datensicherheit. Unternehmen stehen vor der Herausforderung, sensible und personenbezogene Daten nach der EU-Datenschutz-Grundverordnung zu schützen. Deshalb ist es zwingend notwendig, den Speicherort der Daten vertraglich festzulegen. Die Datensicherheit wird an den Cloud-Service-Provider ausgelagert. Der Service-Provider muss vertraglich verpflichtet werden, seine IT-Infrastruktur auf dem „aktuellen Stand der Technik“ zu halten. Trotz allem ist es notwendig, eigene Sicherheitsmaßnahmen speziell im Bereich der Verschlüsselung zu implementieren. [MÜ09, S. 53f.]

- Verfügbarkeit

  Die ständige Verfügbarkeit von Cloud-Services ist von der Verfügbarkeit und Verlässlichkeit der Netzwerk- und Internetverbindung abhängig. Durch einen Ausfall von zentralen Netzwerkkomponenten wird die Verfügbarkeit von Cloud-Diensten gefährdet. Des Weiteren können Störungen des Internet-Service-Providers den Zugriff auf die Cloud-Services unterbinden. Diese Unterbrechungen können durch redundante Netzwerkkomponenten und Internet-Outbreaks reduziert

beziehungsweise verhindert werden. Die Verfügbarkeit des Cloud-Providers muss wiederum über SLAs definiert werden. [Mü09, S. 41]

- Performance
  Die Performance von Cloud-Services ist sehr von der Geschwindigkeit der Netzwerk- beziehungsweise Internetverbindung abhängig. Kommt es zu einem erhöhten Datentransfer beziehungsweise ist die Verbindung unterdimensioniert, dann kann es zu Performance-Einbußen kommen. [De10, S. 42]

2.1.8 Zusammenfassung

Im Kapitelabschnitt 2.1 wurde das Thema „Cloud-Computing" mit den existierenden Betriebs- und Servicemodellen detailliert beschrieben. Des Weiteren wurden die zahlreichen Anwendungsmöglichkeiten von Cloud-Computing für Unternehmen sowie für private Endnutzer dargestellt. Das Ende des Kapitelabschnitts beschäftigte sich mit den Pro- und Contra-Argumenten von Cloud-Services. Diese beschriebenen Vor- und Nachteile sind sehr stark von den einzelnen Unternehmen beziehungsweise Organisationen und deren Anforderungen abhängig. Deshalb können diese Vor- und Nachteile nicht pauschaliert auf alle Unternehmen umgelegt werden, sondern müssen für jedes Unternehmen neu evaluiert werden.

Der nächste Kapitelabschnitt erläutert die EU-Datenschutz-Grundverordnung (kurz DSGVO). Für die Beantwortung der Forschungsfrage ist die theoretische Ausarbeitung des Kapitelabschnitts 2.2 essenziell.

2.2 Datenschutz-Grundverordnung (DSGVO)

Die EU-Datenschutz-Grundverordnung (kurz DSGVO) wurde durch das Europäische Parlament und durch den Europäischen Rat am 27. April 2016 verabschiedet. Diese Grundverordnung führte zur Aufhebung der Richtlinie 95/46/EG, die bisher für den Schutz personenbezogener Daten natürlicher

Personen verantwortlich war. [Ra16, S. 257] Nach einer zweijährigen Übergangsfrist wurde die EU-Datenschutz-Grundverordnung am 25. Mai 2018 in allen Mitgliedsstaaten der Europäischen Union verpflichtend geltend gemacht. Ein Kernziel dieser Grundverordnung ist es, ein einheitliches Datenschutzniveau in den EU-Mitgliedsstaaten zu etablieren. Weitere „Kernziele der DSGVO" werden im Kapitelabschnitt 2.2.3 dieser Arbeit beschrieben. Der gesetzlich vorgegebene Rahmen gibt den nationalen Gesetzgebern den Spielraum, ergänzende oder ausfüllende Regularien zu schaffen. [Wi18]

Im Rahmen der vorliegenden Masterthesis wird nun auf die Entstehungsgeschichte der Verordnung sowie auf die Aufgaben der DSGVO eingegangen. Außerdem soll die Struktur näher dargelegt und die nach der Umsetzung betroffenen Einsatzgebiete thematisiert werden. Dieser Kapitelabschnitt beschäftigt sich zudem mit der theoretischen Ausarbeitung der europäischen Datenschutz-Grundverordnung. Es wird die Definition und der geschichtliche Hintergrund der DSGVO erläutert. Des Weiteren werden die Kernziele und die Rollen der Datenschutz-Grundverordnung beschrieben. Abschließend werden die Aufgaben der Datenschutzbehörde und die Strafrahmen der Unternehmen thematisiert.

2.2.1 Begriffsdefinitionen

2.2.1.1 Personenbezogene Daten

Gemäß der EU-Datenschutz-Grundverordnung Artikel 4 Abschnitt 1 sind personenbezogene Daten jene Informationen, die Rückschlüsse auf eine natürliche Person ziehen können. Somit ermöglichen Daten wie Name, Geburtsdatum, Onlinekennung, etc. Rückschlüsse auf eine natürliche Person und können damit die eine „betroffene Person" identifizieren. Nach der Definition des Datenschutzgesetzes sind personenbezogene Daten jene Daten, „***die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person***" sind. [Ra16, S. 111]

Des Weiteren definieren die Grundsätze des Datenschutzes, dass anonyme Informationen von der Verordnung ausgenommen sind. Das bedeutet, dass Informationen, die nicht oder nicht mehr (Pseudonymisierung) auf natürliche Personen zurückzuführen sind, der Verordnung nicht unterliegen. [Ra16, S. 16]

2.2.1.2 Besonderer Kategorien personenbezogener Daten

Die besonderen Kategorien der personenbezogenen Daten werden im Artikel 9 Absatz 1 der DSGVO beschrieben. Gemäß der DSGVO zählen zu den besonderen Kategorien der personenbezogenen Daten Informationen, „***aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person***". [Ra16, S. 124]

2.2.1.3 Verarbeitung

Unter dem Begriff „Verarbeitung" versteht man jegliche automatisierte sowie nichtautomatisierte Maßnahmen zur „***Erhebung, Erfassung, Organisation, Ordnung, Speicherung, Anpassung oder Veränderung***" von personenbezogenen Daten natürlicher Personen. Die Verarbeitung wird im Artikel 4 Absatz 2 der DSGVO definiert. [Ra16, S. 111]

2.2.1.4 Verantwortlicher und Auftragsverarbeiter

Die Begriffe „Verantwortlicher" und „Auftragsverarbeiter" werden im Artikel 4 Abschnitt 7 und 8 der DSGVO beschrieben. Der Verantwortliche ist jene natürliche oder juristische Person, die über den „***Zweck und die Mittel***" der Verarbeitung von personenbezogenen Daten natürlicher Personen entscheidet. [Ra16, S. 112]

Im Gegensatz zum Verantwortlichen ist der Auftragsverarbeiter jene natürliche oder juristische Person, die im Auftrag des Verantwortlichen die personenbezogenen Daten natürlicher Personen verarbeitet. [Ra16, S. 112]

2.2.1.5 Empfänger

Der Begriff „Empfänger" wird im Artikel 4 Absatz 9 der DSGVO definiert und beschreibt eine natürliche oder juristische Person, deren personenbezogene Daten offengelegt werden. Nach dieser Definition wird auch der Auftragsverarbeiter als Empfänger bezeichnet. [Ra16, S. 112]

2.2.1.6 Pseudonymisierung

Durch das Pseudonymisieren von personenbezogenen Daten natürlicher Personen kann der Personenbezug dieser Daten aufgelöst werden. Das bedeutet, dass ohne das Hinzufügen zusätzlicher Informationen kein Personenbezug hergestellt werden kann. Das wiederum senkt die Risiken der Betroffenen und unterstützt den Verantwortlichen und den Auftragsverarbeiter bei der Einhaltung der DSGVO. Die Pseudonymisierung der Daten erfolgt durch die technischen und organisatorischen Maßnahmen. Diese werden im Kapitelabschnitt 2.2.7 im Detail erläutert. Die Pseudonymisierung wird im Artikel 4 Absatz 5 der DSGVO definiert. [Ra16, S. 112]

2.2.2 Geschichtlicher Hintergrund der DSGVO

Vor der Verabschiedung der „Datenschutz-Grundsatzverordnung" galt in Bezug auf Datenschutz die Richtlinie 95/46/EG. Dabei wichen die Datenschutzvorschriften der einzelnen EU-Mitgliedsstaaten stark voneinander ab. Eine Vereinheitlichung des Datenschutzes innerhalb der EU sollte dazu beigetragen den freien Datenverkehr zwischen den Mitgliedsstaaten zu ermöglichen. [Mo06, S. 3ff.]

Aufgrund dieser Diversität kam es zu langwierigen Verhandlungsprozessen, welche erst nach vier Jahren endgültig abgeschlossen werden konnten. Der Grund für diese lange Dauer lag dabei vor allem in einer Vielzahl an Änderungsvorschlägen des zugrunde liegenden Gesetzestextes. Somit konnte die Verordnung 2016/679 „***zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG***", die am 26. April 2016 vom europäischen Gesetzgeber verabschiedet wurde, erst mit 25. Mai 2018 verpflichtend geltend gemacht werden. [Ra16, S. 1]

Wie bereits erwähnt, ist die Datenschutz-Grundverordnung „***in allen ihren Teilen verbindlich und gilt ohne mitgliedstaatlichen Umsetzungsakt unmittelbar***". [VB18, S. 3] Hierbei ist es den Mitgliedsstaaten jedoch möglich, mit Hilfe diverser Öffnungsklauseln diese um national geltende und zusätzliche Regelungen zu ergänzen. [VB18, S. 3f.] In Österreich wurde das Bundesgesetz, welches das Datenschutzgesetz 2000 aufgehoben hat, am 31. Juli 2017 veröffentlicht. [Wi18]

2.2.3 Kernziele der DSGVO

Die europäische Datenschutz-Grundverordnung verfolgt als Hauptziel, das Recht des Einzelnen in Bezug auf personenbezogene Daten zu stärken. Neben diesem Hauptziel werden auch die Ziele der Standardisierung und des freien Verkehrs von personenbezogenen Daten verfolgt. Diese drei Kernziele der DSGVO werden in diesem Kapitellabschnitt behandelt und erläutert.

Ziel 1: Datenschutzrecht natürlicher Personen stärken

Der Schutz personenbezogener Daten stellt für die Bürger ein Grundrecht dar. Aus diesem Grund besteht für die öffentliche Verwaltung die Notwendigkeit, dieses Gemeinwohl der Bürger zu schützen und zu stärken. Der Schutz von Grundrechten und der Grundfreiheit aller natürlichen Personen, ist eines der Kernziele der Datenschutz-Grundverordnung. Insbesondere der Schutz

personenbezogener Daten natürlicher Personen soll gestärkt werden. Im Artikel 1 Abschnitt 2 der Datenschutz-Grundverordnung wird dieses Ziel definiert. [Ra16, S. 2]

Ziel 2: Datenschutz-Standards etablieren

Das zweite Ziel ist ein übergreifender Datenschutz-Standard innerhalb der Europäischen Union. Unternehmen sowie Einzelpersonen können sich an diesen Standards orientieren, egal in welchem Mitgliedsland sich das Unternehmen oder die Einzelperson befindet. Des Weiteren ist die Standardisierung notwendig, um die Behörden bei der Überprüfung der Gesetze zu unterstützen. Somit ist ein weiteres Ziel der europäischen Datenschutz-Grundverordnung die Etablierung von Datenschutz-Standards innerhalb der europäischen Gemeinschaft. [Ra16, S. 6]

Ziel 3: Freien Verkehr personenbezogener Daten

Das dritte Kernziel der Datenschutz-Grundverordnung ist der freie Verkehr von personenbezogenen Daten von natürlichen Personen zwischen den EU-Mitgliedsstaaten. Durch die Harmonisierung und Standardisierung des Datenschutzes auf EU-Ebene kann ein freier Verkehr der personenbezogenen Daten ermöglicht werden. Des Weiteren verhindert dieses Ziel eine Diskriminierung von Mitgliedsländern bei der Standortwahl von Unternehmen. Vor dem Inkrafttreten der DSGVO konnte ein EU-Mitgliedsland den Wettbewerb um Unternehmensniederlassungen gegenüber weiteren Mitgliedsländern durch ein niedrigeres Datenschutzniveau für sich entscheiden. Der freie Verkehr personenbezogener Daten ist im Artikel 1 Abschnitt 3 der DSGVO verankert. [Ra16, S. 5]

Der nächste Kapitelabschnitt erläutert die verschiedenen Anwendungsbereiche der Datenschutz-Grundverordnung.

2.2.4 Anwendungsbereiche der DSGVO

Die Anwendungsbereiche der EU-Datenschutz-Grundverordnung werden in sachliche und räumliche Anwendungsbereiche aufgeteilt. Beide Anwendungsbereiche werden in den folgenden Kapitelabschnitten genauer erläutert.

2.2.4.1 Sachlicher Anwendungsbereich

Im Artikel 2 der Datenschutz-Grundverordnung wird der sachliche Anwendungsbereich geregelt. Dieser Artikel besagt, dass personenbezogene Daten natürlicher Personen, die in einem System vollautomatisiert, teilweise automatisiert oder nichtautomatisiert verarbeitet werden, von der Grundverordnung betroffen sind. Das bedeutet wiederum, dass das Gesetz sehr wenige Ausnahmen in Bezug auf die Verarbeitung von personenbezogenen Daten macht. Dies soll den Schutz der personenbezogenen Daten natürlicher Personen stärken. Ausgenommen sind lediglich Daten juristischer Personen, und Daten, die die nationale Sicherheit beziehungsweise die Außen- und Sicherheitspolitik der Nation oder der Europäischen Union betreffen. [VB18, S. 11]

2.2.4.2 Räumlicher Anwendungsbereich

Der Artikel 3 der Datenschutz-Grundverordnung regelt die räumlichen Anwendungsbereiche der Verordnung. Die Verordnung regelt die Verarbeitung von personenbezogenen Daten, die innerhalb einer in der EU ansässigen Niederlassung verarbeitet werden. Dies ist unabhängig davon, ob es sich dabei um den Verantwortlichen oder den Auftragsverarbeiter handelt. Ein weiterer Anwendungsbereich kommt zum Tragen, wenn personenbezogene Daten natürlicher Personen, die sich in der EU befinden, von nicht EU-Unternehmen verarbeitet werden. Dabei ist es irrelevant, ob diese Person ein Bürger eines europäischen Mitgliedsstaates ist oder nicht. Des Weiteren ist es unabhängig, ob

es sich bei dem Unternehmen um den Verantwortlichen oder den Auftragsverarbeiter handelt. [VB18, S. 25]

Nachdem in den vorherigen Abschnitten die Kernziele und die Anwendungsbereiche der Datenschutz-Grundverordnung erläutert wurden, werden im nachfolgenden Kapitelabschnitt die Grundsätze beziehungsweise die Fundamente der europäischen Datenschutz-Grundverordnung im Detail erläutert.

2.2.5 Fundament der EU-Datenschutz-Grundverordnung

Wenn der sachliche und der räumliche Anwendungsbereich, wie im Kapitelabschnitt 2.2.4 beschrieben, geprüft wurde, dann müssen die Grundsätze der Datenschutz-Grundverordnung bei Verarbeitung von personenbezogenen Daten, nach Artikel 5 der DSGVO geprüft werden. Die Abbildung 6 stellt die Grundsätze der Datenschutz-Grundverordnung grafisch dar. Nachfolgend werden die Grundsätze der DSGVO, die bei der Verarbeitung von personenbezogenen Daten natürlicher Personen zwingend eingehalten werden müssen, erläutert. [Ra16, S. 17f.]

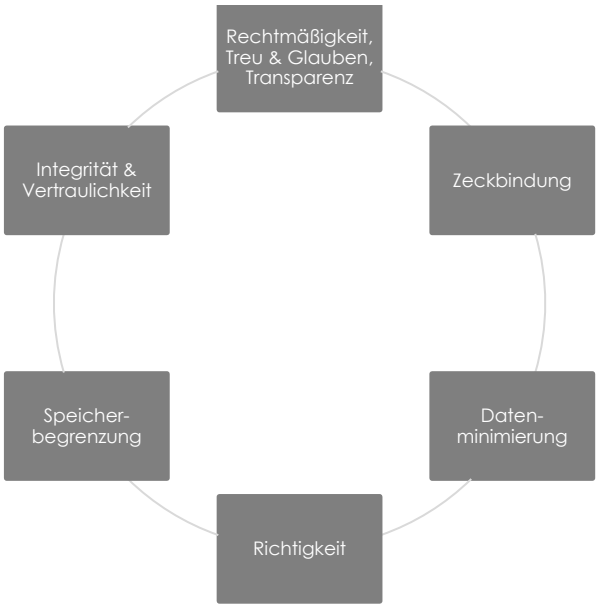


Abbildung 6 - Grundsätze der DSGVO [Ra16, S. 17f.]

2.2.5.1 Rechtmäßigkeit, Treu und Glauben, Transparenz

Durch die Datenschutz-Grundverordnung wird der Schutz von personenbezogenen Daten von natürlichen Personen nicht neu erfunden. Die Verordnung soll den Schutz innerhalb der EU vereinheitlichen und stärken. Somit ist eine rechtmäßige Verarbeitung von personenbezogenen Daten durch ein Unternehmen weiterhin eine Rechtsgrundlage. Im Artikel 6 der DSGVO wird definiert, wann eine Rechtmäßigkeit der Verarbeitung gegeben ist. Folgende Rechtsgrundlagen müssen gegeben sein damit eine Verarbeitung rechtmäßig ist: Die **„*Einwilligung der betroffenen Person*“**, die „***Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist***“, die **„Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt“** oder die „***Erforderlichkeit zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt***“. [VB18, S. 114]

Des Weiteren müssen personenbezogene Daten neben der Rechtmäßigkeit nach Treu und Glauben verarbeitet werden. Der Grundsatz „***Treu und Glauben***“ setzt ein ehrliches und redliches Verhalten des Auftragsverarbeiters voraus. Im Artikel 1 Abschnitt 5 der DSGVO wird dieser Grundsatz im Detail erläutert. Neben der „**Rechtmäßigkeit**“ und dem Grundsatz „***Treu und Glauben***“ ist die „**Transparenz**“ ein weiterer wichtiger Grundsatz für die Verarbeitung personenbezogener Daten. [VB18, S. 114]

Personenbezogene Daten müssen sowohl rechtmäßig als auch nach dem Grundsatz von Treu und Glauben verarbeitet werden. Außerdem muss die Verarbeitung der personenbezogenen Daten für die betroffene Person

nachvollziehbar sein. Den betroffenen natürlichen Personen muss nachvollziehbar sein, welche ihrer personenbezogenen Daten gesammelt, gespeichert, ausgewertet oder weiterverarbeitet werden. Des Weiteren muss dargestellt sein, in welchem Ausmaß die Daten aktuell genutzt werden und zukünftig genutzt werden sollen. Durch den Grundsatz der Transparenz hat die betroffene Person das Recht: [VB18, S. 114]

- auf Information zu der „Identität des Verantwortlichen“ (Datenverarbeiter)
- auf Information zum „Zweck“ der Datenverarbeitung
- auf Information über die „betreffenden personenbezogenen Daten“ die verarbeitet werden
- auf die „Berichtigung und Löschung“ der personenbezogenen Daten
- auf dass die „Verarbeitung eingeschränkt“ wird und dass die Daten an die betroffene Person „ausgehändigt“ werden

Der Begriff der „Transparenz“ wird im Artikel 12 der DSGVO näher erläutert.

2.2.5.2 Zweckbindung

Die Zweckbindung ist ein weiterer Grundsatz der Datenschutz-Grundverordnung und besagt, dass ohne einen vorliegenden Zweck keine Datenverarbeitung stattfinden darf. Diese Zwecke, um personenbezogene Daten zu verarbeiten, müssen präzise und eindeutig formuliert sein, sie müssen aber vor allem legitim sein. Wenn es vor Inkrafttreten der Datenschutz-Grundverordnung schon eine Verarbeitung mit einem definierten Zweck gegeben hat, dann darf die Weiterverarbeitung dieser Daten nur erfolgen, wenn der neue Zweck mit dem ursprünglichen Zweck übereinstimmt beziehungsweise vereinbar ist. Die Zweckbindung wird im Artikel 5 Abschnitt 1 der DSGVO definiert. [Ra16, S. 117]

2.2.5.3 Datenminimierung

Die Minimierung der Daten besagt, dass die zu verarbeitenden personenbezogenen Daten für ihren Zweck im „angemessen und erheblichen" Maß beschränkt werden müssen. Diesbezüglich ist es notwendig, vor der Verarbeitung der personenbezogenen Daten die Prüfung der Verhältnismäßigkeit vorzunehmen. Zusammenfassend zielt der Grundsatz der Datenminimierung auf die zweckgemäße Minimierung der zu verarbeitenden Daten ab. [Ra16, S. 117]

2.2.5.4 Richtigkeit

Die verarbeitenden personenbezogenen Daten müssen nach dem Grundsatz der Richtigkeit „sachlich korrekt" und „auf dem neuesten Stand" sein. Gemäß Artikel 5 Abschnitt 1 der DSGVO müssen Daten, die hinsichtlich ihres Verarbeitungszwecks unrichtig sind, sofort berichtigt oder gelöscht werden. Für die Richtigkeit der Daten ist der Auftragsverarbeiter verantwortlich und muss gegebenenfalls die notwendigen Maßnahmen treffen. [Ra16, S. 117]

2.2.5.5 Speicherbegrenzung

Der Grundsatz der Speicherbegrenzung besagt, dass die personenbezogenen Daten nur so lange gespeichert und verarbeitet werden dürfen, solange der Zweck der Verarbeitung aufrecht oder die Verarbeitung notwendig ist. Wenn das nicht der Fall ist, dann ist der Verantwortliche verpflichtet, die Daten unverzüglich zu löschen. Wenn die Daten aus statistischen Gründen weiter gespeichert werden müssen, dann ist es notwendig, den Personenbezug der Daten aufzuheben. [Ra16, S. 118]

2.2.5.6 Integrität und Vertraulichkeit

Durch den Grundsatz der Integrität und Vertraulichkeit soll der angemessene Schutz der personenbezogenen Daten durch technische und organisatorische

Maßnahmen (kurz TOMs) sichergestellt werden. Die personenbezogenen Daten müssen vor unbefugtem Zugriff beziehungsweise unbefugter Verarbeitung, vor unbeabsichtigtem Verlust, Zerstörung oder Beschädigungen geschützt werden. Des Weiteren besagt der Grundsatz, dass die Daten gegen unbefugte Weitergabe oder Offenlegung durch unbefugte Dritte geschützt werden müssen. Mögliche technische und organisatorische Maßnahmen werden im Kapitelabschnitt 2.2.7 erläutert. Der Grundsatz der Integrität und Vertraulichkeit wurde im Artikel 5 Absatz 1 der DSGVO festgehalten. [Ra16, S. 118]

2.2.5.7 Rechenschaftspflicht

Durch die Rechenschaftspflicht sind die Verantwortlichen verpflichtet, die vorab erläuterten Grundsätze einzuhalten und diese Einhaltung nachzuweisen. Diese Rechenschaftspflicht hat das Ziel, dass die Datenschutzbehörde zu jeder Zeit die Einhaltung der Verarbeitungsgrundsätze prüfen kann. Des Weiteren bewirkt dieser Grundsatz das Führen einer vollständigen Dokumentation durch den Verantwortlichen. [VB18, S. 313]

Dieses Ziel kann durch interne Compliance-Maßnahmen wie, die vollständige Dokumentation aller Verarbeitungstätigkeiten und den dazugehörigen Verarbeitungszweck in einem Datenschutz-Managementsystems sowie durch die Sicherstellung der Verarbeitung von personenbezogenen Daten durch interne Richtlinien, erzielt werden.

Nachdem in diesem Kapitelabschnitt die Grundsätze der Datenschutz-Grundverordnung erläutert wurden, werden im nächsten Kapitelabschnitt die Rechte und Pflichten der Betroffenen beschrieben.

2.2.6 Rechte und Pflichten

Mit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung am 25. Mai 2018 wurden die Rechte der Betroffenen gestärkt und den Verantwortlichen

beziehungsweise den Unternehmen einige Pflichten in Bezug auf den Datenschutz auferlegt. Dieser Kapitelabschnitt beschreibt die Rechte der Betroffene und die Pflichten der Verantwortlichen beziehungsweise Unternehmen gemäß der Datenschutz-Grundverordnung im Detail.

2.2.6.1 Informationspflicht

Durch das Recht der Informationspflicht soll der Grundsatz der fairen und transparenten Verarbeitung personenbezogener Daten natürlicher Personen sichergestellt werden. Nach Erhebung der personenbezogenen Daten ist der Verantwortliche verpflichtet, diese Informationen in „***präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zu übermitteln und zur Verfügung zu stellen***". Die Informationspflicht wird im Artikel 12 der DSGVO geregelt. [Ra16, S. 129]

2.2.6.2 Auskunftsrecht

Das Auskunftsrecht wird im Artikel 5 der DSGVO geregelt. Dieses Recht bewirkt, dass der Betroffene ein Recht auf Auskunft über seine erhobenen personenbezogenen Daten hat und darüber, zu welchem Zweck diese Daten verarbeitet werden. Der Verantwortliche hat die Pflicht, das Auskunftsbegehren zu erwidern und diese Informationen an den Betroffenen zu übermitteln. Der Verantwortliche hat das Recht die Identität, des Betroffenen einzufordern. Der Identitätsnachweis kann auf verschiedenen Wegen erfolgen, jedoch basiert der Identitätsnachweis auf dem Grundsatz der „möglichst einfachen Handhabe". Damit soll sichergestellt werden, dass der Betroffene auf dem unkompliziertesten Weg zu seinen Rechten kommt. Die Auskunft über die Daten des Betroffenen muss innerhalb eines Monats an den Betroffenen übermittelt werden. Der Verantwortliche hat die Möglichkeit, je nach Komplexität oder Anzahl der Datensätze die Frist auf zwei Monate auszuweiten. [Ra16, S. 138]

Der Betroffene hat das Recht auf folgende Daten: [Ra16, S. 138]

- Verarbeitende personenbezogene Daten
- Datenkategorie
- Verarbeitungszweck
- Datenherkunft
- Speicherfrist der Daten

2.2.6.3 Richtigstellung

Durch die Richtigstellung der personenbezogenen Daten hat der Betroffene das Recht, unrichtige Daten berichtigen beziehungsweise ergänzen zu lassen. Der Verantwortliche hat die Pflicht, die unrichtigen Daten innerhalb eines Monats zu berichtigen beziehungsweise zu ergänzen. [Ra16, S. 140]

2.2.6.4 Löschung

Der Betroffene hat das Recht der Löschung. Das bedeutet im Detail, dass der Verantwortliche verpflichtet ist, die Daten des Betroffenen zu löschen. Das Löschbegehren muss vom Verantwortlichen innerhalb eines Monats erfüllt werden. [Ra16, S. 140]

2.2.6.5 Datenübertragbarkeit

Das Recht der Datenübertragbarkeit dient nicht dem Aspekt des Datenschutzes. Durch die Datenübertragbarkeit soll der Betroffenen einen leichteren Zugang zu seinen Daten erhalten. Das Unternehmen muss dafür sorgen, dass der Betroffene seine Daten in einem „***strukturierten, gängigen und maschinenlesbaren Format***“ erhält. Dies soll den Wechsel zwischen Online-Diensten erleichtern. [Ra16, S. 144]

2.2.6.6 Widerspruchsrecht

Das Widerspruchsrecht ist vom bereits beschriebenen Widerrufsrecht zu unterscheiden. Im Gegensatz zum Widerrufsrecht richtet sich das

Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten natürlicher Personen. Das Widerrufsrecht widerruft die freiwillige Einwilligung der Datenverarbeitung, das Widerspruchsrecht wiederspricht der Verarbeitung personenbezogener Daten. [Ra16, S. 145]

Die technische und organisatorische Umsetzung der Betroffenenrechte wird im nächsten Kapitelabschnitt 2.2.7 erläutert.

2.2.7 Technische und organisatorische Maßnahmen (TOMs)

Um den Schutz der personenbezogenen Daten sicherzustellen, ist der Verantwortliche verpflichtet, technische und organisatorische Maßnahmen zu implementieren. Die Datenschutz-Grundverordnung definiert diese Maßnahmen im Artikel 24 Abschnitt 1, im Artikel 25 und im Artikel 32 Abschnitt 1. Ziel dieser Maßnahmen ist der Schutz der personenbezogenen Daten natürlicher Personen in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit.

Der Artikel 32 der DSGVO beschreibt technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten folgend: „***Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: [Ra16, S. 160f.]***

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) ***die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;***
d) ***ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung." [Ra16, S. 160f.]***

Organisatorische Maßnahmen werden in Datenschutzstrategien definiert. Diese Strategien verfolgen Ziele wie die Definition von Rollen und Verantwortlichkeiten, die Kategorisierung von Daten, die Regelung der Speicherdauer der Daten sowie die Vorgehensweise bei Sicherheitsverletzungen. Neben den organisatorischen Maßnahmen verfolgen auch die technischen Maßnahmen das Ziel der Datensicherheit. Diese Maßnahmen zielen vordergründig darauf, die Risiken zu minimieren. [VB18, S. 46ff.]

Durch die Datenschutz-Grundverordnung werden die Verantwortlichen verpflichtet, folgende Maßnahmen umzusetzen: „Privacy by Design" (Datenschutz durch Technik) und „Privacy by Default" (Datenschutz durch Voreinstellung). Das Ziel von „Privacy by Design" ist es, den Schutz der Privatsphäre der Betroffenen bereits bei der Entwicklung der Systeme oder Prozesse sicherzustellen. Schon bei der Entwicklung muss das Grundrecht auf Datenschutz berücksichtigt werden. Der Grundsatz „Privacy by Default" verfolgt den Schutz der Privatsphäre über datenschutzfreundliche Grundeinstellungen. Diese Grundeinstellungen können jedoch jederzeit von den Betroffenen verändert werden. [VB18, S. 81f.]

Die Europäische Agentur für Netz- und Informationssicherheit (kurz ENISA) definiert vier datenorientierte und vier prozessorientierte Maßnahmen, um die Grundsätze „Privacy by Default" und „Privacy by Design" zu verfolgen beziehungsweise umzusetzen.

Datenorientierte Maßnahmen laut ENISA: [Ho12, S. 5]

- Minimieren (minimse)
  Die zu verarbeitende Menge an Daten muss reduziert werden und somit so gering wie möglich sein.
- Verbergen (hide)
  Daten mit personenbezogenem Bezug müssen verborgen gehalten werden.
- Getrennt (serperate)
  Daten mit personenbezogenem Bezug müssen getrennt verarbeitet und gespeichert werden.
- Gesamtheit (aggregate)
  Personenbezogene Daten, die in einer Beziehung stehen sollen zusammenfasst und verarbeitet werden.

Prozessorientierte Maßnahmen laut ENISA: [Ho12, S. 6]

- Informieren (inform)
  Die betroffenen Personen müssen über die Verarbeitung ihrer personenbezogenen Daten informiert werden.
- Steuern (control)
  Die betroffenen Personen müssen bei der Verarbeitung ihrer personenbezogenen Daten die Kontrolle behalten.
- Erzwingen (enforce)
  Die rechtlichen Anforderungen der Datenschutz-Grundverordnung müssen durchgesetzt werden.
- Beweisen (demonstrate)
  Die Einhaltung der Datenschutz-Grundverordnung muss durch den Verantwortlichen nachgewiesen werden.

Konkretere Maßnahmen werden im Österreichischen Datenschutz-Anpassungsgesetz 2018 §54 Datensicherheitsmaßnahmen beschrieben. In

diesem Anpassungsgesetz wird das Schutzniveau, dass für die Verarbeitung von personenbezogenen Daten notwendig ist, beschrieben. Folgende Maßnahmen werden im §54 des Datenschutz-Anpassungsgesetzes beschrieben:

2.2.7.1 Zugangskontrolle

Es muss sichergestellt werden, dass nur berechtigte Personen über einen Zugang zu Verarbeitungsanlagen (Server, Client, Drucker, etc.) verfügen. Unbefugten muss der Zugang verwehrt werden. Bei der Zugangskontrolle handelt es sich um eine physische Maßnahme. [Sc18, S. 2]

Maßnahmen:

Versperren der Zugänge zu Verarbeitungsanlagen und Akten, Protokollieren der Zugänge zu Verarbeitungsanalagen und Akten, Unternehmensgeräte wie Notebooks, Smartphones, Datenträger, etc. versperrt aufbewahren. [Sc18, S. 2]

2.2.7.2 Datenträgerkontrolle

Das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern durch Unbefugte muss verhindert werden. [Sc18, S. 3]

Maßnahmen:

Personenbezogene Daten dürfen nur auf speziellen Laufwerken gespeichert werden. Bei der Entsorgung von Datenträgern muss sichergestellt werden, dass alle personenbezogenen Daten gelöscht wurden. [Sc18, S. 3]

2.2.7.3 Speicherkontrolle

Durch die Speicherkontrolle wird die Eingabe, die Veränderung und die Löschung personenbezogener Daten durch Unbefugte verhindert. [Sc18, S. 3f.]

Maßnahmen:

Personenbezogene Daten sind nur mittels berechtigter Benutzer zugänglich. Die Zugriffe werden protokolliert. Des Weiteren müssen die Daten verschlüsselt abgelegt werden. [Sc18, S. 3f.]

2.2.7.4 Benutzerkontrolle

Die Benutzerkontrolle verhindert die Nutzung von Systemen durch Unbefugte. Der IT-Administrator vergibt Rechte nach dem Grundsatz der „Need-to-Know"-Prinzipien. Das bedeutet, es dürfen nur Berechtigte auf die Daten zugreifen. [Sc18, S. 4f.]

Maßnahmen:

Berechtigungen werden nach dem „Need-to-Know"-Prinzip vergeben. Firewalls sichern den Zugriff der Daten von außen ab. Des Weiteren kann der Schutz durch Passwort-Policy und die Protokollierung des Zugriffs erhöht werden. [Sc18, S. 4f.]

2.2.7.5 Zugriffskontrolle

Durch die Zugriffskontrolle wird gewährleistet, dass die berechtigten Benutzer ausschließlich auf die personenbezogenen Daten Zugriff haben, für die sie auch berechtigt sind. [Sc18, S. 5f.]

Maßnahmen:

Durch eine definierte Passwort-Policy wird der Zugriff auf personenbezogene Daten gesichert. Die Passwort-Policy definiert die Komplexität und den Life-Cycle des Passworts. Unternehmenskennwörter dürfen nicht im privaten Bereich verwendet werden. [Sc18, S. 5f.]

2.2.7.6 Übertragungskontrolle

Es soll gewährleistet werden, dass die Übermittlung der personenbezogenen Daten nur an berechtigte Empfänger möglich ist. [Sc18, S. 6]

Maßnahmen:

Vier-Augen-Prinzip bei der Übermittlung von personenbezogenen Daten, E-Mails werden durch Kennwörter geschützt. Das Kennwort ist nur dem berechtigten Empfänger bekannt. [Sc18, S. 6]

2.2.7.7 Eingabekontrolle

Durch die Eingabekontrolle soll die Nachvollziehbarkeit der Eingaben sichergestellt werden. Das bedeutet, es muss sichergestellt werden, welcher Benutzer zu welcher Zeit auf welche Daten zugegriffen hat. [Sc18, S. 6f.]

Maßnahmen:

Protokollieren der Zugriffe auf personenbezogene Daten und Identifizierung der Benutzer. [Sc18, S. 6f.]

2.2.7.8 Transportkontrolle

Die Transportkontrolle stellt sicher, dass die Daten bei der Übermittlung nicht von Unbefugten gelesen, verändert, kopiert oder gelöscht werden können. [Sc18, S. 7f.]

Maßnahmen:

Verschlüsseln der Datenträger, Zugriffe auf Unternehmenssysteme nur über VPN und sicheres Löschen von Datenträgern sind technische Maßnahmen. Durch vertragliche Regelungen mit Transport- und Lieferunternehmen können organisatorische Maßnahmen definiert werden. [Sc18, S. 7f.]

2.2.7.9 Wiederherstellung

Durch die Wiederherstellung soll sichergestellt werden, dass die Systeme nach einem Störfall zu einer definierten Zeit wiederhergestellt werden können. [Sc18, S. 8]

Maßnahmen:

Durchführen von regelmäßigen Sicherungen und Backups. Wiederherstellungsszenarien müssen in regelmäßigen Abständen getestet werden. [Sc18, S. 8]

2.2.7.10 Zuverlässigkeit und Datenintegrität

Die Zuverlässigkeit von Systemen gewährleistet, dass alle Funktionen jederzeit zur Verfügung stehen und Fehlfunktionen sofort gemeldet werden. Durch die Datenintegrität wird sichergestellt, dass die Daten bei einer Fehlfunktion des Systems nicht beschädigt werden. [Sc18, S. 9]

Maßnahmen:

Schutz vor Viren, Malware, Ransomware und auch vor Stromausfällen. Sicherstellen der Systemüberwachung von Systemen und Services und von regelmäßigen Systemupdates. [Sc18, S. 9]

In diesem Kapitelabschnitt wurden die technischen und organisatorischen Maßnahmen gemäß der Datenschutz-Grundverordnung beschrieben. Diese Maßnahmen verfolgen den Schutz personenbezogener Daten von natürlichen Personen hinsichtlich der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit. Die Einhaltung dieser Maßnahmen wird von der Datenschutzbehörde überprüft. Die Aufgaben und Pflichten der Behörde sowie die Strafen bei einer Nichteinhaltung der beschriebenen Maßnahmen werden im nachfolgenden Kapitelabschnitt 2.2.8 beschrieben.

2.2.8 Die Datenschutzbehörde

Um die Pflichten der Verantwortlichen zu auditieren und die Rechte der Betroffenen zu wahren wurde die Datenschutzbehörde ins Leben gerufen. Oberstes Ziel der Datenschutzbehörde ist „die Einhaltung des Datenschutzes in Österreich“. [Ös19]

Die Aufgaben und Ziele der Datenschutzbehörde werden im Artikel 57 der DSGVO beschrieben. Dort werden folgende zentrale Aufgaben der Behörde festgelegt: [Ra16, S. 205ff.]

- Die Behörde hat die Aufgabe, die gesetzliche Erfüllung der Datenschutz-Grundverordnung zu überwachen und gegebenenfalls durchzusetzen.
- Durch die Öffentlichkeitsarbeit der Behörde soll die Öffentlichkeit beim Thema Datenschutz sensibilisiert werden. Die Rechte der Betroffenen und Pflichten der Verantwortlichen stehen dabei im Fokus der Öffentlichkeitsarbeit.
- Eine weitere Aufgabe der Behörde ist die Beratung nationaler Gremien und Behörden in Bezug auf den Schutz von personenbezogenen Daten natürlicher Personen.
- Betroffene können sich bei Fragen und Beschwerden an die Datenschutzbehörde wenden. Die Behörde ist verpflichtet jeder Datenschutzbeschwerde nachzugehen. Beschwerden können sich auf das Nichteinhalten des Auskunftsbegehren oder auf Verstöße gegen die Richtigstellung, Löschung und Geheimhaltung stützen.
- Technologische Entwicklungen im IKT-Bereich, soweit diese Auswirkungen auf die Verarbeitung beziehungsweise den Schutz personenbezogener Daten natürlicher Personen haben, müssen von der Behörde verfolgt und stetig weiterentwickelt werden.

- Gemäß Artikel 42 der DSGVO ist die Behörde für die Einführung und für die regelmäßige Überprüfung neuer Datenschutzzertifizierungen beziehungsweise Mechanismen zuständig.

Um den Aufgaben nachzukommen, wurde die Datenschutzbehörde mit umfangreichen Befugnissen ausgestattet. Durch diese Befugnisse ist die Datenschutzbehörde berechtigt, Datenschutzprüfungen und Zertifizierungsverfahren durchzuführen. Eine Prüfung muss bei einer eingehenden Beschwerde eines Betroffenen durchgeführt werden, kann aber auch ohne eine Beschwerde erfolgen. Bei Rechtswidrigkeiten kann die Datenschutzbehörde Verwarnungen oder Verwaltungsstrafen aussprechen. Der Strafrahmen wird im nächsten Kapitelabschnitt 2.2.9 genauer erläutert.

2.2.9 Strafrahmen

Die Nichteinhaltung der Pflichten in Bezug auf die Verarbeitung personenbezogener Daten natürlicher Personen führt zu erheblichen Strafen bei den Verantwortlichen. Gemäß Artikel 83 der DSGVO sollen die Strafen in jedem Einzelfall verhältnismäßig, wirksam und vor allem abschreckend sein. Des Weiteren wird im Artikel 83 der DSGVO das Ausmaß der Strafen definiert. [Ra16, S. 244ff.] Demnach drohen den verantwortlichen Unternehmen bei Verstößen Strafen bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten Jahresumsatzes. Diese Strafen können je nach Größe des Unternehmens, nach dem Grad der Verantwortung des Verantwortlichen sowie unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen (TOMs) abgeschwächt werden. Wenn man den Strafrahmen der Datenschutz-Grundverordnung mit dem Datenschutzgesetz 2000 vergleicht, dann fällt der Strafrahmen des Datenschutzgesetzes 2000 mit maximalen Strafen bis zu 25.000 Euro gering aus. Die Datenschutzbehörde kann neben dem beschrieben Geld- und Strafrahmen auf weitere Rechtsbehelfe zurückgreifen. So

kann die Behörde bei Verstößen auch Schadensersatz für materielle und immaterielle Schäden einfordern. [Wi18]

2.2.10 Zusammenfassung

Die europäische Datenschutz-Grundverordnung ist durch ihre umfangreichen Pflichten eine große Herausforderung für die Verantwortlichen beziehungsweise für die Unternehmen. Die Herausforderungen beziehen sich auf das Ergänzen und Erweitern der Auskunfts-, Dokumentations-, Mitteilungs-, Lösch- und Meldepflicht. Des Weiteren kann die Behörde, bei Nichteinhaltung der beschriebenen Pflichten mit hohen Strafen sanktionieren. Diese Sanktionen sind ein weiterer Druck, der auf den Verantwortlichen lastet. Den Betroffenen wurden mit der neuen Datenschutz-Grundverordnung mehr Rechte bei ihren personenbezogenen Daten zugesprochen. Die DSGVO verfolgt das Ziel der Harmonisierung des Datenschutzrechts in Europa und stärkt dabei die Transparenz bei der Speicherung und Verarbeitung personenbezogener Daten. Des Weiteren wurde den Betroffenen über die Datenschutzbehörde ein Verwaltungsorgan mit umfangreichen Befugnissen zur Verfügung gestellt. Auskünfte oder Beschwerden können Betroffene direkt an die Datenschutzbehörde weiterleiten.

Der nachfolgende Kapitelabschnitt 2.3 beschreibt und definiert kleine und mittelständische Unternehmen (KMUs). Diese theoretische Ausarbeitung ist für die Beantwortung der gestellten Forschungsfrage relevant.

2.3 Kleine und mittelständische Unternehmen (KMUs)

Die Masterthesis untersucht die Nutzung von Cloud-Services von KMUs vor und nach Inkrafttreten der Datenschutz-Grundverordnung. Aus diesem Grund ist es von Nöten, dass Thema KMU in dieser Arbeit zu behandeln. Im folgenden Kapitelabschnitt wird der Begriff KMU definiert und die Verteilung der KMUs in Österreich dargestellt.

2.3.1 Begriffsdefinition

Das Kürzel KMU steht für kleine und mittelständische Unternehmen. KMUs sind auf internationaler Ebene verschieden definiert. KMUs werden nach quantitativen und qualitativen Kriterien unterteilt. Diese Kriterien sind international standardisiert. Der Jahresumsatz, die Bilanzsumme, die Eigenständigkeit des Unternehmens sowie die Anzahl der Mitarbeiter zählen zu den quantitativen Auswahlkriterien. Zu den qualitativen Auswahlkriterien zählt man ökonomische, gesellschaftliche und auch psychologische Werte. In Österreich zählen jene Unternehmen zu KMUs die weniger als 250 Mitarbeiter beschäftigen und weniger als 50.000.000 € Jahresumsatz generieren oder eine Bilanzsumme von weniger als 43.000.000 € aufweisen. Die Abbildung 7 stellt die Definition der KMUs in Österreich grafisch dar. [Ko03, S. 4ff.]

Kategorie des Unternehmens	Mitarbeiteranzahl	∧	Jahresumsatz	∨	Jahresbilanz
Mittel	< 250	∧	< 50.000.000€	∨	< 43.000.000€
Klein	< 50	∧	< 10.000.000€	∨	< 10.000.000€
Kleinst	< 10	∧	< 2.000.000€	∨	< 2.000.000€

Abbildung 7 - Definition KMUs in Österreich [GB19]

2.3.2 Verteilung der KMUs in Österreich

Kleine und mittelständische Unternehmen (kurz KMUs) sind das Rückgrat der österreichischen Wirtschaft. 99,7 Prozent aller Unternehmen in Österreich sind kleine und mittelständische Unternehmen. Diese 328.900 Unternehmen beschäftigen insgesamt knapp zwei Millionen Personen und erzielen einen

Umsatz in Höhe von 455 Milliarden Euro. Nachfolgend werden diese Daten der „KMU-Forschung“ in der Tabelle 2 dargestellt. [GB19]

Bereich	KMUs (Stand 2016)	Anteil an allen Unternehmen
Unternehmenszahl	328.900	99,6 %
Beschäftigte	1.958.600	68 %
Umsatzerlös	455.000.000 €	63 %

Tabelle 2 - Statistische KMU-Daten aus Österreich (Stand 2016) [GB19]

2.3.3 Zusammenfassung

In diesem Kapitelabschnitt wurde die Definition von kleinen und mittelständischen Unternehmen erläutert. Um die nachfolgende Forschung zielgerecht auszurichten, ist es unerlässlich, KMUs von Großunternehmen abzugrenzen. Des Weiteren konnte in diesem Kapitel die Bedeutung der KMUs für die österreichische Wirtschaft dargestellt werden. 99,6 Prozent der österreichischen Unternehmen sind KMUs und lediglich 0,4 Prozent der österreichischen Unternehmen sind Großunternehmen. Hervorzuheben ist jedoch, dass 32 Prozent aller österreichischen Arbeitnehmer bei Großunternehmen angestellt sind. [GB19]

Im Kapitel 2 wurden alle notwendigen theoretischen Grundlagen erläutert, um auf die Forschungsfrage einzugehen und diese im Zuge dieser Arbeit zu beantworten. Das nachfolgende Kapitel 3 wird auf die „Cloud-Compliance“ ausgerichtet. Diese Cloud-Compliance setzt sich aus den technischen und organisatorischen Maßnahmen gemäß der Datenschutz-Grundverordnung und den notwendigen technischen und organisatorischen Maßnahmen der Cloud-Service-Provider zusammen. Alle daraus resultierenden Maßnahmen führen zu einer Compliance der Cloud-Nutzung.

3. CLOUD-COMPLIANCE

Nachdem im zweiten Kapitel die theoretischen Grundlagen ausführlich erläutert wurden, bezieht sich das dritte Kapitel auf die praktische Umsetzung von Cloud-Compliance-Maßnahmen. Cloud-Compliance beinhaltet alle internen und externen Maßnahmen für einen rechtskonformen Cloud-Service-Einsatz. Dabei versucht die IT-Governance alle Vorgaben, hinsichtlich der IT-Sicherheit und des Datenschutzes, umzusetzen. Der Begriff Cloud-Compliance wird im „Cloud-Kompass" wie folgt definiert:

„***Cloud-Compliance bezeichnet die Einhaltung von gesetzlichen, vertraglichen und sonstigen regulativen Vorgaben im Rahmen des Betriebs und der Nutzung von Cloud-Services.***" [Bu17, S. 11]

Des Weiteren wird Cloud-Compliance vom „Cloud-Kompass" in Ebenen und Säulen unterteilt. Der Cloud-Kompass ist eine unabhängige Orientierungshilfe für Unternehmen sowie für Privatpersonen, um diese bei der Herausforderung der komplexen Cloud-Service-Nutzung zu unterstützen. Der Cloud-Kompass wird von einem gemeinnützigen Verein namens „A-SIT" erstellt und veröffentlicht. Finanziert wird der Cloud-Kompass durch das Sicherheitsforschungs- und Förderprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie und dem Bundesministerium für Finanzen. Der Cloud-Kompass wird in vier Teilbereiche untergliedert. [Bu17, S. 4]

Die Abbildung 8 stellt die grundlegende Ebene „Vertragliche Rahmenbedingungen" sowie die drei Säulen „IT-Servicemanagement", „Informationssicherheit" und „Datenschutz" grafisch dar. [Bu17, S. 42]

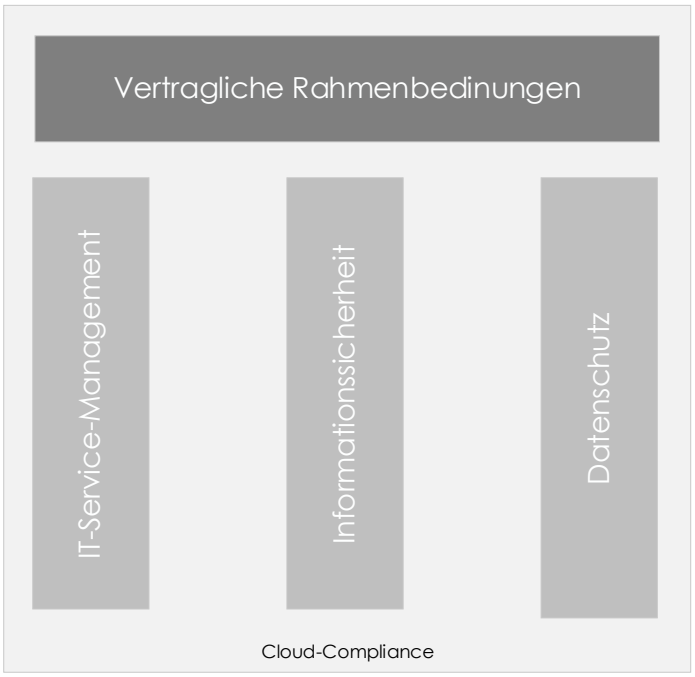


Abbildung 8 - Cloud-Compliance

Die vier Aspekte „Vertragliche Rahmenbedingungen“, „IT-Service-Management“, „Informationssicherheit“ und „Datenschutz“ werden in den folgenden Kapitelabschnitten im Detail erläutert. Des Weiteren werden zu den angegebenen Aspekten, Empfehlungen und mögliche Maßnahmen beschrieben.

3.1 Vertragliche Rahmenbedingungen

Die vertraglichen Rahmenbedingungen sind der Grundstein für die Cloud-Compliance. Diese Rahmenbedingungen sind wichtige Bestandteile des IT-Service-Management (Kapitelabschnitt 3.2), der Informationssicherheit (Kapitelabschnitt 3.3) und des Datenschutzes (Kapitelabschnitt 3.4). Die vertraglichen Rahmenbedingungen enthalten die definierten Leistungen sowie die wechselseitigen Anforderungen der Vertragspartner. Des Weiteren müssen klare vertragliche Vereinbarungen über das geltende Recht definiert werden. Dazu gehören unter andere, Konfliktlösungsmechanismen, Gerichtsstand, Nutzungsrechte sowie Schiedsgerichtsvereinbarungen. Service-Level-

Agreements (kurz SLAs) sind ein Teil der vertraglichen Rahmenbedingungen. Sie sind sehr stark mit den beschriebenen drei Säulen verbunden. In den SLAs werden die vertraglichen Leistungen sowie die Folgen bei Nichteinhaltung dieser Leistungen definiert. Des Weiteren werden in den SLAs Kennzahlen definiert, um schlussendlich die Leistungen messbar zu machen. Mit diesen definierten Kennzahlen kann das Unternehmen die bezogenen Leistungen steuern und überwachen. Ein weiterer wichtiger Aspekt bei den vertraglichen Rahmenbedingungen ergibt sich aus einem „Exit-Szenario". Vor dem Eintritt in die Cloud muss der geregelte Austritt vertraglich festgelegt werden. Diese Rahmenbedingungen sind zwingend notwendig, um einen sicheren Einstieg, Betrieb und Ausstieg zu gewährleisten. [De10, 31-32]

3.2 IT-Service-Management

Das Management von IT-Services ist heutzutage unerlässlich für ein Unternehmen. Für die Steuerung der IT-Organisation und der zugehörigen Prozesse hat sich das IT Infrastructure Library Framework (kurz ITIL) etabliert. ITIL ist eine Ansammlung von Best-Practice-Leitlinien für die Bereitstellung von IT-Services und Prozessen. Der ITIL-Service-Life-Cycle besteht aus den fünf Kernprozessen Service-Strategy, Service-Design, Service-Transition, Service-Operation und Continual-Service-Improvement und aus weiteren 21 untergliederten Prozessen. Durch den Bezug von Cloud-Services verändern sich die Prozesse des IT-Service-Managements. Die Veränderungen betreffen vor allem die ITIL-Prozesse Service-Operation, Service-Transition, Service-Design und Service-Strategy, wobei die Prozesse Service-Strategy und Service-Design für den Cloud-Nutzer mehr an Bedeutung gewinnen und die Prozesse Service-Operation und Service-Transition an Bedeutung verlieren. Die letzteren Prozesse sind für den Leistungsgeber beziehungsweise für den Cloud-Service-Provider von großer Bedeutung. Der Prozess Continual-Service-Improvement bleibt für Cloud-Nutzer unverändert wichtig. [Pr14, 1-3]

IT-Service-Management hilft, mit dem ITIL-Framework, Cloud-Services effizient zu implementieren und zu betreiben. In der nachfolgenden Tabelle 3 wird die Prozesssicht des ITIL-Service-Life-Cycle aus der Nutzer beziehungsweise Unternehmenssicht sowie aus der Cloud-Service-Provider-Sicht dargestellt. [Bü16]

Beim Einsatz von IT-Service-Management in Bezug auf Cloud-Services spricht man auch von „Cloud-Service-Management". Durch die Veränderung der IT-Services hinsichtlich der Cloud-Service-Nutzung ist es unabdingbar, die IT-Service-Management-Prozesse neu zu bewerten. Die Prioritäten werden sich auf der Nutzer-Seite sowie auf der Seite des Cloud-Service-Providers verändern. Letztendlich wird IT-Service-Management im Zusammenhang mit Cloud-Services wichtiger denn je, denn die Steuerung der Prozesse kann nur durch standardisierte und vorab definierte Regeln erfolgen. Aus diesem Grund ist es unerlässlich, auf „Best Practice" wie ITIL zurückzugreifen. Die Prozesse rücken immer weiter in den Vordergrund und machen somit eine prozessorientierte Steuerung und Kontrolle unerlässlich.

ITIL-Service-Life-Cycle	Nutzer / Unternehmen	Anbieter / Cloud-Service-Provider
Service-Strategie	Die Angebote verschiedener Cloud-Service-Anbieter werden evaluiert und ausgewertet. Des Weiteren werden die verschiedenen Services zusammengefasst.	Entwickeln von Services die auf einer On-Demand-Basis zur Verfügung gestellt werden. Hierbei ist das Bedarfsmanagement eine zentrale Komponente.
Service-Design	Fokussierung auf die Integration von IT-Services der Cloud-Service-Provider und den Aufbau von IT-Sicherheitsmaßnahmen.	Zusammenfassen von Service-Paketen für eine einfache Nutzung dieser Services. Das Kapazitätsmanagement spielt dabei eine wichtige Rolle.

Service-Transition	Steuern und kontrollieren von unterschiedlichen Cloud-Services und den CSP.	Schnelle und automatisierte Bereitstellung der Cloud-Services. Sicherstellen eines sicheren Betriebs.
Service-Operation	Messen und kontrollieren der definierten Services. Eventuelle Ausfälle des Cloud-Service koordinieren.	Bereitstellen beziehungsweise liefern der definierten Services. Verhindern von Service-Ausfälle.
Continual-Service-Improvement	Auswerten der gemessenen Kennzahlen und ableiten von KVP-Maßnahmen.	Durch bereitgestellte Kennzahlen sowie durch die Kundenzufriedenheit, die bereitgestellten Services stätig weiterentwickeln.

Tabelle 3 - ITIL-Prozesse aus der Verantwortlichen-Sicht [Bü16]

3.3 Informationssicherheit

Durch die Auslagerung von Applikationen, Plattformen und Infrastrukturen in Cloud-Umgebungen muss ein definiertes Vorgehen eingehalten werden. Dieses definierte Vorgehen wird als „Life-Cycle-Cloud-Computing“ bezeichnet. Der Life-Cycle beinhaltet die Phasen Planung, Umsetzung, Migration, Betrieb und Beendigung. In jeder dieser Phasen muss die Sicherheit der Daten gewährleistet werden. Unter Gewährleistung der Sicherheit wird die Einhaltung der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität verstanden. Das bedeutet, dass durch diese Schutzziele die Rechenzentren, die Cloud-Plattformen, die Cloud-Applikationen sowie die Zugänge und Zugriffe auf die Cloud-Services abgesichert werden müssen. Diese Sicherheit wird durch organisatorische und technische Maßnahmen gewährleistet. Ein weiterer Teil der Informationssicherheit sind die qualitativen Maßnahmen, die zur Einhaltung der Informationssicherheit beitragen. Dabei greifen die Cloud-Service-Provider auf Sicherheits- und Qualitätsstandards, wie ISO/IEC 27001 und IT-Service-Management (siehe Kapitelabschnitt 3.2), zurück. Diese Normen geben Auskunft über ein definiertes Schutzniveau der Provider. Um die Informationssicherheit näher zu erläutern, wird im Folgenden das „Life-Cycle-Cloud-Computing“ im

Detail erläutert. Die Abbildung 9 stellt die einzelnen Schritte des „Life-Cycle-Cloud-Computing“ grafisch dar, in den folgenden Kapitelabschnitten werden die einzelnen Schritte im Detail erläutert. [De10, S. 72]

Abbildung 9 - Life-Cycle-Cloud-Computing [De10, S. 73]

3.3.1 Planungsphase

In der Planungsphase werden die gewünschten Cloud-Services erarbeitet. Diese Services ergeben sich aus den Cloud-Service-Modellen (Kapitelabschnitt 2.1.3) sowie aus den Betriebsmodellen (Kapitelabschnitt 2.1.4). Dazu wird in der Planungsphase eine Sicherheitsanalyse durchgeführt. Diese Sicherheitsanalyse beinhaltet eine Struktur, Schutzbedarfs- und Risikoanalyse. Des Weiteren werden durch diese Analyse die rechtlichen Anforderungen geprüft. Anschließend werden aus den erhobenen Informationen die Sicherheitsanforderungen abgeleitet. Diese Anforderungen müssen vom Cloud-Service-Provider und dem Unternehmen eingehalten werden. [De10, S. 73]

Im zweiten Schritt der Planungsphase werden anhand der erhobenen Anforderungen und der Cloud-Kriterien, die im Kapitelabschnitt 2.1.5 beschrieben wurden, die Anbieter evaluiert und schlussendlich mittels eines Pflichtenheftes ausgewählt. [De10, S. 73]

3.3.2 Umsetzungs- und Migrationsphase

Die Vertragsgestaltung und die Definition eines Service-Level-Agreements gehören zu den Aufgaben in der dritten Phase des „Life-Cycle-Cloud-Computing". Bei der Definition der SLAs müssen die ITIL-Prozesse (Kapitelabschnitt 3.2) berücksichtigt werden. Diese Prozesse gewährleisten die Aufgabenverteilung zwischen den Unternehmen sowie dem Cloud-Service-Provider und sind somit für die Aufrechterhaltung der Service-Qualität verantwortlich. Des Weiteren empfiehlt die „BITKOM", dass das Augenmerk besonders auf folgende Aspekte der Informationssicherheit gelegt werden soll: [De10, S. 73]

- Definition von Schnittstellen insbesondere zu IT-Security-Monitoring
- Regel der Zugriffskontrolle mittels „Identity und Accessmanagement"
- Verschlüsselung der Daten beziehungsweise der Datenübermittlung
- Standort der Daten festlegen
- Desaster-Recovery-Szenarien definieren und Wiederherstellungszeiten festlegen
- Exit- beziehungsweise Ausstiegsregelungen definieren

Diese Anforderungen an die Informationssicherheit sind Empfehlung der „BITKOM" zugleich aber gesetzliche Anforderungen der Datenschutz-Grundverordnung (Kapitelabschnitt 2.2.7). Nachdem die Anforderungen erhoben wurden, kann die Umsetzung erfolgen. Die Umsetzung erfolgt anhand der erhobenen Informationen der Sicherheitsanalyse und natürlich anhand der vertraglich definierten und gesetzlichen Anforderungen. Die Migrations- und Umsetzungsphase schließt mit einem Abnahmeverfahren und einem Test ab. In

diesem Schritt werden alle relevanten Funktionen und Sicherheitsmaßnahmen überprüft. [De10, S. 74]

3.3.3 Betriebsphase

In der Betriebsphase muss der Cloud-Service-Provider alle vertraglichen und gesetzlichen Anforderungen erfüllen, um einen sicheren Betrieb zu gewährleisten. Anhand des Monitorings können die definierten SLA nach ITIL kontrolliert überprüft und nachgewiesen werden. Bei einer Abweichung muss der Service-Provider reagieren und das Service berichtigen. Jede Betriebsstörung sowie jeder Sicherheitsvorfall muss vom Service-Provider erhoben und behoben werden. Des Weiteren besteht eine Informationspflicht an den Nutzer beziehungsweise an den Kunden [De10, S. 74]

3.3.4 Beendigung (Exit)

Durch die Beendigung wird das Vertragsverhältnis zwischen den Vertragspartnern aufgelöst. Um die Informationssicherheit der Daten nicht zu gefährden, muss zu jedem Zeitpunkt das definierte Sicherheitsniveau gehalten werden. Des Weiteren muss der Cloud-Service-Provider nach der Auflösung des Vertrages die unwiederbringliche Löschung der Daten sicherstellen. [De10, S. 74]

Dieses beschriebene „Life-Cycle-Cloud-Computing“ der „BITKOM“ entspricht dem PDCA-Zyklus (Plan, Do, Check, Act), wie er auch in der Informationssicherheit (ISO/IEC 27001), dem IT-Service-Management (ITIL) und der Datenschutz-Grundverordnung (DSGVO) eingesetzt wird.

3.4 Datenschutz

Wie schon im Kapitelabschnitt 2.2 erläutert, verfolgt die Datenschutz-Grundverordnung das ambitionierte Ziel einen einheitlichen und hohen Datenschutzstandard innerhalb der EU zu etablieren. Dieses Ziel stellt einige Verantwortliche beziehungsweise Unternehmen vor eine große Herausforderung.

Die im Artikel 24, 25 und 32 der DSGVO beschriebenen technischen und organisatorischen Maßnahmen sind im Gesetzestext nicht immer eindeutig, sondern erfordern ein gewisses Maß an Interpretation. Somit ist die Umsetzung dieser Maßnahmen mit OnPremises-Systemen schon sehr herausfordernd. Nun stellt sich die Frage, wie Unternehmen mit Cloud-Services umgehen? Was muss ein Unternehmen aufweisen, um die Cloud-Compliance gemäß Artikel 24, 25 und 32 der Datenschutz-Grundverordnung zu gewährleisten? Laut einer Studie der „KMPG" ist Datenschutz das Top-Kriterium für die Auswahl eines Cloud-Anbieters. 97 Prozent aller deutschen Unternehmen wählten die Datenschutzkonformität bei Cloud-Services als wichtigstes Auswahlkriterium. [He19, S. 5]

Die „Cloud-Compliance" hängt von verschiedenen Aspekten ab. Die wichtigsten dieser Aspekte nach dem Cloud-Kompass wurden in diesem Kapitelabschnitt beschrieben. Die wechselseitigen Abhängigkeiten der beschriebenen Aspekte „Vertragsbedingungen", „IT-Service-Management", „Informationssicherheit" und „Datenschutz" konnten in diesem Kapitel deutlich herausgestellt werden. Nur wenn alle diese vier Aspekte berücksichtigt werden, kann ein sicherer und qualitativer Betrieb beziehungsweise Nutzung nach den vier Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit gewährleistet werden.

Im Kapitelabschnitt 3.5 werden mögliche Bedrohungen hinsichtlich der Einführung, des Betriebs und der Nutzung erläutert. Des Weiteren werden im folgenden Kapitelabschnitt 3.6 die dafür notwendwendigen technischen und organisatorischen Maßnahmen beschrieben. Diese Maßnahmen sollten für die nötige Cloud-Compliance sorgen. Die nachfolgenden Szenarien und Maßnahmen werden für Verantwortliche beziehungsweise für Unternehmen beschrieben. Aus diesem Grund referenzieren sich diese Maßnahmen und Empfehlungen auf die Nutzer und nicht auf die Cloud-Service-Provider-Sicht.

3.5 Bedrohungen von Cloud-Services

Cloud-Services sind stetig Bedrohungen von innen sowie von außen ausgesetzt. Um eine sichere Nutzung beziehungsweise einen sicheren Betrieb von Cloud-Services zu ermöglichen müssen die Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit gewährleistet werden. Deshalb ist es für Cloud-Nutzer beziehungsweise Cloud-Anwender essenziell wichtig, zusätzlich zu den Sicherheitsmaßnahmen des Cloud-Service-Provider eigene Maßnahmen zu ergreifen. Für die im folgenden Kapitelabschnitt beschriebenen Maßnahmen und Empfehlungen werden mögliche Bedrohungen von Cloud-Services beschrieben. Das „Bundesamt für Sicherheit in der Informationstechnik“ (kurz BSI) hat dazu einen Leitfaden für Cloud-Service-Nutzer veröffentlicht. Dieser Leitfaden soll eine sichere Cloud-Service-Einführung und -Nutzung gewährleisten. Anschließend werden im Kapitelabschnitt 3.6, für die beschriebenen Bedrohungen, mögliche Gegenmaßnahmen im Detail beschrieben.

3.5.1 Cloud-Provider-Infrastruktur

Die Cloud-Provider-Infrastruktur wird vom Cloud-Service-Provider verantwortet. Die Infrastruktur kann folgenden Bedrohungen ausgesetzt sein:

3.5.1.1 Administration

Durch eine fehlerhafte Administration sowie durch unbefugte oder ungeschulte Mitarbeiter kann es zu massiven Beeinträchtigungen oder zu Ausfällen des Cloud-Service kommen. Diese Fehler können sowohl vom Cloud-Service-Provider als auch vom Cloud-Service-Nutzer erfolgen. Eine Abhilfe schafft eine klare Rollenverteilung, ein Berechtigungskonzept sowie regelmäßige Schulungs- und Weiterbildungsmaßnahmen. [Bu16, S. 8]

3.5.1.2 Data-Loss

Auch ein Cloud-Service-Provider ist nicht vor Datenverlusten beziehungsweise von unerwünschten Datenabflüssen sicher. Die Daten können durch unbefugten Zugriff sowie durch ein fehlerhaftes Verhalten seitens des Cloud-Service-Providers oder dem Cloud-Nutzers zerstört werden. Der unbefugte Zugriff kann von innen, mangels eines unzureichenden Rollen- und Berechtigungskonzepts als auch von außen erfolgen. Data-Loss-Abhilfe können ein zureichendes Berechtigungs- beziehungsweise Rollenkonzept, eine Sicherungs- und Backupstrategie sowie Verschlüsselungsmechanismen schaffen. [Bu16, S. 8]

3.5.1.3 Verbindungsausfall

Durch einen Ausfall der Verbindung – in der Regel ist dies der Ausfall der Netzwerk- oder Internetverbindung zum Cloud-Service – kann das gewünschte Service nicht mehr genutzt werden. Die Verbindungsprobleme können sowohl beim Cloud-Service-Provider als auch beim Cloud-Service-Nutzer auftreten. Durch redundante Verbindungen vom Nutzer zum Cloud-Service-Provider können solche Ausfälle kompensiert werden. Wenn eine Verbindung ausfällt, dann wird automatisch auf die zweite Verbindung gewechselt. In den meisten Fällen setzen Unternehmen zwei Internet-Outbreacks von unterschiedlichen Providern ein, damit kann ein Internetausfall und somit der Ausfall zum Cloud-Provider verhindert werden. Die Cloud-Service-Provider müssen zudem über redundante Verbindungen von außen beziehungsweise nach außen verfügen. [Bu16, S. 8]

3.5.1.4 DDoS-Attacken

Distributed-Denial-of-Service-Attacken (kurz DDoS-Attacken) sind die häufigsten Bedrohungen rund um Cloud-Services. DDoS-Attacken sorgen über eine Überflutung von Anfragen zu einer Beeinträchtigung oder zu einem Ausfall des Service. Durch DDoS-Attacken auf das Cloud-Service beziehungsweise auf den

Cloud-Nutzer ist die Verfügbarkeit des Service betroffen. Aus diesem Grund muss der Cloud-Service-Provider beziehungsweise der Cloud-Nutzer für eine angemessene Sicherheit sorgen. Die Infrastruktur kann nur mittels spezieller Appliances gegen DDoS-Attacken geschützt werden. Diese Appliances sorgen dafür, dass der sichere von dem unsicheren Datenverkehr getrennt wird. Diese Appliances können OnPremises aber auch direkt als Cloud-Service bezogen werden. Wenn eine DDoS-Attacke bereits soweit fortgeschritten ist, dass die Bandbreite komplett belegt ist, dann muss der Internet-Provider den Datenverkehr zu einem sogenannten Scrubbing-Center umleiten. Diese Scrubbing-Center sorgen dafür, dass der Datenverkehr bereinigt wird. Nach der Bereinigung wird der Datenverkehr zum gewünschten Unternehmen weitergeleitet. Des Weiteren muss der Datenverkehr über ein Monitoring laufend überprüft werden. DDoS-Attacken können somit schnell entdeckt und abgewehrt werden. [Bu16, S. 8]

3.5.2 Nutzung von Cloud-Services

Die nächsten Bedrohungspotentiale werden bei der Nutzung von Cloud-Services ersichtlich. Folgende Bedrohungen können bei der Nutzung auftreten:

3.5.2.1 Identitätsmissbrauch

Der Identitätsdiebstahl und der anschließende Handel mit gestohlenen Identitäten ist in den vergangenen Jahren ein lukratives Geschäft geworden. Laut einer Studie von „Onlinesicherheit.at“ wurden im Jahr 2015 in den USA 490.220 Personen Opfer eines Identitätsdiebstahls. [A-18]

Durch einen Identitätsdiebstahl kann es zu unerlaubtem Zugriff auf die Cloud-Services kommen. Das bedeutet, dass die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität nicht mehr gewährleistet werden können. Durch den unerlaubten Zugriff kann es zu Zerstörung oder Manipulation der Daten sowie zu einem Komplettausfall des Service kommen. Ein Identitätsdiebstahl kann nur

durch klare Sicherheitsrichtlinien beziehungsweise Kennwort-Richtlinien und schlussendlich nur durch den Mitarbeiter selbst verhindert werden. Eine weitere Maßnahme, um sich vor einem Identitätsdiebstahls zu schützen, ist die Multi-Faktor-Authentifizierung. Durch die Absicherung eines zweiten oder dritten Faktors sind die gestohlenen Benutzerdaten wertlos. [Bu16, S. 8]

3.5.2.2 Endgerätesicherheit

Die Endgerätesicherheit stellt ein weiteres Risiko bei der Nutzung von Cloud-Services dar. Cloud-Services können, wie bereits in Kapitelabschnitt 2.1 beschrieben, von jedem Ort, zu jeder Zeit und von jedem Endgerät aus genutzt werden. Das bedeutet, dass sich die Endgerätesicherheit nicht mehr nur auf den klassischen Desktop beziehungsweise auf das klassische Notebook bezieht, sondern ebenso auf Smartphones, Tablets sowie auf alle gängigen IoT-Geräte. Diese Vielfallt an Geräten stellt Unternehmen vor eine große Herausforderung. Zum Schutz dieser Geräte müssen eine Endpoint-Protection sowie sichere Authentifizierungsmethoden etabliert werden. Des Weiteren müssen die Daten und Informationen auf den Geräten mit einer Verschlüsselung versehen werden. Somit haben potenzielle Angreifer keine Möglichkeit, auf die lokalen Daten der Geräte und somit keine Möglichkeit, auf die Cloud-Services zuzugreifen. [Bu16, S. 8]

3.5.2.3 Datendiebstahl

Der Datendiebstahl wurde bereits im Kapitelabschnitt 0 kurz erläutert. Bei der Nutzung von Cloud-Services kann es aber noch zu einem weiteren Fall des Datendiebstahls kommen. Die Daten können bei einer nicht vorhandenen oder unzureichenden Transportverschlüsselung abgefangen werden. Bei der Übertragung der Daten hat der Angreifer die Möglichkeit, die Daten zu stehlen. Eine klassische Angriffsmethode ist die „Man-in-the-Middle-Attacke“. Bei dieser Methode platziert sich der Angreifer zwischen dem Nutzer und dem Cloud-Service. Damit besteht die Möglichkeit, den Datentransfer abzufangen. Abhilfe

kann eine verschlüsselte Verbindung mittels Virtual Private Network (kurz VPN) schaffen. Durch VPN wird eine verschlüsselte Verbindung zum Ziel, in diesem Fall zum Cloud-Provider beziehungsweise Cloud-Services, aufgebaut. [Bu16, S. 8]

3.5.2.4 Missachtung von Vorgaben und Richtlinien

Die Nutzung von Cloud-Services setzt Richtlinien voraus, die die angemessene Nutzung der Cloud-Services regeln. Die Inventarisierung und Klassifizierung von Daten ist eine weitere maßgebliche Vorgabe. Diese Vorgabe regelt, welche Daten in der Cloud gespeichert beziehungsweise verarbeitet werden dürfen. Des Weiteren muss geregelt werden, welche Cloud-Services genutzt werden dürfen und welche vom Nutzer nicht genutzt werden dürfen. Die Nutzung von Cloud-Services kann man organisatorisch als auch technisch regeln, indem man den Zugang zu den nicht erwünschten Cloud-Services unterbindet. Des Weiteren muss das Unternehmen über Vorgaben und Richtlinien hinsichtlich der Datenschutz-Grundverordnung verfügen und ihre Mitarbeiter darauf hinweisen sowie die Mitarbeiter darauf schulen. Zudem müssen anhand von Richtlinien die Handhabung der Firmengeräte und der Benutzerdaten geregelt werden. Durch Missachtung der Richtlinien kann es im schlimmsten Fall zu Daten- sowie Identitätsverlusten kommen. Die Vorgaben und Richtlinien müssen den Mitarbeitern durch Schulungen und Trainings nähergebracht werden. Durch sogenannte Awareness-Trainings sollen die Mitarbeiter den sicheren Umgang mit Unternehmensdaten lernen. Diese Awareness-Trainings sind ein wesentlicher Bestandteil der Datenschutz-Grundverordnung und der Informationssicherheit gemäß ISO/IEC 27001. Die Einhaltung der Richtlinien kann organisatorisch als auch technisch überprüft werden. Bei nicht Einhaltung von Richtlinien müssen Sanktionen folgen. [Bu16, S. 8]

3.5.3 Einführung von Cloud-Services

Bei der Einführung von Cloud-Services kann es zu weiteren Sicherheitsbedrohungen kommen. Diese Gefahren und Risiken müssen bei der

Einführung beziehungsweise Migration minimiert oder ausgeschlossen werden. Durch folgende Bedrohungen könnte die Einführung eines Cloud-Services scheitern:

3.5.3.1 Cloud-Strategie

Eine vorhandene Cloud-Strategie ist die Grundlage für die Nutzung von Cloud-Services. Vor der Auslagerung von betriebskritischen Daten oder Anwendungen in die Cloud muss eine Cloud-Strategie erstellt werden. Die Cloud-Strategie wird von der Unternehmensstrategie abgeleitet und muss die wesentlichen organisatorischen und rechtlichen Rahmenbedingungen berücksichtigen. Besonders wichtig ist die Abgrenzung der bestehenden IT-Infrastruktur beziehungsweise IT-Systeme. Ein weiterer und auch sehr wichtiger Aspekt der Cloud-Strategie sind die sicherheitsrelevanten Rahmenbedingungen, die schon vor der Einführung der Cloud-Services definiert werden müssen. Ohne eine fundierte Cloud-Strategie kann der erhoffe Mehrwert der Cloud-Services sowie die sicherheits- und datenschutzrelevanten Aspekte nicht umgesetzt werden. [Bu12, S. 19]

3.5.3.2 Mangelhafte Planung beziehungsweise Anforderung

Eine weitere Gefahr besteht durch eine mangelhafte Planung sowie durch ein mangelndes Anforderungsmanagement. Eine mangelhafte Planung geht in den meisten Fällen aus einer mangelhaften oder nicht vorhandenen Cloud-Strategie hervor. Das bedeutet, dass ohne klare Anforderungen versucht wird, einen Cloud-Provider zu evaluieren und Cloud-Services einzuführen. Dies führt zu einer unzureichenden Sicherheits- und Datenschutzbetrachtung, was letztendlich die Sicherheit der personenbezogenen Daten gefährdet. Im Kapitelabschnitt 2.1.5 wurden die Cloud-Service-Kriterien des „Bundesamts für Sicherheit in der Informationstechnik“ (kurz BSI) beschrieben. Diese Kriterien des BSI helfen dem Nutzer den gewünschten Cloud-Service-Provider sowie das geforderte Cloud-Service zu evaluieren. Im Grunde handelt es sich hierbei um einen Leitfaden, der

die Entscheidungsfindung erleichtert und alle relevanten Sicherheits- und Datenschutzfaktoren berücksichtigt. [Bu16, S. 9]

3.5.3.3 Verantwortlichkeiten

Durch fehlende Verantwortlichkeiten kann es zu einer weiteren Gefahr bei der Einführung von Cloud-Services kommen. Es ist essenziell notwendig die Verantwortlichkeiten des Auftraggebers (Nutzer) und des Auftragnehmers (Cloud-Service-Provider) zu definieren. Die unzureichende Definition der Verantwortlichkeiten kann zu einem nicht gewünschten Ergebnis sowie zu Schuldzuweisungen zwischen den Parteien führen. Dies wiederrum kann ein Einführungsprojekt zeitlich verzögern oder zum Scheitern bringen. Die klare Definition der Aufgaben und der Zuständigkeiten sind bei der Einführung sowie für den Betrieb von Cloud-Services essenziell notwendig. Eine unzureichende Auslegung dieser Aufgaben und Zuständigkeiten bergen eine große Gefahr bei der Einführung und dem Betrieb von Cloud-Services. [Bu16, S. 9]

3.5.3.4 Projektmanagement

Ein professionelles Projektmanagement führt zu einem erfolgreichen Einführungsprojekt. Ein Cloud-Service-Projekt entsteht aus der hervorgegangenen Cloud-Strategie und beinhaltet nicht nur die bereits beschriebenen Punkt 3.5.3.2, sondern ist auch für die ersten zwei Phasen des Life-Cycle-Cloud-Computing, der im Kapitelabschnitt 3.3 beschrieben wurde, verantwortlich. Des Weiteren ist das Projektmanagement für die Überführung des Cloud-Service in den Betrieb unerlässlich. Das bedeutet, dass aus einem Cloud-Service-Projekt ein produktiver Service generiert wird. Das ist ein wesentlicher Schritt, der in viele Projekten - somit auch in Cloud-Service-Projekten - zu Problemen führt. Eine mangelhafte Servicedefinition sowie eine unzureichende Serviceübergabe können im anschließenden Betrieb des Cloud-Service zu Problemen führen. [Bu16, S. 9]

Um diese Bedrohungen und Gefahren ausschließen zu können, werden im nächsten Kapitelabschnitt Empfehlungen und Maßnahmen beschrieben und im Detail erläutert.

3.6 Empfehlungen und mögliche Maßnahmen

In diesem Kapitel werden Empfehlungen und Maßnahmen dargestellt, um die „Cloud-Compliance“ zu gewährleisten. In den vorherigen Kapitelanschnitten 3.1, 3.2, 3.3 und 3.4 wurden die vier Faktoren der „Cloud-Compliance“ beschrieben. Des Weiteren wurde im Kapitelabschnitt 3.5 auf die Gefahren und Bedrohungen bei der Einführung und des Betriebs von Cloud-Services hingewiesen. Auf Grundlage der genannten Faktoren werden nun Empfehlungen und Maßnahmen abgeleitet, um eine sichere und datenschutzkonforme Cloud-Service-Einführung sowie einen Cloud-Service-Betrieb zu gewährleisten. Die Maßnahmen werden in organisatorische und technische Maßnahmen untergliedert. In der Regel gestalten die organisatorischen Maßnahmen den Rahmen beziehungsweise die Vorgaben für die technischen Maßnahmen. Nur eine Kombination aus organisatorischen und technischen Maßnahmen können einen ganzheitlichen Schutz gewährleisten.

3.6.1 Organisatorische Maßnahmen

Bei organisatorischen Maßnahmen handelt es sich um alle vertraglichen und innerbetrieblichen Maßnahmen, um alle Aspekte die die Cloud-Compliance betreffen, zu erfüllen. Organisatorische Maßnahmen werden durch Richt- und Leitlinien, Service-Level-Agreements und Verträge geregelt. Eine weitere nicht unwesentliche, organisatorische Maßnahme ist das Risikomanagement. Dieses ist unerlässlich für die Einführung und den Betrieb von Cloud-Services.

3.6.1.1 Inventarisieren der Daten

Bevor es zu einer Auslagerung von Daten oder Services kommen kann, müssen diese identifiziert und klassifiziert werden. Daten müssen vom Unternehmen identifiziert und anschließend nach ihrer Kritikalität klassifiziert werden. Das bedeutet, dass die Daten je nach Klassifizierung einen unterschiedlichen Schutzniveau unterliegen. Die Datenklassifizierung sollte gemäß dem Anforderungskatalog (C5) des BSI nach folgenden Kriterien erfolgen: [Bu17, S. 39]

- Die Kritikalität der Verfügbarkeit des Cloud-Service und der Offenlegung gegenüber den Daten nicht autorisierter Dritter
- Der Datentyp und Servicetyp
- Rechts- und Geschäftsordnung
- Lokation der Daten
- Rechtliche und vertragliche Einschränkungen
- Der Wert der Daten

3.6.1.2 Risikomanagement

Eine weitere organisatorische Maßnahme ist das Risikomanagement. Hinsichtlich der Cloud-Compliance sind zwei Aspekte des Risikomanagements zu betrachten, erstens hinsichtlich der Informationssicherheit und zweitens hinsichtlich des Datenschutzes. Somit muss das Risiko hinsichtlich der Sicherheitsziele Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit minimiert, beseitigt oder ausgelagert werden. Ein mögliches Restrisiko muss so gering wie möglich gehalten werden. Veränderungen der Organisation und Systeme müssen stetig neu bewertet und in der Risikoanalyse ergänzt werden. Durch regelmäßige Audits und Reviews kann das Risikomanagement überprüft werden. [Ke16, S. 40]

Des Weiteren ist Risikomanagement ein essenzieller Teil der Datenschutz-Grundverordnung. Ein effizientes Risikomanagement ist die Voraussetzung für die

Datenschutzfolgeabschätzung. Diese Datenschutzfolgeabschätzung (kurz DSFA) bewertet das Risiko der einzelnen Verarbeitungstätigkeiten. Ziel der DSFA ist es, die Höhe des Risikos für die Rechte und Freiheiten der Betroffenen abzuschätzen. Diese DSFA ist bei systematischer massenhafter Datenverarbeitung sowie bei Neueinführungen von Systemen notwendig. [BI16, S. 14]

3.6.1.3 Cloud-Provider-Auswahl

Voraussetzung für die Cloud-Provider-Auswahl ist eine Cloud-Strategie und klare Anforderungen an das Cloud-Service. Wie im Kapitelabschnitt 2.1.5 beschrieben, erleichtert der Kriterienkatalog von „Trusted Cloud“ die Auswahl der Anbieter. Folgende Kriterien sind ausschlaggebend, um die Cloud-Compliance zu gewährleisten: [Bu18, S. 20ff.]

- Vertragsvollständigkeit und Transparenz
  Die Vertragsgestaltung muss vollständig und nach nationalem Recht ausgerichtet sein. Die Datenschutzbestimmungen, die Informationssicherheit und die Service-Level-Agreements sind wesentliche Bestandteile der Vertragsgestaltung. Die Vertragsbestimmungen und das Preismodell sind transparent darzustellen. Die Nachweißpflichten hinsichtlich der Datenschutz-Grundverordnung und der Informationssicherheit müssen vorhanden sein. Diese können mittels Zertifikaten bekräftigt werden. Des Weiteren müssen die Verantwortlichkeiten der Vertragsparteien in den Verträgen definiert werden. Diese genannten Punkte werden zu einem Dienstleistervertrag zusammengefasst.
- Der Anbieter kann ein effizientes IT-Service-Management mit der entsprechenden Service-Qualität vorweisen und abbilden. Die beschriebenen ITIL-Prozesse des Kapitelabschnitt 3.2 müssen berücksichtigt werden.

- Subunternehmen müssen explizit ausgewiesen werden. Des Weiteren müssen die Subunternehmer die beschriebene Vertragsvollständigkeit und Transparenz nachweisen.
- Der Speicherort der Daten muss vom Cloud-Service-Provider dargelegt werden. Wenn die Daten innerhalb der Europäischen Union gespeichert und verarbeitet werden, muss der Cloud-Service-Provider gemäß Artikel 25 und 32 für den ausreichenden Schutz der Speicherung und die Verarbeitung der Daten sorgen. Sollten die Daten außerhalb der Europäischen Union gespeichert oder verarbeitet werden, muss das Drittland gemäß Artikel 55 der DSGVO über einen angemessenen Datenschutz verfügen. Ein angemessener Datenschutz kann durch EU-Standardverträge mit Drittländern gewährleistet werden. So hat die EU mit den Vereinigten Staaten von Amerika ein angemessenes Datenschutzniveau beschlossen (EU-US Privacy Shield). Wenn ein amerikanisches Unternehmen diese Kriterien erfüllt, dann entspricht es den Vorgaben der EU-Datenschutz-Grundverordnung.
- Cloud-Service-Zertifikat

  Ein Cloud-Service-Provider kann sich durch Zertifizierungen einen Wettbewerbsvorteil schaffen. Den Nutzern erleichtern solche Zertifizierungen die Auswahl der Cloud-Service-Provider. Folgende Zertifizierungen sind für die Cloud-Compliance relevant:

Abdeckung	Zertifizierungen
Informationssicherheit	ISO/IEC 27001 und 27018; BSI IT-Grundschutz; CSA Star; TÜV Cloud-Security; TÜV „Trusted-Cloud"
Servicemanagement	ITIL v4; ISO/IEC 20000;
Datenschutz	Trusted Cloud Privacy; EuroPrise;
Vertragsbedingungen und Compliance	EuroCloud Star Audit; Trust in Cloud; ISAE 3402/SSAE16

Tabelle 4 - Cloud-Provider-Zertifizierungen [Tr16, S. 6]

3.6.1.4 Rollendefinitionen und Berechtigungskonzepte

Eine weitere organisatorische und nicht unwesentliche Maßnahme ist ein klares Rollen- und Berechtigungskonzept. Die Vertragspartner sowie die Mitarbeiter des Unternehmens müssen definierten Rollen zugeordnet werden. Diese Rollen bestimmen über die Aufgaben und Pflichten sowie über die Zugriffsberechtigungen dieser Parteien. Das sogenannte rollenbasierte Zugriffsmodell vergibt die Zugriffsrechte über die davor definierten Rollen. Welche Zugriffsberechtigung mit welcher Rolle verknüpft wird, hängt vom „Need-to-Know" sowie von der Kritikalität und Sensibilität der Daten ab. Das „Need-to-Know-Prinzip" besagt, dass nur die Mitarbeiter auf die Daten zugreifen dürfen, die sie unmittelbar für ihre Arbeit benötigen. Diese Rollen werden in ein Berechtigungskonzept umgelegt. Dieses Berechtigungskonzept schützt Systeme und Daten vor unberechtigtem Zugriff durch Dritte und vermeidet damit die Zerstörung und Manipulation schutzwürdiger Daten. Damit werden die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet. [Ec06, S. 444]

3.6.1.5 Clean-Desk-Policy / Clean-Screen-Policy

Ein aufgeräumter Arbeitsplatz kann Security-Incidents verhindert. Es wird empfohlen, eine Clean-Desk-Policy zu erstellen. Das Ziel dieser Policy ist es, die herumliegende Speichermedien, Arbeitsgeräte sowie aufgeschriebene Kennwörter vor Unbefugten beziehungsweise Angreifern zu schützen. Mobile Endgeräte müssen versperrt aufbewahrt werden. Kennwörter dürfen nicht aufgeschrieben und am Arbeitsplatz platziert werden. Ein weiterer Schritt ist die Clean-Screen-Policy. Diese soll bei nicht Anwesenheit des Mitarbeiters eine Bildschirmsperre bewirken. Damit soll auch bei einer kurzen Abwesenheit des Mitarbeiters der unbefugte Zugriff verhindert werden. Hinsichtlich der Cloud-Compliance kann eine Clean-Desk- und Clean-Screen-Policy einen

unerwünschten Zugriff auf Cloud-Services verhindern und somit die Schutzziele Vertraulichkeit und Integrität gewährleisten. [Ke16, S. 149]

3.6.1.6 Passwort-Policy

Eine Passwort-Policy regelt die Länge, die Komplexität sowie die periodische Änderung des Benutzerpassworts. Des Weiteren soll durch die Passwort-Policy sichergestellt werden, dass die Kennwörter sicher verwahrt und nicht weitergegeben werden. Diese Maßnahmen sollen einen unbefugten Zugriff auf Daten und Systeme verhindern. Das „National Institute of Standards and Technology“ (kurz NIST) hat im Jahr 2018 seine Passwortempfehlungen aktualisiert. Laut NIST müssen sichere Passwörter nur wenige beziehungsweise keine Sonderzeichen enthalten und auch nicht häufig geändert werden. Laut NIST muss ein sicheres Kennwort mindestens zwölf Zeichen lang sein. Eine Passwort-Policy wird durch technische Maßnahmen unterstützt. So wird eine Passwort-Policy über ein zentrales Management wie z.B. Active Directory oder Mobile Device Management ausgerollt und auf den Geräten erzwungen. [Bo17]

Eine weitere Maßnahme, um die Zugriffskontrolle zu sichern, ist die Multi-Faktor-Authentifizierung. Diese unterstützt die Identifizierung des Benutzers durch mehrere Faktoren. Die Multi-Faktor-Authentifizierung wird im Kapitelabschnitt 3.6.2 im Detail erläutert.

3.6.1.7 Schulungen und Leitlinien

Mitarbeiterschulungen und Sensibilisierungsmaßnahmen sind ein wichtiger Bestandteil der organisatorischen Maßnahmen. Schulungen, Trainings und Awareness-Maßnahmen sind wichtige und verpflichtende Bestandteile der Informationssicherheit gemäß ISO/IEC 27001 sowie der EU-Datenschutz-Grundverordnung. Mitarbeiter müssen über die korrekte Handhabe elektronischer Medien aufgefordert werden. Laut Datenschutz-Grundverordnung Artikel 9 Absatz 2 wird die „Sensibilisierung der an

Verarbeitungsvorgängen Beteiligten“ verpflichtend vorgeschrieben. Die Schulungsmaßnahmen können intern als auch extern gestaltet werden. Wichtig ist, dass alle Maßnahmen dokumentiert werden und für eventuelle Audits nachweisbar sind. Die Schulungsmaßnahmen sollten durch Richt- beziehungsweise Leitlinien verstärkt werden. Diese Leitlinien sollen die Nutzung und den Einsatz von Informations- und Kommunikationstechnologie und damit zusammenhängende Handlungsanweisungen beschreiben. [VB18, S. 153]

3.6.1.8 Change-Management

Das Change-Management muss mit dem Cloud-Service-Provider vertragliche geregelt und festgelegt werden. Ohne einen funktionierenden Change-Management-Prozess kann es zu Problemen bei der Verfügbarkeit kommen. Unzureichendes Change-Management kann z.B. die Skalierbarkeit der Kapazitäten und der Performance beeinflussen. Der Change muss vertraglich definiert und fixiert werden. Jeder Change wird von einer verantwortlichen Person gesteuert, freigegeben, durchgeführt, getestet und anschließend dokumentiert. Change-Management ist somit ein unverzichtbarer Prozess für die Realisierung der Cloud-Compliance. [LBD14, S. 29]

3.6.1.9 Computer-Security-Incident-Response-Team

Durch ein Computer-Security-Incident-Response-Team (kurz CSIRT) sollen mögliche Sicherheitsvorfälle standardisiert und mit dem geringsten Impact für das Unternehmen abgearbeitet werden. Ein CIRST besteht in der Regel aus Mitarbeitern der IT und der Geschäftsführung. Dieses Gremium ist der Single-Point-of-Contact bei einem Sicherheitsvorfall in der Informationstechnik. Das ist insbesondere wichtig, da jeder Security-Incident Auswirkungen auf die Datenschutz-Grundverordnung hat. Durch die Verletzung der Sicherheitsziele muss der Vorfall analysiert, protokolliert und geeignete technische und organisatorische Maßnahmen abgeleitet werden. Wenn zudem personenbezogen Daten betroffen sind, muss eine Meldung an die

Datenschutzbehörde erfolgen. Dies erfolgt über den Data-Breach-Prozess der im nachfolgenden Kapitelabschnitt 3.6.1.10 erläutert wird. Ein CSIRT ist eine unerlässliche Organisation in der Organisation. [TL16, S. 253]

3.6.1.10 Data-Breach

Gemäß Artikel 33 der DSGVO handelt es sich bei einem Data-Breach um die Verletzung des Schutzes von personenbezogenen Daten. Nach dem Eintritt des Data-Breaches hat der Verantwortliche 72 Stunden Zeit, den Vorfall der Datenschutzbehörde zu melden. Die Meldung an die Behörde muss detaillierte Informationen und Analysen über den Vorfall enthalten. [VB18, S. 84]

Um diese gesetzlichen Anforderungen erfüllen zu können, müssen klare und strafe Prozesse eingeführt werden. Aus diesem Grund ist es ratsam, ein CSIRT im Unternehmen zu etablieren. Speziell in KMUs übernimmt ein bestehendes CSIRT die Kommunikation mit der Datenschutzbehörde. Das hat den Vorteil, dass ein und dasselbe Team die Vorfälle vom Erkennen bis hin zum Ableiten der Verbesserungsmaßnahmen behandelt.

3.6.1.11 Business-Continuity-Management

Als nächste organisatorische Maßnahme wird das Business-Continuity-Management (kurz BCM) beschrieben. Das BCM definiert den Notfallplan der Unternehmen im Falle eines Systemausfalls. Im Fall der Cloud-Compliance handelt das BCM vom Ausfall der Cloud-Services. Die Ausfälle können verschiedenste Gründe haben z.B. Netzwerkausfall, Ausfall der Internetverbindung, DDoS-Attacken, technischer Ausfall des Cloud-Service, etc.. Aus diesem Grund benötigt ein Unternehmen egal in welcher Größe einen Notfallplan. Das BCM ist Teil des Risikomanagements und wird in die Risikobewertungen miteinbezogen. BCM umfasst Notfallübungen und die Notfallbehandlung. Die Notfallübungen sollten in regelmäßigen Abständen durchgeführt werden und sollen mögliche Notfallszenarien wiederspiegeln.

Aufgrund dieser gewonnenen Erkenntnisse aus der Notfallübung müssen Notfallmaßnahmen abgeleitet und dokumentiert werden. [Ke16, S. 219]

BCM ist ein wichtiger Bestandteil der Informationssicherheit gemäß ISO/IEC 27001 und der EU-Datenschutz-Grundverordnung, wenn es um die Risiko- und Datenschutz-Folgenabschätzung geht. Damit ist BCM ein wichtiger Bestandteil der Cloud-Compliance.

3.6.1.12 Audit

Audits sind ein weiterer wichtiger Bestandteil, um die organisatorischen und technischen Maßnahmen in regelmäßigen Abständen zu prüfen. Audits können von externen sowie internen Auditoren durchgeführt werden. Ziel des Audits ist es, alle implementierten Maßnahmen zu prüfen, um den gesetzlichen und organisatorischen Vorgaben zu entsprechen. Die Audits sollten sich nicht nur rein auf das verantwortliche Unternehmen stützen, sondern müssen auch beim Cloud-Service-Provider durchgeführt werden beziehungsweise muss der CSP einen Nachweis erbringen, dass er in regelmäßigen Abständen Audits durchführen lässt. [Jo18, S. 7]

Eine weitere Maßnahme eines Audits kann ein Penetrationstest sein. Dabei wird eine Cyberattacke auf das Unternehmen oder auf definierte Systeme simuliert. Durch solche geplanten Attacken können Schwachstellen identifiziert und in späterer Folge geschlossen werden. Penetrationstests sind ein wichtiger Bestandteil der ISO/IEC 27001 und unterstützen bei der Einhaltung der DSGVO Artikel 32. Dort wird auf den „aktuellen Stand der Technik“ verwiesen. Penetrationstest können dabei eine Unterstützung sein, um den Nachweis zu erbringen, den gesetzlichen Vorgaben zu entsprechen. [Ke16, S. 208]

Organisatorische Maßnahmen sind die erste Sperrspitze, um die beschriebenen Sicherheitsziele Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit zu gewährleisten. Die beschriebenen Maßnahmen müssen im Unternehmen

verankert und gelebt werden. Das bedeutet, dass die Maßnahmen einem kontinuierlichen Verbesserungsprozess unterliegen müssen. Nur so kann eine stetige Verbesserung der Prozesse und somit die Sicherheit der Daten gewährleistet werden. Im nächsten Kapitel werden die technischen Sicherheitsmaßnahmen beschrieben.

3.6.2 Technische Maßnahmen

Technische Maßnahmen gewährleisten gemeinsam mit den bereits beschriebenen organisatorischen Maßnahmen die Schutzziele der Informationssicherheit und des Datenschutzes. Gemäß DSGVO müssen die technischen Maßnahmen „dem Stand der Technik" entsprechen. Das bedeutet, dass auch alle technischen Maßnahmen einem kontinuierlichen Verbesserungsprozess unterliegen müssen. Nur so kann eine stetige Verbesserung und Weiterentwicklung der technischen Maßnahmen erfolgen. In den folgenden Kapitelabschnitten werden technische Maßnahmen beschrieben, um eine sichere Cloud-Service-Nutzung für KMUs zu gewährleisten.

3.6.2.1 Muti-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (kurz MFA) ist eine technische Maßnahme, die den Zugriff auf Cloud-Services absichern soll. Die bereits beschriebene Passwort-Policy ist der Grundstein der Multi-Faktor-Authentifizierung. In dieser organisatorischen Maßnahme werden die Richtlinien der Authentifizierung und somit des Zugriffschutzes festgelegt. Eine Authentifizierung rein mit Benutzer und Kennwort ist heutzutage nicht mehr ausreichend. Bei einer MFA benötigt der User mehrere unabhängige Faktoren um sich zu Authentifizieren. Meist wird der Faktor „Wissen" (Passwort, Pin, etc.) mit dem Faktor „Besitz" (Token, Chipkarte, etc.) und mit dem Faktor „Physisches Merkmal" (Fingerabdruck, Stimme, Iris, etc.) verbunden und abgefragt. Alle drei Faktoren müssen stimmen, um den User zu authentifizieren. Gemäß dem Cloud-Computing-Kompass und dem BSI wird für die Nutzung von Cloud-Services mindestens ein zweiter Faktor empfohlen. Durch

die MFA wird der Zugriff auf das Cloud-Service und somit die Vertraulichkeit der Daten geschützt. [Bu17, S. 26]

3.6.2.2 Backup

Eine weitere technische Maßnahme ist die lokale Sicherung der in der Cloud gespeicherten Daten und Konfigurationen. Durch diese Backupstrategie wird das Schutzziel „Verfügbarkeit" gewährleistet. Wenn es zu einem Ausfall der Internetverbindung oder des Cloud-Service-Provider kommen sollte, kann das Unternehmen weiterhin auf das lokale Backup zugreifen. Die Backupstrategie kann auch auf einen zweiten Cloud-Service-Provider ausgelagert werden, jedoch muss das Unternehmen in diesem Fall für eine redundante Internetverbindung sorgen. Die Backups sollten im Zuge des BCM einer stetigen Überprüfung unterliegen. [Bu17, S. 25]

3.6.2.3 Data Leckage Prevention

Das Unternehmen kann mit organisatorischen und technischen Maßnahmen den Cloud-Zugriff erlauben oder sperren. Wenn sich das Unternehmen anhand einer Cloud-Strategie für einen Cloud-Service-Provider entschieden hat, muss es dafür sorgen, dass diese Strategie nicht umgangen wird und weiterhin andere Cloud-Services genutzt werden. Die Gefahr besteht darin, dass das Unternehmen die Datenhoheit verliert und es somit zu Datenverlusten kommt. Das Unternehmen muss deshalb mittels technischer Maßnahmen den unerwünschten Datenabfluss verhindern. Zum einen müssen die Daten dem Unternehmen bekannt sein. Aus diesem Grund ist es vorab sehr wichtig, die Daten, wie bereits im Kapitelabschnitt 3.6.1.1 beschrieben, zu inventarisieren und zu kategorisieren. Anhand dieser Kategorisierung können unterschiedliche Rechte vergeben werden und damit verhindert werden, dass Daten unerwünscht weitergeben werden können. Zum anderen müssen technische Maßnahmen gesetzt werden, um den unerwünschten Datenabfluss zu verhindern. Der Zugriff auf nicht freigegebene Cloud-Service-Provider muss technisch verhindert werden. Das kann anhand von

zentralen Netzwerkeinstellungen sowie Clienteinstellungen erfolgen. [Ke16, S. 168]

Eine weitere technische Maßnahme, um die Vertraulichkeit und Integrität der Daten zu schützen, ist die Verschlüsselung. Sie wird im nächsten Kapitelabschnitt beschrieben.

3.6.2.4 Verschlüsselung

Gemäß Artikel 32 der DSGVO müssen personenbezogene Daten verschlüsselt werden. Somit ist die Verschlüsselung ein wichtiger Faktor der Cloud-Compliance hinsichtlich der Informationssicherheit und des Datenschutzes. Die Verschlüsselung der Daten gewährleistet die Einhaltung des Schutzziels Vertraulichkeit. [Ra16, S. 51]

Um einen ausreichenden Schutz der Daten zu gewährleisten, ist es notwendig, alle in der Cloud gespeicherten Daten und nicht nur die personenbezogenen Daten zu verschlüsseln. Durch eine Verschlüsselungsstrategie, die ein unternehmensübergreifendes Verschlüsselungsverfahren unterstützt muss, kann das Schutzziel am effektivsten umgesetzt werden. Das bedeutet wiederum, dass jegliches Endgerät, das Zugriff auf das Unternehmensnetzwerk und auf das Cloud-Service hat, verschlüsselt werden muss. Des Weiteren muss das Unternehmen für eine sichere externe und interne Kommunikation mittels einer sicheren Ende-zu-Ende-Verschlüsselung sorgen. [Bu17, S. 69]

3.6.2.5 Endpoint-Protection

Um eine Infiltrierung des Benutzers als auch der Daten zu verhindern, ist es essenziell notwendig eine effiziente Endpoint-Protection zu implementieren. Sobald Unbefugte Zugriff auf den Client bekommen, haben diese auch Zugriff auf die Cloud-Services und die darauf gespeicherten Daten. Zur Absicherung des Endpoints zählt heutzutage nicht nur der reine Virenscanner. Mehrere

Faktoren sind für eine effiziente Endpoint-Protection unerlässlich. Der Virenscanner wurde in den vergangenen Jahren stetig weiterentwickelt, um mit den aktuellen Bedrohungen mitzuhalten. Die neueste Generation der Viren- und Malwarescanner sind auf einer verhaltensbasierten Plattform aufgebaut. Damit wird das stetige Verhalten des Endpoints geprüft und bei unerwünschtem Verhalten wird der Prozess gestoppt oder verhindert. Diese Technologie ist aus den „Ransomware-Attacken" entstanden und ist bei den führenden Herstellern Stand-der-Technik. Des Weiteren muss dafür Sorge getragen werden, dass die Sicherheitsapplikationen, sowie das Betriebssystem und alle weiteren Applikationen auf dem Endpoint immer auf dem aktuellen Stand gehalten werden. Das kann durch ein Patchmanagement realisiert werden. Die Herausforderung sind die Dritt-Hersteller-Anwendungen, die vom Microsoft-Patchmanagement nicht berücksichtigt werden. Aber die Endpoint-Protection gilt nicht nur für die klassischen Endpoints wie Desktops oder Notebooks. Vielmehr müssen heutzutage alle Endpoints geschützt werden. Dazu zählen auch Smartphones, Tablets sowie sämtliche IoT-Geräte. Alle Geräte verfügen über Schnittstellen und sind somit ein mögliches Angriffsziel. [Bu17, S. 73]

3.6.2.6 Angriffserkennung und -abwehr

Die letzte Maßnahme beschreibt eine Methode, um Angriffe von außen zu verhindern. Die Angriffserkennung und -abwehr bietet eine technische Maßnahme, um Angriffe auf das Netzwerk von außer zu erkennen und abzuwehren. Intrusion Detection Systeme (kurz IDS) bieten den Unternehmen eine effiziente Unterstützung bei der Angriffserkennung. Mittels IDS werden Verbindungen über Zugriffsmuster erkannt und je nach Konfiguration der Intrusion Prevention Systeme (kurz IPS) geblockt, beobachtet oder durchgelassen. Somit können gefährliche Verbindungen beziehungsweise Angriffe von außen schnell erkannt und automatisch behandelt werden. Diese Maßnahme muss sowohl vom Cloud-Service-Provider als auch vom Verantwortlichen eingesetzt werden.

Durch die Angriffserkennung und -abwehr kann die Verfügbarkeit, Vertraulichkeit und Belastbarkeit gewährleistet werden [De10, S. 76]

Die technischen Maßnahmen ergänzen die organisatorischen Maßnahmen und gewährleisten somit das Schutzziel der Informationssicherheit und der Datenschutz-Grundverordnung. Nur durch einen kombinierten Einsatz von organisatorischen und technischen Maßnahmen kann die Cloud-Compliance gewährleistet werden. Im letzten Abschnitt wird das Kapitel „Cloud-Compliance" zusammengefasst.

3.7 Zusammenfassung

Das Kapitel 3 stand im Fokus der „Cloud-Compliance". Die Cloud-Compliance setzt sich gemäß dem „Cloud-Kompass" aus den vier Teilbereichen „vertragliche Rahmenbedingungen", „IT-Service-Management", „Informationssicherheit" und „Datenschutz" zusammen. Wie in diesem Kapitel beschrieben, kann nur eine Kombination aus diesen vier Teilbereichen einen ausreichenden Schutz von personenbezogenen Daten gewährleisten. Alle Schutzmaßnahmen dieser vier Teilbereiche müssen einem kontinuierlichen Verbesserungszyklus (PDCA) unterliegen. Nur damit kann auch ein nachhaltiger Schutz gewährleistet werden. Durch das beschriebene „Life-Cycle-Cloud-Computing" wurde ein weiteres Modell beschrieben, um die Cloud-Nutzung hinsichtlich der Informationssicherheit zu gewährleisten. Die vier beschriebenen Phasen des „Life-Cycle-Cloud-Computing" entsprechen ebenfalls dem PDCA-Zyklus.

Des Weiteren wurden in diesem Kapitel auf die Bedrohungen von Cloud-Services hingewiesen. Cloud-Services unterliegen einer Vielzahl von Bedrohungen. Diese Bedrohungen können bereits bei der Einführung schlagend werden. Die beschriebenen Schutzziele gemäß der Informationssicherheit und der Datenschutz-Grundverordnung (Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit) können nur durch die, im Kapitelabschnitt 3.6, beschriebenen

technischen und organisatorischen Maßnahmen geschützt werden. Die beschriebenen Maßnahmen und Empfehlungen wurden speziell für KMUs ausgelegt. Durch diese beschriebenen Maßnahmen und Empfehlungen können alle Cloud-Services, die personenbezogene oder sensible Daten verarbeiten, geschützt werden. Des Weiteren müssen die Zugriffe auf die Cloud-Services auditiert werden. Nur jene Personen, die darauf zugreifen müssen, werden tatsächlich mit den notwendigen Zugriffsberechtigungen ausgestattet. Dabei kommt das „Need-to-Know" Konzept zur Anwendung. Zudem müssen geeignete technische Vorkehrungen zur Erhaltung und Sicherstellung der Verfügbarkeit, Vertraulichkeit, Integrität sowie Belastbarkeit der Systeme getroffen werden. Darüber hinaus muss das Unternehmensnetzwerk gegenüber Angriffen durch geeignete technische Vorkehrungen geschützt werden. Es muss ein geeignetes Sicherungs- und Wiederherstellungskonzept der einzelnen Services erarbeitet werden, sodass im Fehlerfall die Daten mit einer bekannten Wiederherstellungsprozedur in einem angemessenen Zeitrahmen wiederhergestellt werden können. Vor allem aber muss man regelmäßige Überprüfungen und Bewertungen der Wirksamkeit der technischen und organisatorischen Maßnahmen durchführen. Hier müssen alle Services, Komponenten und das gesamte Umfeld betrachtet werden, um prüfen zu können, ob die aktuellen Maßnahmen den Anforderungen nach wie vor entsprechen beziehungsweise ob diese wirksam sind. Nur so kann die Cloud-Compliance und die damit verbundenen gesetzlichen Anforderungen der EU-Datenschutz-Grundverordnung gemäß Artikel 25 und 32 gewährleistet werden.

Das nachfolgende Kapitel 4 dieser Arbeit beschreibt den Aufbau und die Entwicklung der empirischen Studie. Des Weiteren werden die Ergebnisse der Studie analysiert und interpretiert.

4. EMPIRISCHE STUDIE

Im folgenden Kapitel wird das Forschungsdesign der zugrundeliegenden Arbeit beschrieben. Im ersten Abschnitt dieses Kapitels wird das Erhebungsinstrument, der quantitative Fragenbogen, erläutert. Des Weiteren wird die Durchführung der Umfrage und die wichtigsten Themengebiete des Online-Fragebogens beschrieben. Der zweite Kapitelabschnitt beschreibt die quantitative Analyse und Interpretation des Forschungsinhaltes. Als Zielgruppe für die quantitative Befragung wurden österreichische KMUs identifiziert. Mit Hilfe der Wirtschaftskammer Österreich konnten einige hundert KMUs identifiziert und adressiert werden.

4.1 Methodik

Die empirische Studie wurde nach der nachfolgenden Vorgehensweise aufgebaut und anschließend durchgeführt. Die einzelnen Schritte der Vorgehensweise werden in der Abbildung 10 grafisch dargestellt.

Abbildung 10 - Vorgehensweise d. empirischen Studie

Die Studie startet mit einer umfangreichen Literaturrecherche zu den Themengebieten „Cloud-Computing“, „EU-Datenschutz-Grundverordnung“ und den „kleinen und mittelständischen Unternehmen (KMUs)“. Diese theoretischen Grundlagen wurden bereits im Kapitel 2 erläutert und dokumentiert. Des Weiteren konnten durch das Thema „Cloud-Compliance“ die zuvor beschriebenen Themenbereiche kombiniert und die dazugehörigen Abhängigkeiten aufgezeigt werden. Nachdem die Literaturrecherche abgeschlossen war, konnte die Fragestellung der zugrundeliegenden Forschungsfrage und die davon abgeleitete Hypothese definiert werden. Nach der Definition der Forschungsfrage wurde der Entwurf mit dem Betreuer

abgestimmt. Nach kleinen Optimierungen beziehungsweise Anpassungen konnte die Forschungsfrage finalisiert werden.

Die quantitative Forschungsmethode basiert auf einem Online-Fragenbogen. Die Bereiche des Fragebogens bauen auf den zuvor genannten Themengebieten „EU-Datenschutz-Grundverordnung“, „Cloud-Computing“ sowie „kleine und mittelständische Unternehmen (KMUs)“ auf. Der Fragenbogen schließt mit dem Themenbereich „Nutzungsverhalten“ ab. Der Aufbau und die beinhalteten Themengebiete werden im nächsten Kapitelabschnitt 4.2 im Detail erläutert. Beim Design des Fragebogens wurde versucht, einen breiten Überblick über die abgefragten Themengebiete zu bekommen. Die Ergebnisse sollen anhand der breiten Fragestellung einen guten Überblick der zusammenhängenden Aspekte der oben genannten Themengebiete geben. Nach einem groben Design des Fragenbogens wurde dieser mit dem Betreuer dieser Arbeit abgestimmt und anschließend einem Pre-Test unterzogen. Durch den Pre-Test war es möglich alle Antwort-Szenarien zu testen ohne die Ergebnisse zu verfälschen. Der Fragenbogen wurde insgesamt von drei verschiedenen Probanden vorab getestet. Der Testzeitraum betrug 10 Tage. Durch diese Testdurchläufe war es möglich erste Testdaten zu sammeln sowie den Fragenbogen inhaltlich zu prüfen. Durch die Rückmeldung konnten inhaltliche und funktionale Schwächen erkannt werden. Zum einen zeigten sich Schwächen bei der ungenauen Definition der Fragen und Antworten. Des Weiteren wurde durch den Pre-Test funktionale Schwächen aufgedeckt. Durch diese Rückmeldungen konnte der Fragenbogen angepasst beziehungsweise optimiert werden. Nach der Anpassungsphase und dem Abschluss des Pre-Tests wurden die Testdaten aus der Datenbank gelöscht.

Die Durchführung der Studie konnte mit einem Online-Fragenbogen-Tool namens "SoSci Survey“ realisiert werden. Der Service ist für wissenschaftliche Umfragen ohne kommerziellen Hintergrund kostenlos. Des Weiteren kann durch diese Online-Plattform der Online-Fragenbogen ohne großen Aufwand per

Online-Link verteilt werden. Ein weiterer Vorteil dieser Online-Plattform ist die einfache Bedienung und der übersichtliche Export der gesammelten Ergebnisse. Die Umfrage war von Ende Februar 2019 bis Ende März 2019 öffentlich zugänglich. In dieser Zeit wurde der Link zu der Umfrage über diverse Soziale Netzwerke und über eine Kontaktliste, die von der Wirtschaftskammer Österreich zur Verfügung gestellt wurde, verteilt.

Nachdem die Durchführung beendet war, konnten die Ergebnisse exportiert und analysiert werden. Bei der Analyse wurden die einzelnen Themenbereiche, die einzelnen Fragen und die Abhängigkeiten zwischen den zugrunde liegenden Themenbereichen behandelt. Die Auswertungsergebnisse werden im Kapitelabschnitt 4.3 im Detail beschrieben.

Im nächsten Kapitelabschnitt wird spezielles Augenmerk auf das Design des Fragebogens und den damit verbundenen Themengebieten gelegt.

4.2 Fragebogendesign

Der Fragenbogen wurde anhand der zuvor genannten Themenbereiche in vier Rubriken und insgesamt 24 Fragen aufgeteilt. In den folgenden Kapitelabschnitten werden die verschiedenen Rubriken und Fragen erläutert. Der gesamte Fragenbogen wird im Kapitel II Anhang dargestellt.

4.2.1 Allgemein

Die erste Rubrik des Fragenbogens beschäftigte sich mit der Vorstellung der Studie und des Autors der Umfrage. Des Weiteren wurde darauf hingewiesen, dass die Antworten vertraulich behandelt und anonym verarbeitet werden. Anschließend wurden die ersten Fragen über den Probanden und dem angehörigen Unternehmen des Probanden gestellt. Die Fragen beziehen sich auf die berufliche Position des Probanden, der zugehörigen Branche des Unternehmens sowie auf die Unternehmensgröße hinsichtlich der

Mitarbeiteranzahl. Letzteres ist essenziell, um KMUs zu identifizieren. Unternehmen, die unter 250 Mitarbeiter beschäftigen, werden in der Studie als KMUs identifiziert. Die im Kapitelabschnitt 2.3 beschriebenen Kriterien „Jahresumsatz“ und „Jahresbilanz“ wurden aus Komplexitätsgründen nicht in die Befragung mitaufgenommen. Die Befürchtung bestand, dass die Probanden die genannten Kriterien ihres Unternehmens nicht identifizieren können und somit die Forschungsergebnisse verfälschen könnten.

4.2.2 Cloud-Computing

Cloud-Computing war der Themenbereich der zweiten Rubrik des Fragenbogens. Eine sehr wesentliche Frage wurde am Anfang dieser Rubrik platziert. Diese Frage untersuchte, ob das Unternehmen Cloud-Services aktuell im Einsatz hat. Wenn aktuell keine Cloud-Services von dem Unternehmen genutzt wurden, dann wurde mit Hilfe eines Filters die restlichen Cloud-Computing-Fragen für den Probanden ausgeblendet. Wenn das Unternehmen jedoch Cloud-Services nutzte, dann blieben alle weiteren Fragen eingeblendet.

Des Weiteren wurden in dieser Rubrik die verwendeten Cloud-Service-Modelle, die im Kapitelabschnitt 2.1.3 erläutert wurden, abgefragt. Eine weitere Frage untersuchte die Cloud-Service-Provider (CSP), dazu wurden im Fragenbogen die bekanntesten CSP aufgelistet. Zusätzliche CSP konnten über ein freies Textfeld eingepflegt werden. Die weiteren Fragen bezogen sich auf die größten Treiber für die Cloud-Service-Nutzung, die Herausforderung bei der Nutzung von Cloud-Services und welche Kriterien für die Unternehmen bei der Auswahl von Cloud-Services am wichtigsten sind. Die letzten Fragen der Cloud-Computing-Rubrik beschäftigten sich mit der Cloud-Strategie. Verfolgten Unternehmen vor und nach Inkrafttreten der DSGVO eine Cloud-Strategie? Damit wurde der Übergang zur Rubrik „Datenschutz-Grundverordnung“ geschafften.

4.2.3 Datenschutz-Grundverordnung

Die dritte Rubrik des Fragenkatalogs fokussierte sich auf das Thema Datenschutz-Grundverordnung. Zur Einführung wurden die Probanden über die allgemeinen Ziele der DSGVO befragt. Des Weiteren wurde untersucht, wie wichtig Datenschutz in den einzelnen Unternehmen ist und ob das Unternehmen bereits Mitarbeiterschulungen zum Thema Datenschutz durchgeführt hat. Durch die Frage, ob das Unternehmen über einen Datenschutzbeauftragten verfügt, endeten die organisatorischen Datenschutzfragen. Die nächste Datenschutzfrage beschäftigte sich mit der Cloud-Service-Nutzung, somit wurden die Probanden explizit nach den TOMs und dem Auftragsverarbeitervertrag des CSP befragt. Die letzte Frage der Rubrik untersuchte, ob personenbezogene Daten oder Daten besonderer Kategorien in der Cloud verarbeitet oder gespeichert werden.

4.2.4 Nutzungsverhalten

Die letzte Rubrik des Fragenbogens untersuchte das Nutzungsverhalten von Cloud-Services vor und nach Inkrafttreten der DSGVO. Mit der ersten Frage wurde untersucht, ob es nach Inkrafttreten der DSGVO eine Nutzungsveränderung der Cloud-Services gegeben hat. Wenn es zu keiner Änderung der Nutzung kam ist, dann wurden mit Hilfe von Filtern alle Fragen bis auf die letzte Frage ausgeblendet. Wenn sich die Nutzung verändert hat, dann wurde untersucht, ob die Nutzung stieg oder sank. Des Weiteren wurde der Grund für die veränderte Nutzung der Cloud-Services untersucht. Die Rubrik endete mit der Frage, ob das Unternehmen auch in Zukunft Cloud-Services einsetzen wird.

Die gewonnenen Informationen aus dem Online-Fragenbogen sollen Aufschluss über die Nutzung und das Nutzungsverhalten von KMUs in Bezug auf Cloud-Services liefern. Des Weiteren sollen die Ergebnisse dieses Fragenbogens Auskunft über die Cloud-Strategien der Unternehmen sowie über die Datenschutz-

Priorisierung liefern. Der Online-Fragebogen wurde am 26.02.2019 nach Rücksprache mit dem Betreuer dieser Arbeit Herrn Thomas Krabina M.Sc., veröffentlicht. Die Deadline der Befragung wurde mit 31.03.2019 veranschlagt. Damit betrug der Befragungszeitraum 40 Tage. Der Fragenbogen wurde vom Autor mittels Sozialer Netzwerke, durch Unternehmen sowie durch die Wirtschaftskammer Österreich verteilt. Die Tabelle 5 gibt Aufschluss über die Rücklauf-Statistik der Online-Befragung.

Rücklauf-Statistik	Anzahl
Aufrufe des Interviews	373
Abgeschlossene Interviews	312
Befragungszeitraum	40 Tage

Tabelle 5 - Rücklauf-Statistik

Die Stichprobengröße für die zugrundeliegende Forschung beträgt 269. Als Ausgangswert wurde die Anzahl der österreichischen KMUs (328.900) herangezogen. Des Weiteren ging der Autor von einem Konfidenzniveau von 90 Prozent und einer Fehlerspanne von fünf Prozent aus. Daraus ergibt sich die beschriebene Stichprobengröße von 269. Durch die 312 abgeschlossenen Interviews konnte die berechnete Stichprobengröße erreicht werden.

In diesem Kapitel wurden der Aufbau sowie der Ablauf der quantitativen Online-Befragung dargestellt. Des Weiteren wurden die Fragen und die Rücklaufstatistik der Online-Befragung erläutert. Das nächste Kapitel beschreibt die Ergebnisse der Online-Befragung.

4.3 Analyse und Interpretation

In diesem Kapitelabschnitt werden die Ergebnisse der Online-Befragung grafisch aufbereitet und interpretiert. Die Ergebnisse der 24 Fragen werden anhand von Diagrammen aufbereitet und anschließend erläutert.

4.3.1 Allgemein

In der ersten Rubrik des Fragenbogens wurden Fragen zum Unternehmen sowie zu den Probanden gestellt. Wie in der Abbildung 11 dargestellt, sind 71 Prozent der befragten Unternehmen KMUs. Diese KMUs sind die Zielgruppe dieser Studie. Das bedeutet, dass es sich bei 222 von 312 (71 Prozent) untersuchten Unternehmen um KMUs handelt. 67 untersuchte Unternehmen sind Großunternehmen. Die restlichen 23 Unternehmensgrößen konnten nicht zugeordnet werden.

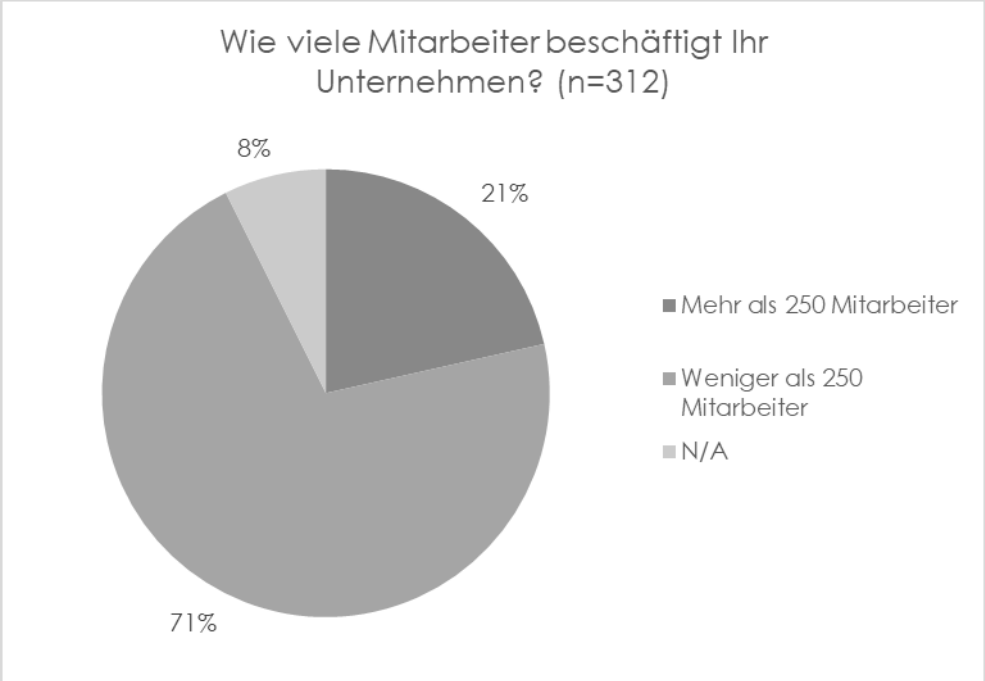


Abbildung 11 - Mitarbeiteranzahl der Unternehmen

Die nächste Frage der Rubrik „Allgemein" untersuchte die Position der Probanden im Unternehmen. Die Abbildung 12 stellt die Ergebnisse der Frage zwei grafisch dar. Durch diese Untersuchung konnte herausgefunden werden, dass 60 Prozent der befragten Probanden über eine Führungsrolle im Unternehmen verfügen. Diese Frage ist wichtig um die Qualität der Antworten zu eruieren. Probanden mit Führungsrollen haben einen tieferen Einblick in das jeweilige Unternehmen und können somit die folgenden Fragen mit einer

höheren Qualität beantworten. Die Großunternehmen und die Unternehmen, die nicht zugeordnet werden konnten, wurden nicht berücksichtigt.

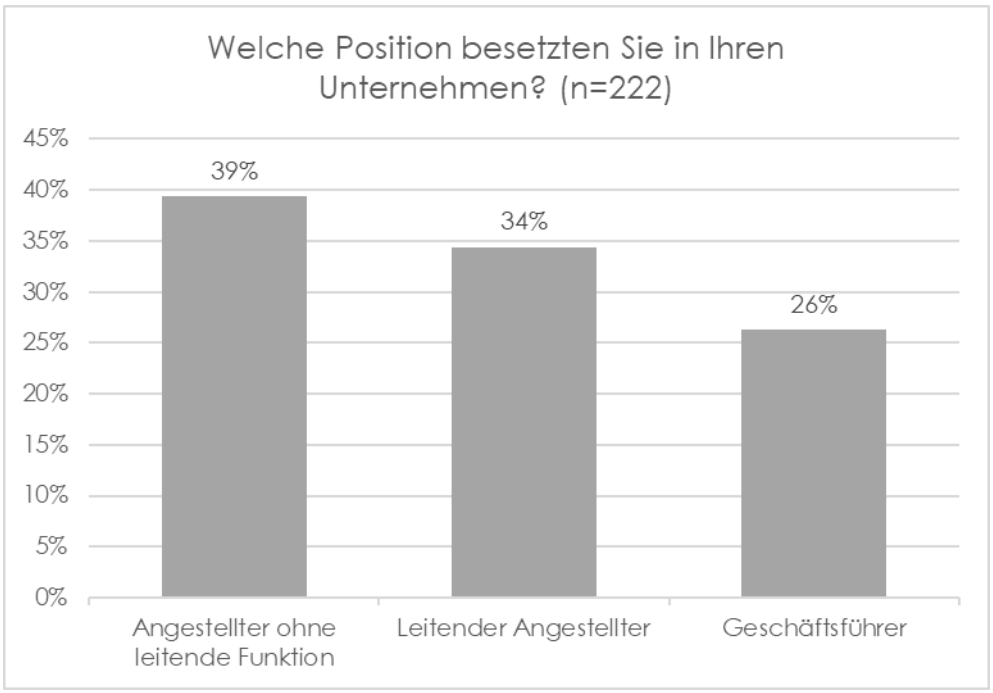


Abbildung 12 - Position des Probanden

Die dritte und somit letzte Frage aus der Rubrik „Allgemein" untersuchte die Branche des Unternehmens. Die folgende Abbildung 13 stellt die Ergebnisse der Befragung in einem Diagramm dar. Die Brache „Informationstechnologie" ist mit 21 Prozent (46 von 222 KMUs) die stärksten Branchen, gefolgt von den Brachen „Beratung" und „Handel". Durch die Auswertung der jeweiligen Branchen konnte im Anschluss das Nutzungsverhalten auf die untersuchten Branchen umgelegt werden. Im Kapitelabschnitt 4.3.4 werden die Ergebnisse des Nutzungsverhalten dargestellt.

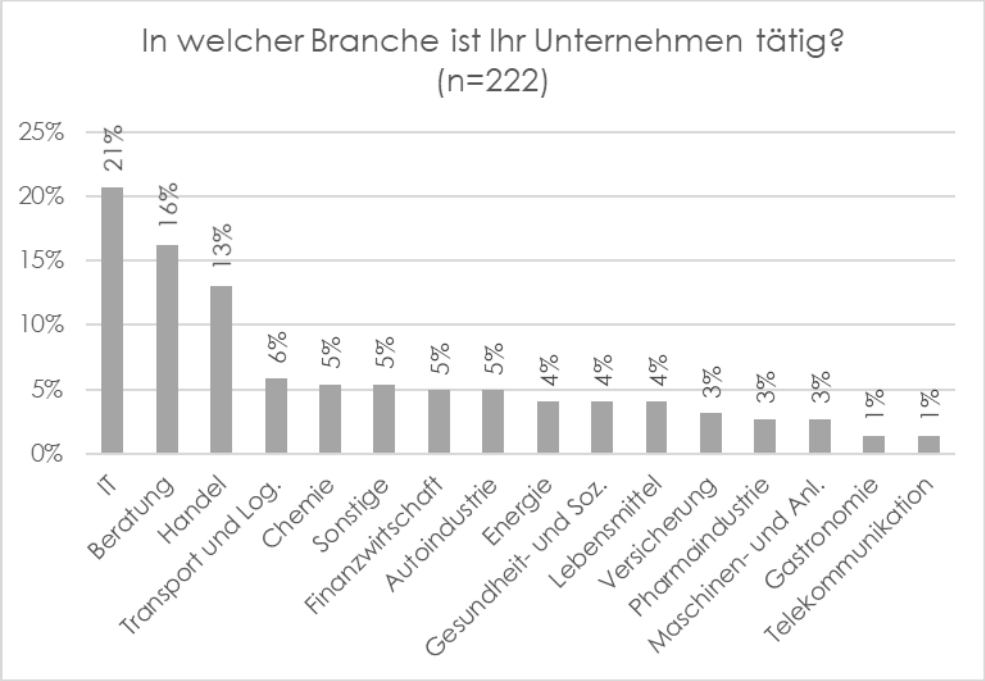


Abbildung 13 - Unternehmensbranchen

Die dargestellte Branchenaufteilung (Abbildung 13) wird von öffentlichen Statistiken belegt. Gemäß einer Studie der „KPMG" konnten IT-Unternehmen bereits im Jahr 2015 mit der Vorreiterrolle bei der Nutzung von Cloud-Services punkten. [Br15]

Des Weiteren kann durch eine Statistik der „Statistik Austria" die Cloud-Service-Nutzung in zwei Bereiche aufgeteilt werden. Laut dieser Statistik teilt sich die Cloud-Service-Nutzung zu 72,7 Prozent auf Dienstleistungsunternehmen auf. Die restlichen 27,3 Prozent fallen auf Produktionsunternehmen. Die Abbildung 13 zeigt ebenfalls einen höheren Anteil an Dienstleistungsunternehmen (IT, Beratung, Handel, Transport und Logistik, Finanzwirtschaft, Gesundheit, Versicherungen, Gastronomie und Telekommunikation). Alle dargestellten Dienstleistungsbranchen ergeben in Summe 70 Prozent der untersuchten Unternehmen. [DH18]

Die Ergebnisse der ersten Rubrik „Allgemein“ wurden in diesem Kapitel grafisch aufbereitet und erläutert. Bei den untersuchten 312 Unternehmen handelt es sich um 222 kleine und mittelständische Unternehmen. Damit fallen über zwei Drittel der untersuchten Unternehmen in die geforderte Zielgruppe. Des Weiteren weisen die Ergebnisse darauf hin, dass sich 60 Prozent der Probanden in Führungspositionen (Geschäftsführer oder leitende Angestellte) befinden. Durch die Analyse der Brachen wurde gezeigt, dass sich die meisten Unternehmen in der Branche „Informationstechnologiebranche“ befinden. Der nächste Kapitelabschnitt erläutert die Ergebnisse der Rubrik „Cloud-Computing“.

4.3.2 Cloud-Computing

Im folgenden Kapitelabschnitt werden die Forschungsergebnisse der zweiten Rubrik „Cloud-Computing“ erläutert. In dieser Rubrik werden die Probanden nach den eingesetzten Cloud-Service-Modellen sowie den eingesetzten Cloud-Service-Providern befragt. Des Weiteren werden in dieser Rubrik die Treiber, die Erfolgskriterien sowie die Herausforderungen bei der Einführung und bei der Nutzung von Cloud-Services analysiert. Der Kapitelabschnitt schließt mit der grafischen Darstellung der Cloud-Strategie ab.

Die Abbildung 14 stellt den Cloud-Service-Nutzungsgrad vor und nach Inkrafttreten der DSGVO grafisch dar. Von den befragten 222 KMUs setzen aktuell 216 KMUs Cloud-Services in verschiedenen Ausprägungen ein. Das bedeutet, dass 97 Prozent der befragen KMUs nach Inkrafttreten der DSGVO Cloud-Services im Einsatz haben. Vor Inkrafttreten der DSGVO konnten 212 Unternehmen mit Cloud-Services identifiziert werden.

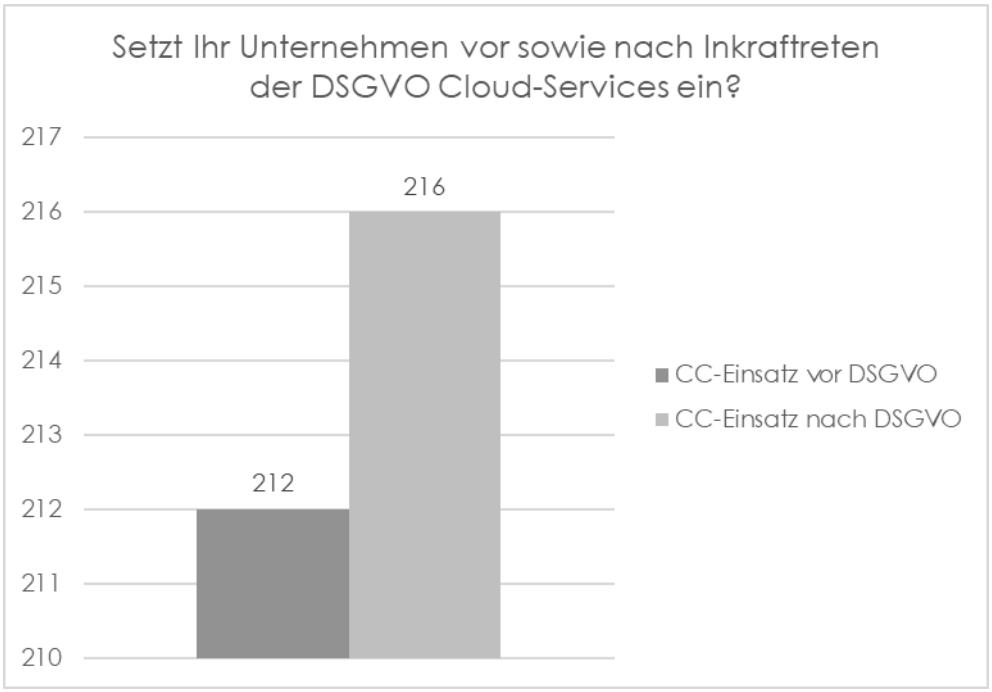


Abbildung 14 - Cloud-Service-Einsatz

Diese Steigerung von Cloud-Services spielgelt sich in einer Statistik der „Statistik Austria“ wieder. Diese Statistik konnte ein Anstieg von Cloud-Services bei KMUs aufzeichnen. Somit konnte von 2014 auf 2018 ein Anstieg von acht Prozent gemessen werden. Diese Statistik beweist, dass der Anstieg von Cloud-Services durch die DSGVO nicht gebremst wurde. [DH18]

Des Weiteren wurden die Probanden befragt, welche Cloud-Service-Modelle die Unternehmen im Einsatz haben. Die Abbildung 15 stellt die eingesetzten Cloud-Service-Modelle in einem Diagramm dar. Die Ergebnisse beziehen sich auf die 216 KMUs und wurden zur besseren Übersichtlichkeit nach der Häufigkeit sortiert. SaaS-Modelle werden mit Abstand am häufigsten bei KMUs eingesetzt. 121 befragte KMUs setzen aktuell SaaS-Lösungen ein. Das bedeutet, dass 56 Prozent aller befragten KMUs SaaS-Modelle nutzen. Die Nutzung von IaaS- und PaaS-Modellen beschränkt sich mit einer Nutzung von 87 sowie 84 hingegen nur auf 40 sowie 39 Prozent. Jedes der 216 Unternehmen musste zumindest eines der definierten Cloud-Service-Modelle auswählen, da es sich bei dieser Frage um

eine Pflichtfrage handelte. Eine Mehrfachauswahl an Antworten war bei dieser Frage zulässig. Somit konnten die Probanden auch mehrere Cloud-Service-Modelle auswählen. Diese und nachfolgende Antworten beziehen sich auf den Zeitraum nach Inkrafttreten der DSGVO.

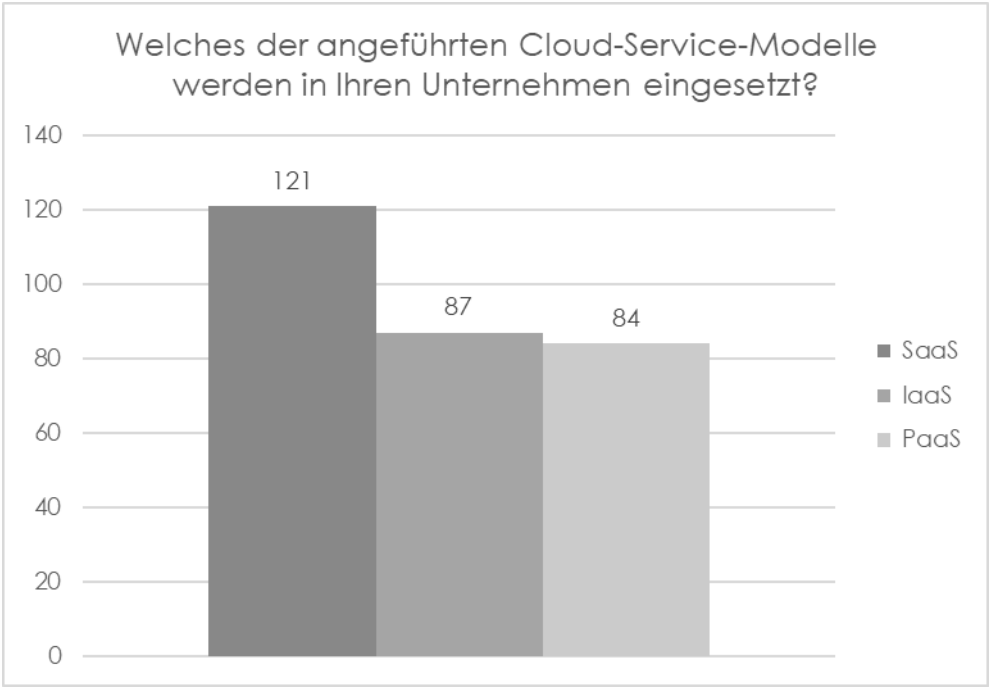


Abbildung 15 - Cloud-Service-Modelle

Des Weiteren konnte durch die Untersuchung der Cloud-Service-Modelle festgestellt werden, dass 139 Unternehmen ein Cloud-Service-Modell einsetzt. 50 Unternehmen setzen parallel auf zwei Cloud-Service-Modelle und 27 Unternehmen setzen parallel auf alle drei beschriebenen Cloud-Service-Modelle.

Die nächste Frage der Rubrik „Cloud-Computing" analysiert die Cloud-Service-Provider. Zwölf Cloud-Service-Provider standen den Probanden zur Auswahl. Die Abbildung 16 stellt die drei häufigsten CSP grafisch dar. Das Ergebnis zeigt, dass 159 der befragte KMUs Microsoft Azure einsetzen. Mit 123 Abstimmungsergebnissen liegt Google auf Platz zwei der häufigsten CSP. Des Weiteren konnte Amazon Web Services mit 114 Stimmen Platz drei erreichen. Das bedeutet, dass 73 Prozent der befragten KMUs Microsoft Azure als CSP

bevorzugen. Jedes Unternehmen musste mindestens einen CSP auswählen. Eine Mehrfachauswahl der Antworten war bei dieser Frage möglich. Die gewonnenen Ergebnisse dieser Frage wiederspiegeln die theoretischen Erkenntnisse aus dem Kapitel 2.1.6 (Top-3 Cloud-Service-Provider).

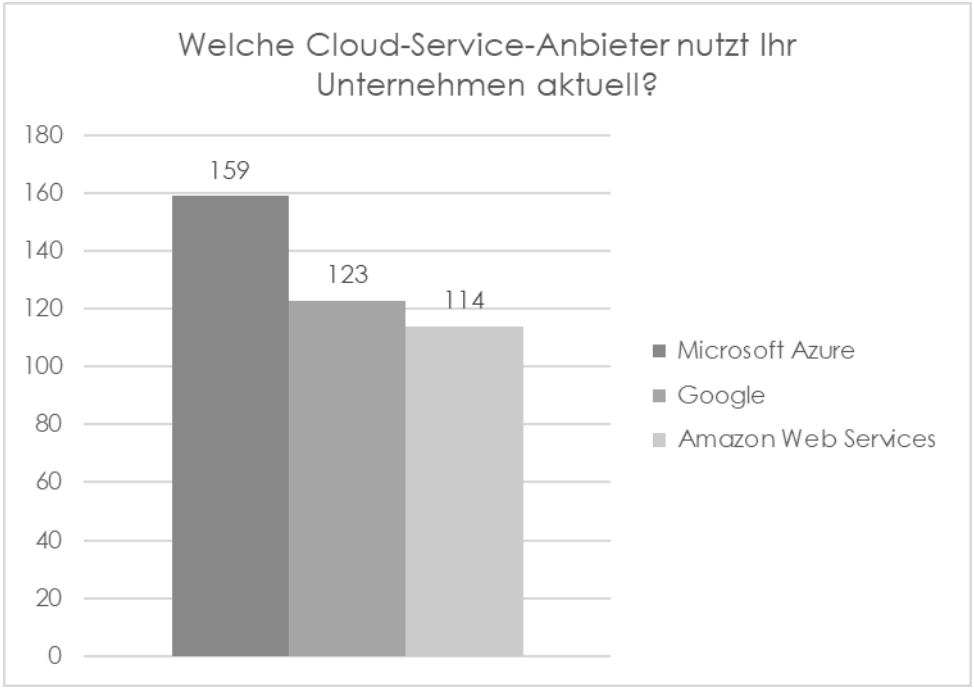


Abbildung 16 - Cloud-Service-Provider

Als nächstes wurden die größten Treiber von Cloud-Services untersucht. Durch diese Frage sollen die größten Treiber von Cloud-Services identifiziert werden. Die Untersuchungsergebnisse wurden in der Abbildung 17 grafisch dargestellt. Die Ergebnisse zeigen, dass 152 der befragten KMUs die Erhöhung der Sicherheit als größten Treiber für die Nutzung von Cloud-Services ansehen. Des Weiteren haben 145 KMUs die Kostenreduktion als zweitwichtigsten Treiber ausgewählt. 99 KMUs sehen den ausgelagerten Service und Support als wichtiges Kriterium an. Die drei wichtigsten Cloud-Service-Treiber spiegeln die Outsourcing-Gedanken wieder. Nur 91 befragte KMUs sehen Cloud-Services als Innovationsbeschleuniger. Die Erhöhung der Flexibilität findet nur noch bei 70 KMUs Zuspruch. Eine Mehrfachauswahl der Antwortmöglichkeiten war gegeben.

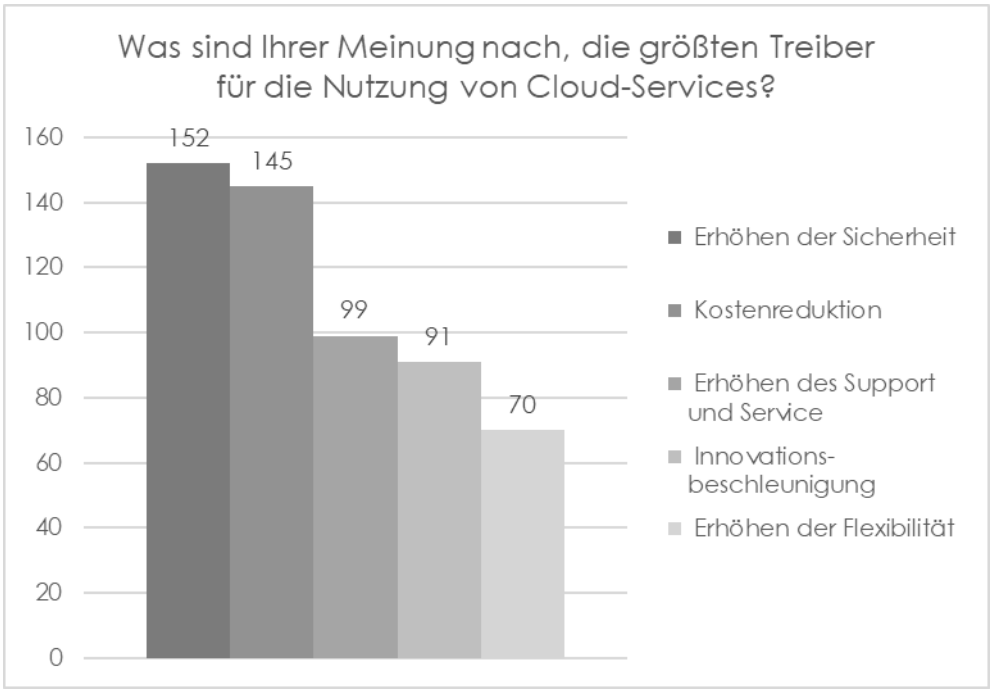


Abbildung 17 - Cloud-Service-Treiber

Die Abbildung 18 erläutert das Ergebnis der Frage neun: „Was sind Ihrer Meinung nach die größten Herausforderungen bei der Nutzung von Cloud-Services?“. Auch bei dieser Frage konnten mehrere Antworten ausgewählt werden. Das Ergebnis zeigt, dass die größte Herausforderung die Abhängigkeit zum CSP darstellt. Die Abhängigkeit zum CSP wurde bereits im Kapitelabschnitt 3.3.4 im Detail erläutert. Diese Abhängigkeit kann nur durch ein vorab definiertes Exit-Szenario reduziert werden. Die zweitwichtigste Herausforderung ist die Informationssicherheit. 94 der 216 befragten KMUs sehen die Informationssicherheit als eine große Herausforderung an. Wie und wo die Daten gespeichert werden sind wesentliche Aspekte. Diese Fragen müssen, wie bereits im Kapitelabschnitt 3.5.3.1 erläutert, in einer Cloud-Strategie definiert werden. Die Kosteneffizienz wählten 83 der 216 Unternehmen als drittwichtigste Herausforderung. Um die Kosteneffizienz zu erreichen, müssen Prozesse schon vor der Auslagerung effizient und standardisiert gestaltet werden. Die rechtlichen Rahmenbedingungen wurden nur von 70 der 216 befragten KMUs identifiziert. Bei dieser Frage waren mehrere Antworten erlaubt.

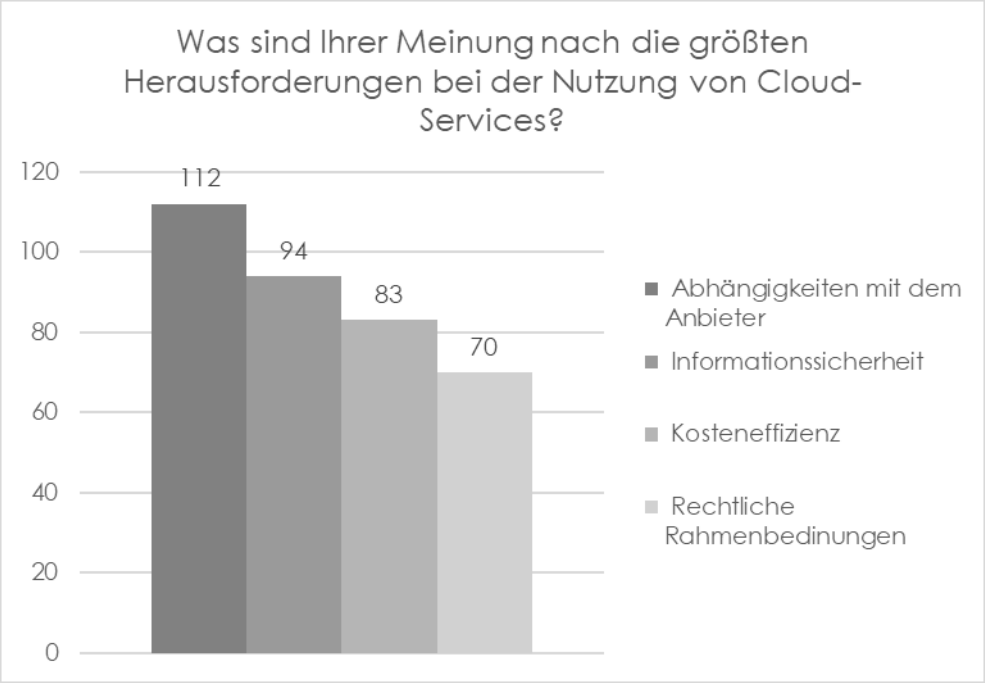


Abbildung 18 - Cloud-Service-Herausforderungen

Die nächste Abbildung 19 stellt die Forschungsergebnisse der wichtigsten Cloud-Service-Kriterien dar. 183 KMUs wählen „Datenschutz“ als wichtiges Auswahlkriterium für Cloud-Services. Des Weiteren wählten 163 KMUs den Punkt „Sicherheit“ als ein weiteres wichtiges Kriterium bei der Auswahl von Cloud-Services. Die Wahl dieser zwei Kriterien zeigt wiederum, dass Cloud-Compliance ein essenzielles Thema bei der Einführung sowie beim Betrieb von Cloud-Services darstellt. Das Thema „Kosten“ ist für 144 KMUs ein weiteres wichtiges Auswahlkriterium für Cloud-Service. Die Kriterien „Funktionalität“ der Cloud-Services, „Cloud-Service-Provider“ sowie „Usability“ der Cloud-Services wurden von den Probanden auf den Plätzen vier, fünf und sechs eingeordnet. Die Probanden konnten mehrere Antwortmöglichkeiten auswählen.

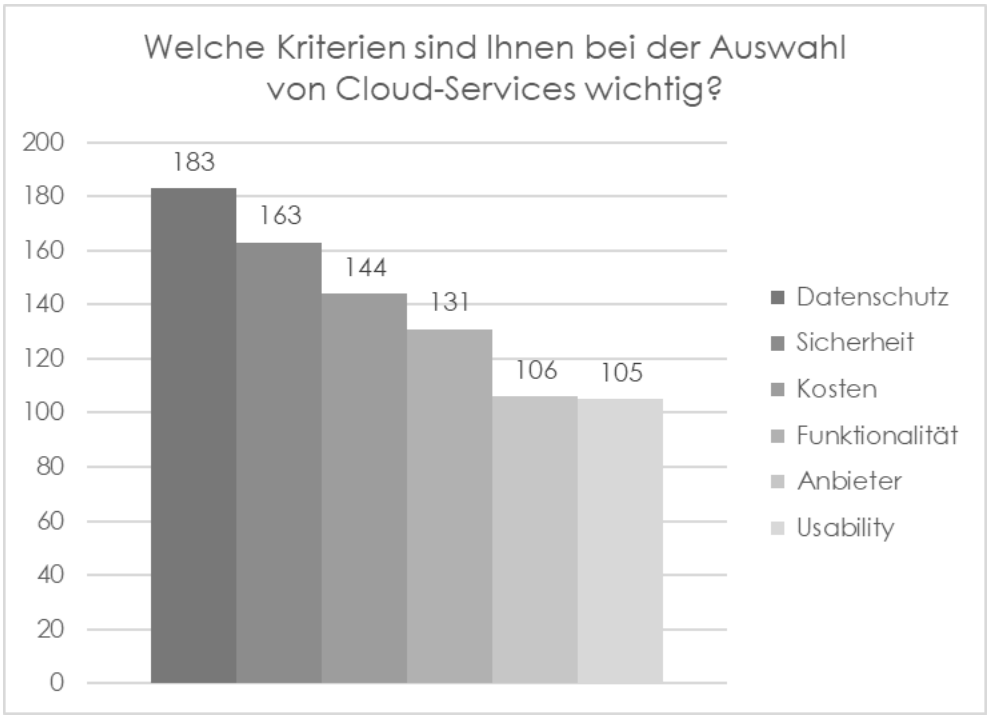


Abbildung 19 - Cloud-Service-Kriterien

Die Cloud-Strategie ist, wie im Kapitel 3.5.3.1 erläutert, essenziell für die Einführung und den Betrieb von Cloud-Services. Aus diesem Grund wurden die untersuchten Unternehmen über ihre Cloud-Strategie sowie über das Verhalten der Strategie im Zusammenhang mit der DSGVO befragt. In der Abbildung 20 wurden die Untersuchungsergebnisse zum Thema Cloud-Strategie grafisch dargestellt. Vor Inkrafttreten der DSGVO verfolgten 166 der 216 befragten KMUs eine Cloud-Strategie. Nach Inkrafttreten der DSGVO stieg der Wert auf 187 KMUs an. Dieses Ergebnis zeigt, dass nach Inkrafttreten der DSGVO Unternehmen vermehrt auf eine Cloud-Strategie setzten. Wie in Abbildung 17, Abbildung 18 und Abbildung 19 ersichtlich, legen die befragten Unternehmen ein großes Augenmerk auf die Informationssicherheit und auf den Datenschutz im Bereich Cloud-Service. Folgend kann daraus geschlossen werden, dass die DSGVO Einfluss auf die Cloud-Strategie von KMUs nimmt. Die Ergebnisse zeigen, dass es nach Inkrafttreten der DSGVO (nach 25.05.2018) in diesem Bereich zu einer dreizehnprozentige Steigerung kam.

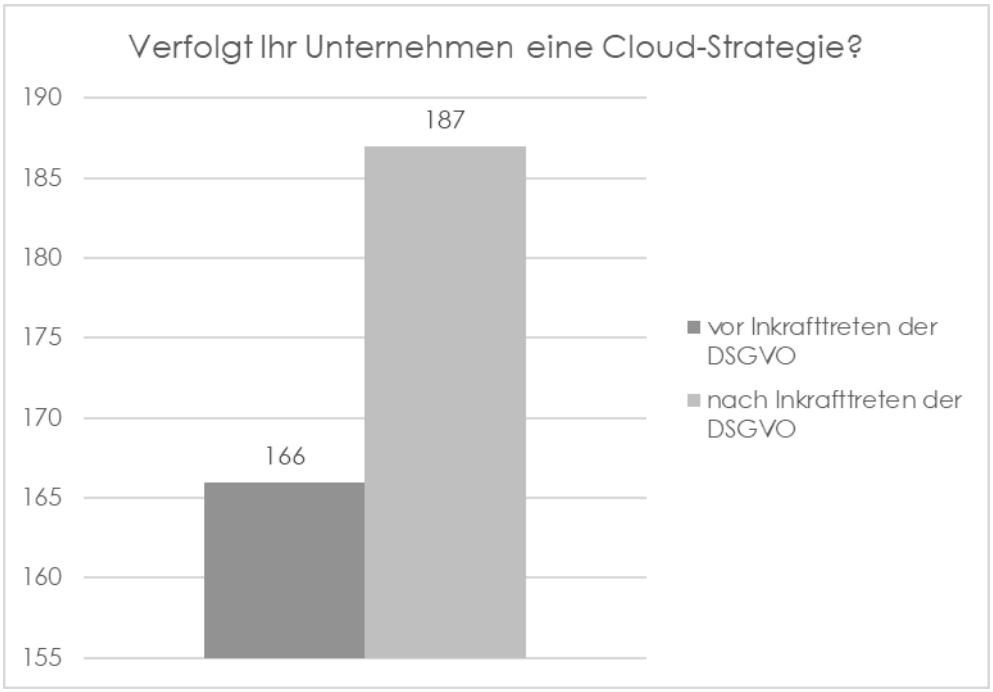


Abbildung 20 - Cloud-Strategie

Der nächste Kapitelabschnitt erläutert die Ergebnisse der dritten Rubrik „Datenschutz-Grundverordnung".

4.3.3 Datenschutz-Grundverordnung

Dieser Kapitelabschnitt erläutert die Forschungsergebnisse der Rubrik „Datenschutz-Grundverordnung". Die DSGVO ist die dritte Rubrik des Onlinefragenbogens. Die Probanden wurden aufgefordert, Fragen über die Ziele der DSGVO, über die Priorisierung der DSGVO-Themen im Unternehmen sowie der operativen DSGVO-Themen zu beantworten. Die Forschungsergebnisse werden in diesem Kapitelabschnitt erläutert sowie grafisch dargestellt.

Die erste Frage der dritten Rubrik stellte die Ziele der DSGVO in den Vordergrund. 74 Prozent der befragten Probanden sind die Ziele der DSGVO bekannt. Lediglich 26 Prozent der Befragten haben angegeben, dass ihnen die Ziele der DSGVO nicht bekannt sind. Die Abbildung 21 stellt das Forschungsergebnis grafisch dar.

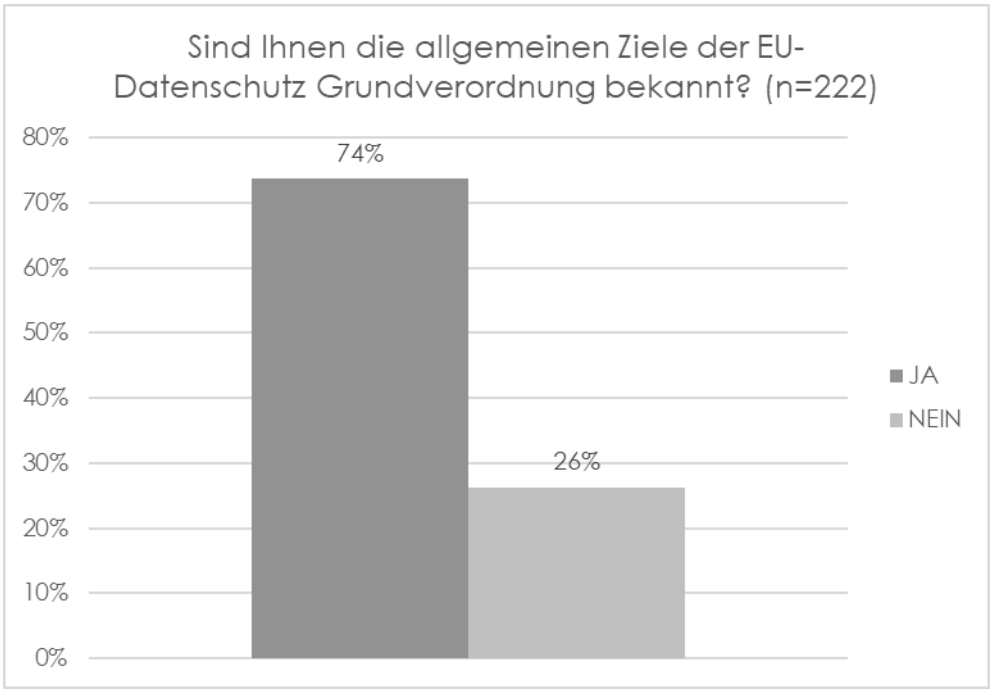


Abbildung 21 - Ziele der DSGVO

Die nächsten zwei Fragen beschäftigen sich mit der Wichtigkeit des Datenschutzes im Unternehmen sowie der Priorisierung der gesetzlichen Einhaltungen der DSGVO im Unternehmen. Datenschutz wird von 47 Prozent der befragen KMUs als „eher wichtig" bis „sehr wichtig" eingestuft. 21 Prozent der befragten KMUs sehen die Wichtigkeit zum Datenschutz als „neutral" an. Lediglich 32 Prozent der untersuchten KMUs sehen die Wichtigkeit des Datenschutzes als „eher unwichtig" bis „sehr unwichtig" an. Dies geht aus den dargestellten Ergebnissen der Abbildung 22 hervor.

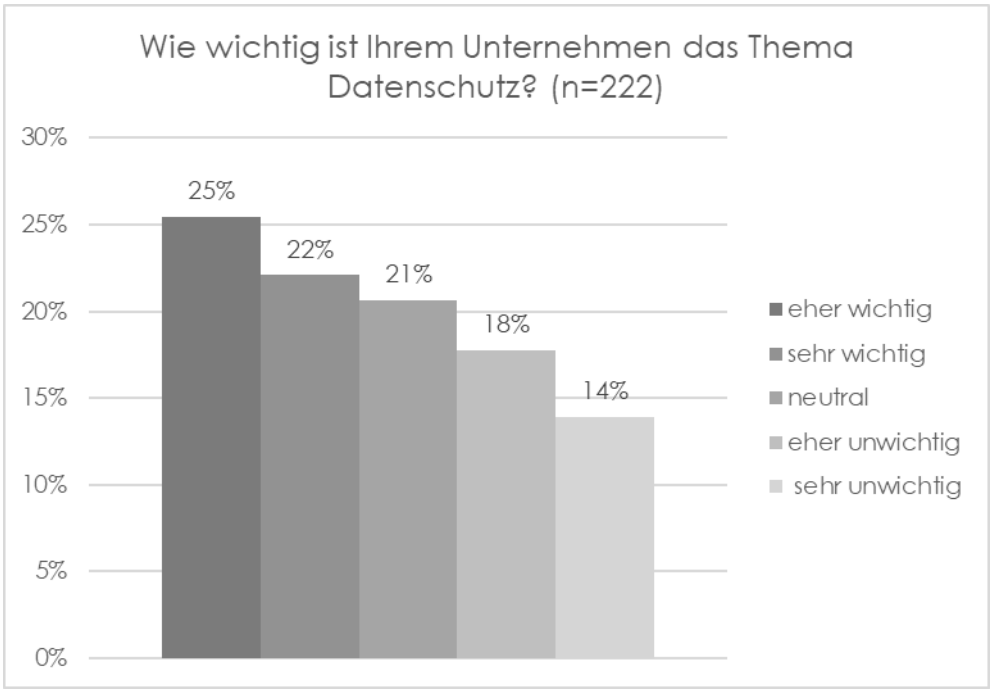


Abbildung 22 - Wichtigkeit DSGVO

Die Priorisierung der gesetzlichen Einhaltung wird im nächsten Forschungsergebnis dargestellt. Das Forschungsergebnis wird in der Abbildung 23 grafisch abgebildet. Die Priorisierung der gesetzlichen Einhaltung wird im Gegensatz zur Wichtigkeit der DSGVO von 51 Prozent der untersuchten KMUs als „eher wichtig“ bis „sehr wichtig“ angesehen. Diese Untersuchungsergebnisse zeigen, dass das Thema Datenschutz von den KMUs als „eher wichtig“ bis „sehr wichtig“ angesehen wird, aber das die Einhaltung der gesetzlichen Anforderungen nicht zwingend mit hoher Priorität verfolgt wird.

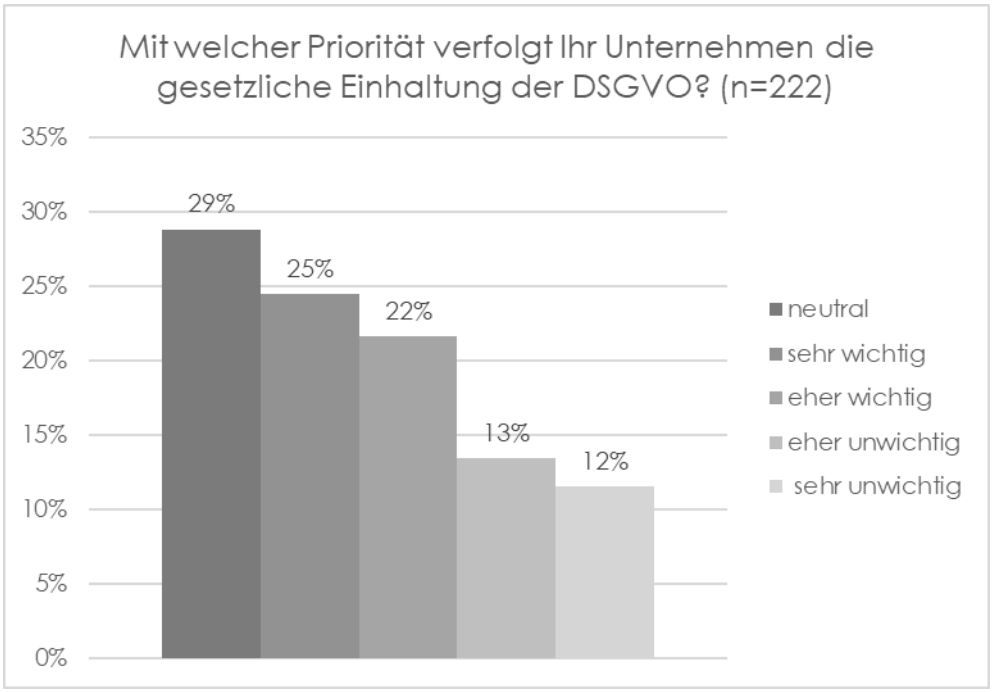


Abbildung 23 - Priorisierung gesetzlicher Anforderungen

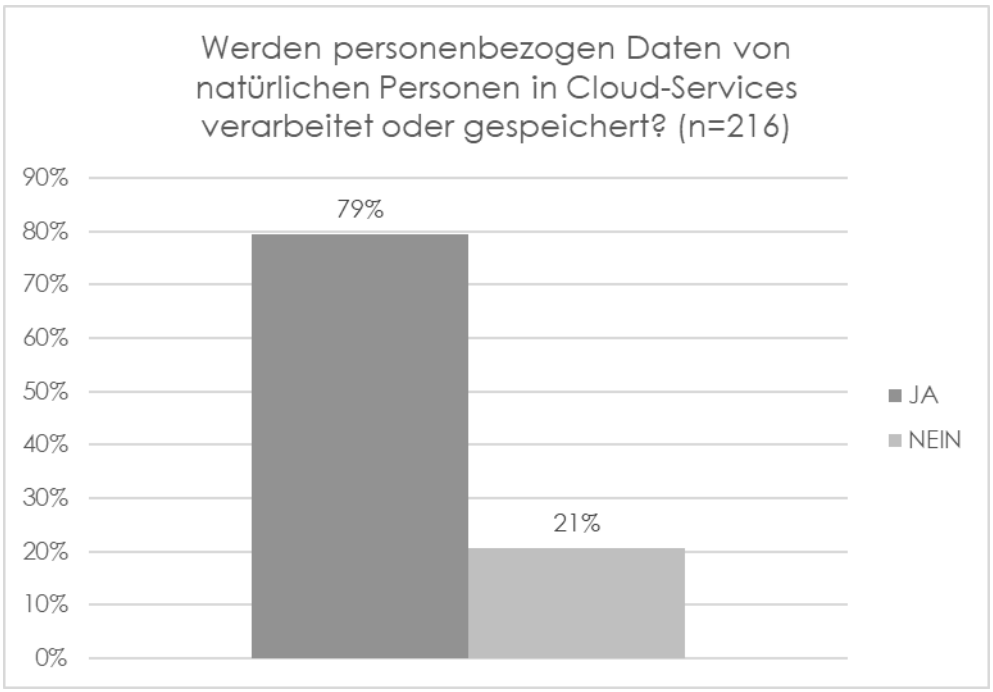


Abbildung 24 - Verarbeitung von personenbezogenen Daten

Die nächste Frage im Bereich DSGVO untersucht, wie viele der befragten Unternehmen personenbezogene Daten in Cloud-Services verarbeiten oder speichern. Von den 216 befragten KMUs verarbeiten oder speichern rund 79 Prozent (171 KMUs) der KMUs personenbezogene Daten in Cloud-Services. Dieses Ergebnis wird in Abbildung 24 grafisch dargestellt. Diese 171 KMUs müssen, wie bereits im Kapitelabschnitt 2.2 beschrieben, die gesetzlichen Vorgaben der Datenschutz-Grundverordnung bei der Speicherung sowie der Verarbeitung von personenbezogenen Daten natürlicher Personen einhalten.

Die Forschungsergebnisse zur Frage „Haben die Mitarbeiter in Ihren Unternehmen eine Schulung erhalten?“, können nur knapp die Hälfte – rund 52 Prozent - der befragten KMUs die personenbezogene Daten verarbeiten oder speichern, mit Ja beantworten. Die Abbildung 25 stellt das Ergebnis in einem Diagramm grafisch dar.

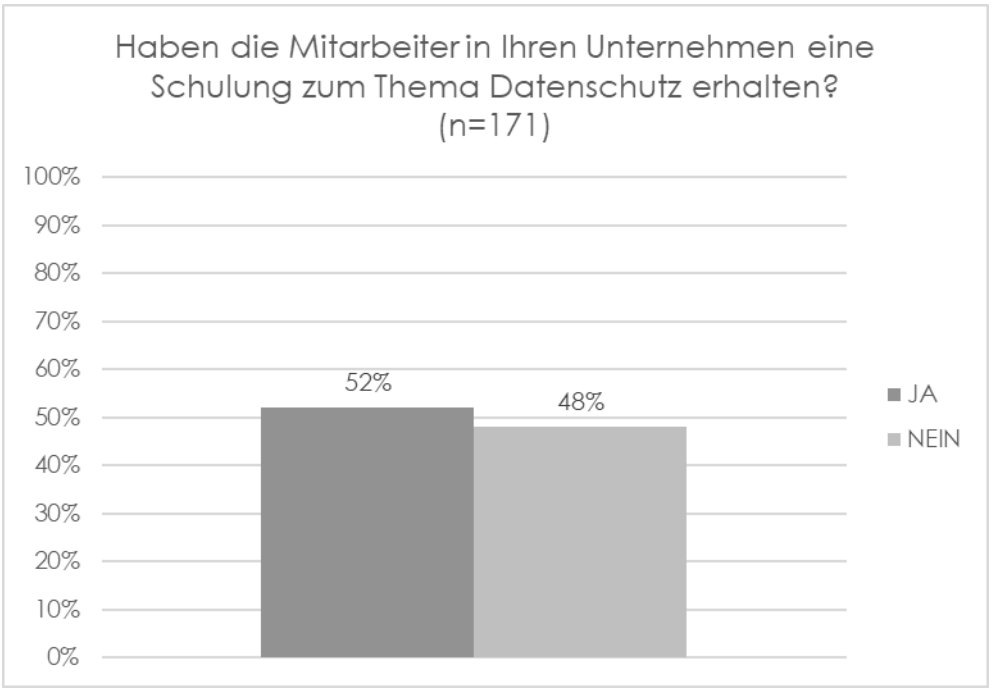


Abbildung 25 - Datenschutzschulung

Des Weiteren verfügen weniger als die Hälfte – rund 47 Prozent – der untersuchten KMUs über einen eigenen Datenschutzbeauftragten. Diese Interpretation geht aus der Abbildung 26 hervor.

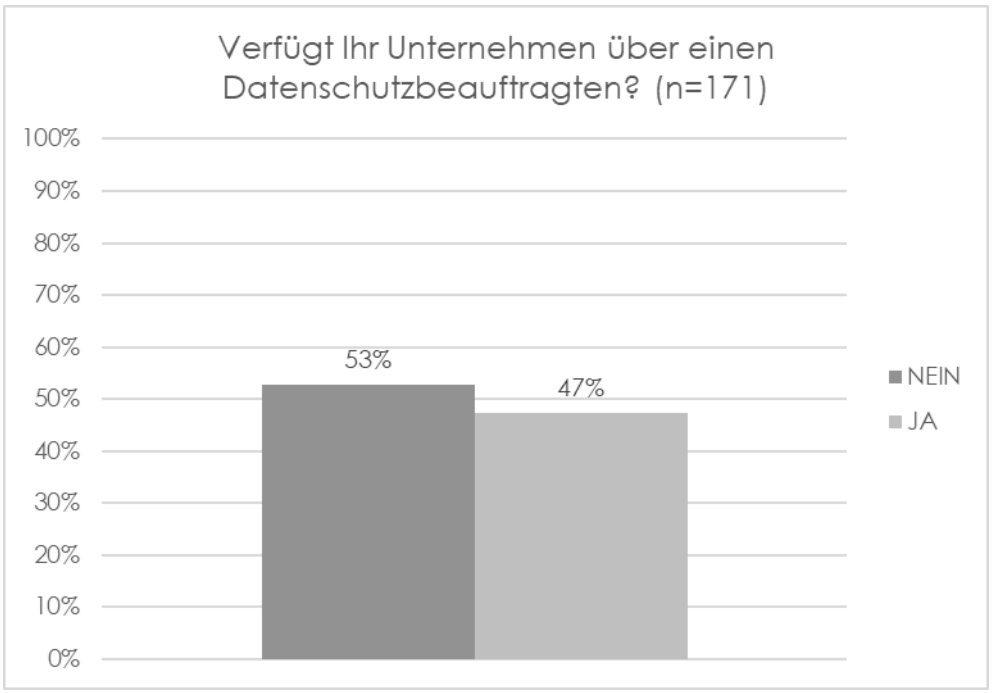


Abbildung 26 - Datenschutzbeauftragten

Die nachfolgenden zwei Forschungsergebnisse behandeln die Auftragsverarbeiterverträge (kurz AVV) mit den CSP sowie die TOMs der CSP. Das Ergebnis dieser nachfolgenden Abbildung 27 zeigt, dass 51 Prozent der befragten KMUs einen AVV mit ihren CSP abgeschlossen haben. In der Abbildung 28 ist ersichtlich, wie viele der befragten KMUs die technischen und organisatorischen Maßnahmen ihrer CSP besitzen. Nur 46 Prozent der befragten Unternehmen haben die TOMs der CSP übermittelt bekommen.

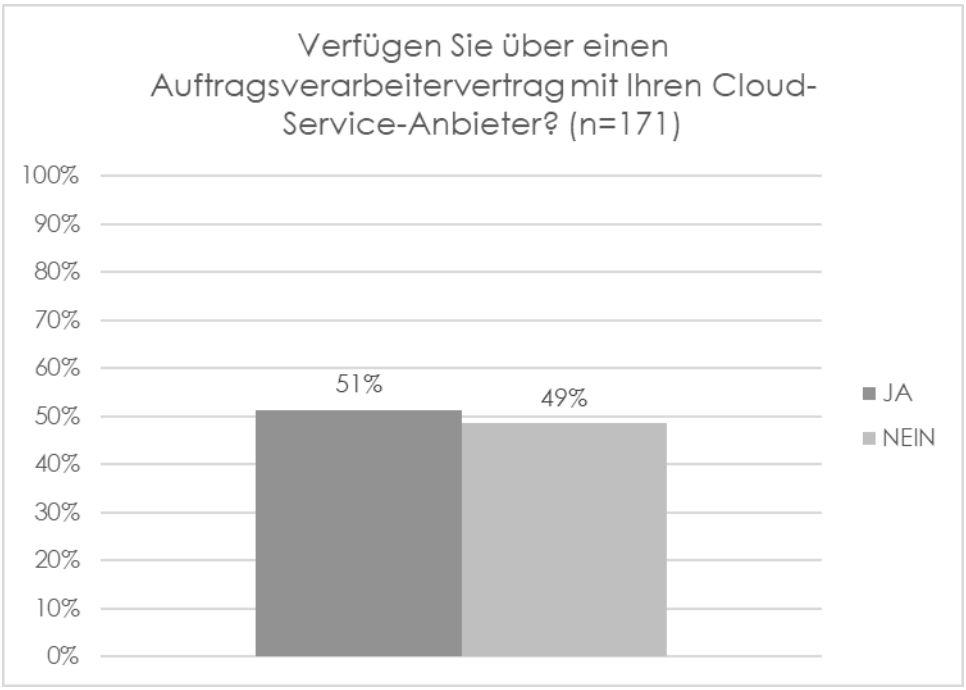


Abbildung 27 – Auftragsverarbeitervertrag

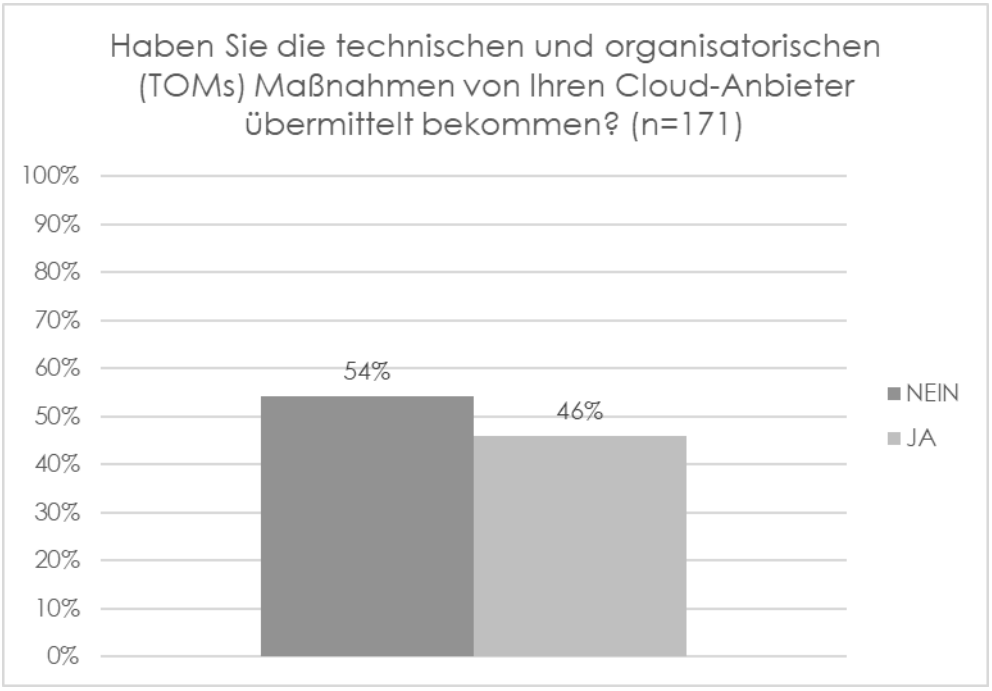


Abbildung 28 – TOMs

Das bedeutet, dass die gesetzlichen Anforderungen gemäß DSGVO nur von knapp der Hälfte der befragten KMUs eingehalten werden. Nur 52 Prozent der untersuchten KMUs haben ihre Mitarbeiter zum Thema Datenschutz geschult beziehungsweise sensibilisiert. Des Weiteren können nur 47 Prozent der KMUs einen Datenschutzbeauftragten aufweisen. Von den 171 untersuchten KMUs, die personenbezogene Daten in Cloud-Services speichern oder verarbeiten, haben lediglich 51 Prozent einen AVV mit dem CSP. Abschließend ist noch hervorzuheben, dass lediglich 46 Prozent der untersuchten KMUs die TOMs des CSP übermittelt bekommen haben.

Der nächste Kapitelabschnitt erläutert die Forschungsergebnisse der vierten und letzten Rubrik „Nutzungsverhalten". Das Nutzungsverhalten der KMUs ist in Bezug auf Cloud-Services und der DSGVO essenziell für die Beantwortung der Forschungsfrage.

4.3.4 Nutzungsverhalten

Das Nutzungsverhalten der untersuchten KMUs wird unter Berücksichtigung der DSGVO in diesem Kapitelabschnitt erläutert und grafisch dargestellt. Der Fokus wird dabei auf die Veränderung der Cloud-Service-Nutzung gelegt. Des Weiteren wird untersucht, warum sich die Cloud-Service-Nutzung verändert hat.

Die erste Frage der Rubrik „Nutzungsverhalten" untersucht, ob sich die Nutzung der Cloud-Services nach Inkrafttreten der DSGVO verändert hat. Die Ergebnisse dieser Forschung werden in der Abbildung 29 grafisch dargestellt. Das Ergebnis zeigt, dass sich die Cloud-Service-Nutzung bei 84 Prozent (181 KMUs) der befragten KMUs verändert hat. Des Weiteren konnte bei 16 Prozent (35 KMUs) der befragten KMUs keine Veränderung der Cloud-Service-Nutzung festgestellt werden. Wie sich die Cloud-Service-Nutzung verändert hat, wird mit der nächsten Frage untersucht.

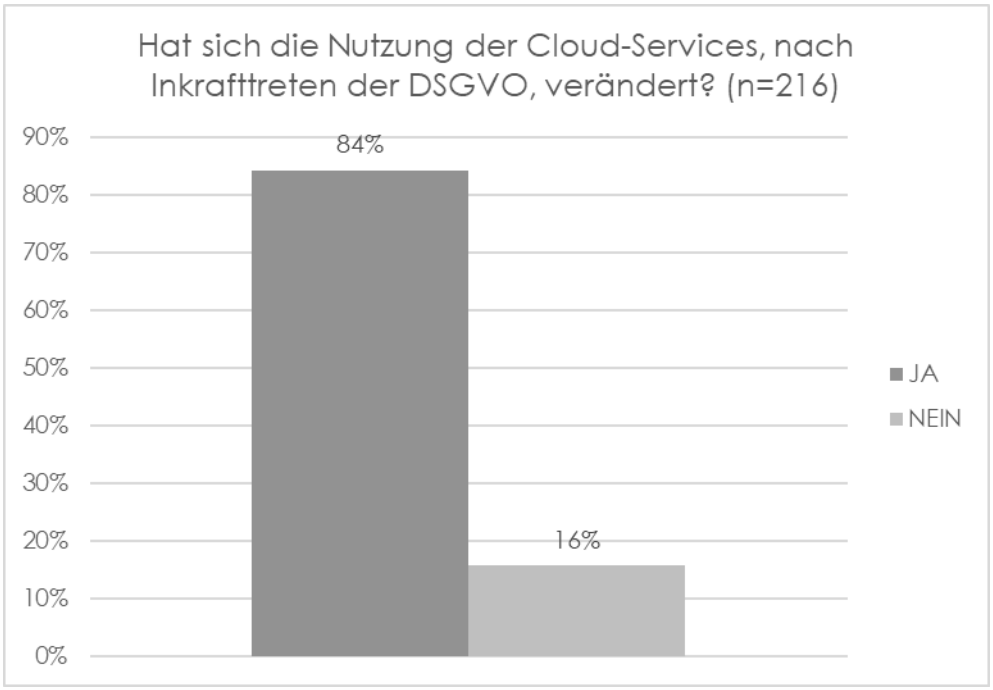


Abbildung 29 - Veränderung der Cloud-Service-Nutzung

Die zweite Frage in der Rubrik „Nutzungsverhalten“ untersucht, wie sich die Cloud-Service-Nutzung bei den 84 Prozent (181 KMUs) der identifizierten KMUs verändert hat. Die Abbildung 30 stellt die veränderte Nutzung grafisch dar. Aus dieser Abbildung geht hervor, dass bei 75 Prozent der identifizierten KMUs die Cloud-Service-Nutzung nach Inkrafttreten der DSGVO gestiegen ist. Lediglich 25 Prozent der untersuchten KMUs geben an, dass die Cloud-Service-Nutzung gesunken ist.

In Zahlen ausgedrückt bedeutet dieses Ergebnis, dass die Cloud-Service-Nutzung nach Inkrafttreten der DSGVO bei 136 der befragten KMUs gestiegen ist. Des Weiteren haben 45 der untersuchten KMUs nach Inkrafttreten der DSGVO ihre Cloud-Service-Nutzung verringert. Die Gründe für die gestiegene sowie die gesunkene Cloud-Service-Nutzung, werden in den Abbildung 31 und Abbildung 32 dargestellt.

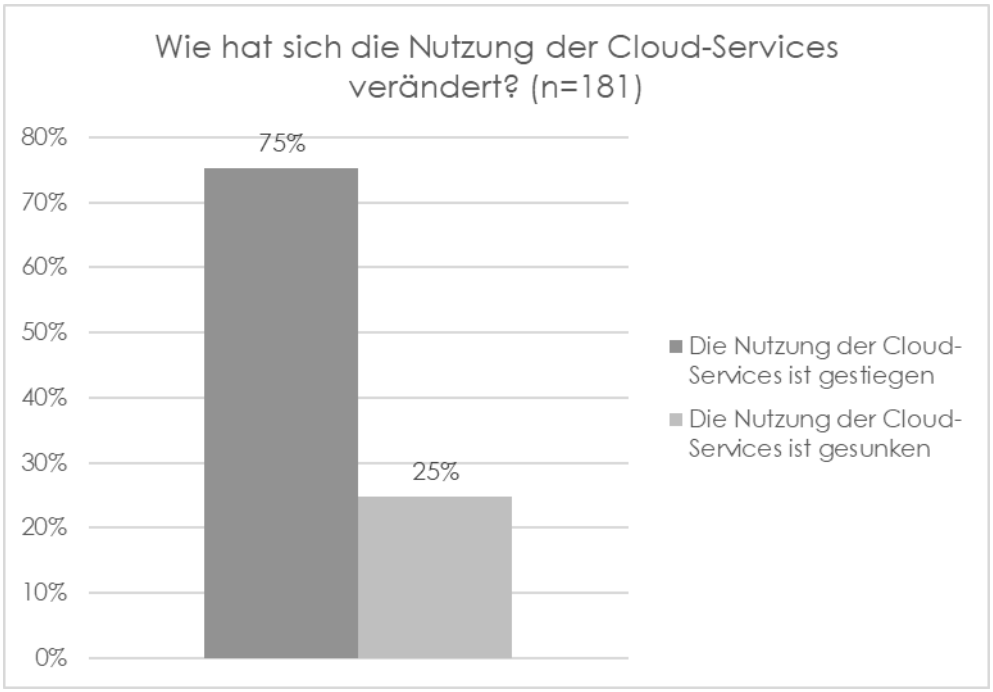


Abbildung 30 - Cloud-Service-Nutzungsveränderung

Die Abbildung 31 stellt die Gründe für die Verringerung der Cloud-Service-Nutzung grafisch dar. Von den 45 untersuchten KMUs, die ihre Cloud-Service-Nutzung verringert haben, gehen folgende Ergebnisse hervor: 43 der 45 untersuchten Unternehmen verringerten die Cloud-Service-Nutzung, weil der CSP das Service nicht DSGVO-konform bereitstellen konnte. Das bedeutet, dass der CSP die technischen und organisatorischen Maßnahmen gemäß Artikel 32 der DSGVO nicht erfüllen konnte. Des Weiteren haben 24 KMUs die unklaren rechtlichen Aspekte als Grund der Nutzungsverringerung angegeben. Das erhöhte Haftungsrisiko wählten 17 KMUs für die Verringerung der Cloud-Service-Nutzung. Des Weiteren gaben neun KMUs an, dass sie die notwendigen TOMs nicht umsetzen konnten. Die Datensicherheit ist mit nur einer Stimme als vernachlässigbar anzusehen. Eine Mehrfachauswahl der Antwortmöglichkeiten war erlaubt.

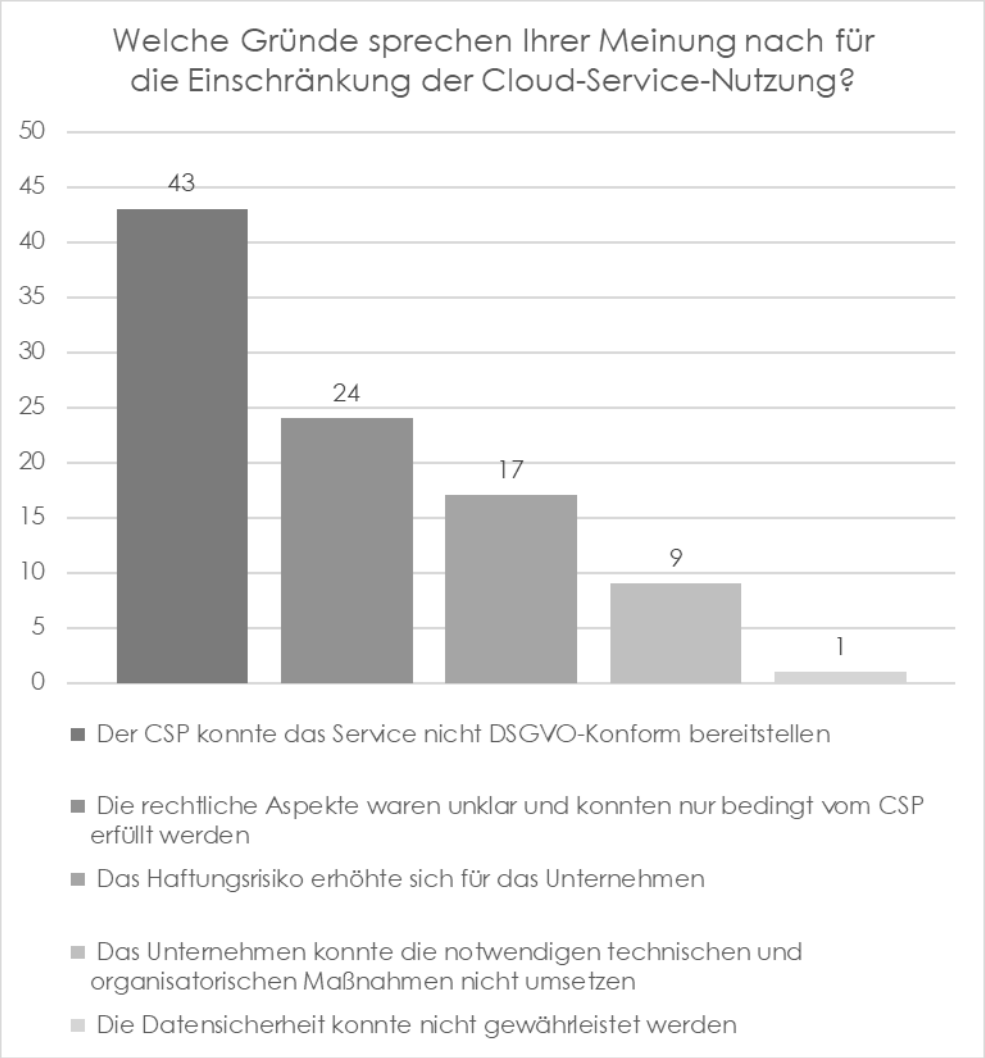


Abbildung 31 - Gründe für die Einschränkung der Cloud-Services

Die Abbildung 32 beschreibt die Gründe für eine gestiegene Cloud-Service-Nutzung bei den ausgewählten 136 KMUs. 116 der 136 KMUs steigerten ihre Cloud-Service-Nutzung, da der CSP das Service DSGVO-konform zur Verfügung stellen konnte. Des Weiteren haben 86 der 136 KMUs die Erhöhung der Datensicherheit als ausschlaggebendes Argument für die Steigerung der Nutzung gewählt. Das bedeutet, dass 63 Prozent der zutreffenden Unternehmen die Datensicherheit an den CSP auslagern beziehungsweise ihn schon ausgelagert haben. 66 KMUs bestätigen, dass sie die notwendigen TOMs erfüllen und somit die Nutzung der Cloud-Services steigern konnten. Um das

Haftungsrisiko für das Unternehmen zu verringern, haben 56 KMUs die Cloud-Service-Nutzung gesteigert. Lediglich 26 der 136 KMUs beziehen sich auf klare rechtliche Aspekte für die gestiegene Cloud-Service-Nutzung.

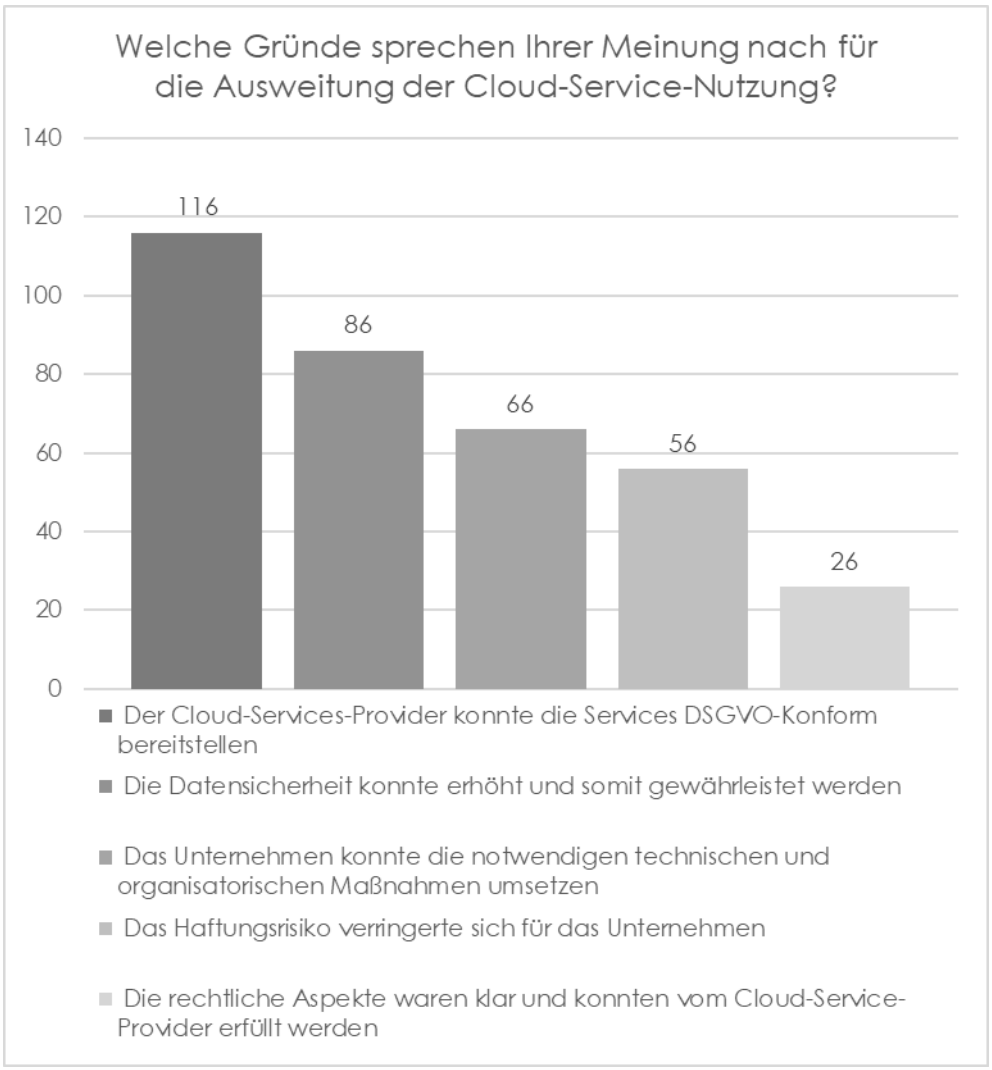


Abbildung 32 - Gründe für die Erweiterung der Cloud-Services

Die letzte Frage der Rubrik „Nutzungsverhalten" sowie des Onlinefragebogens untersucht die zukünftige Nutzung von Cloud-Services. Die Probanden wurden über die zukünftige Cloud-Service-Nutzung befragt. Dabei haben 87 Prozent der untersuchten KMUs angegeben, dass sie auch in Zukunft Cloud-Services nutzen werden. Lediglich 13 Prozent der befragten KMUs schließen eine zukünftige

Cloud-Service-Nutzung aus. Die Ergebnisse wurden in der Abbildung 33 grafisch dargestellt.

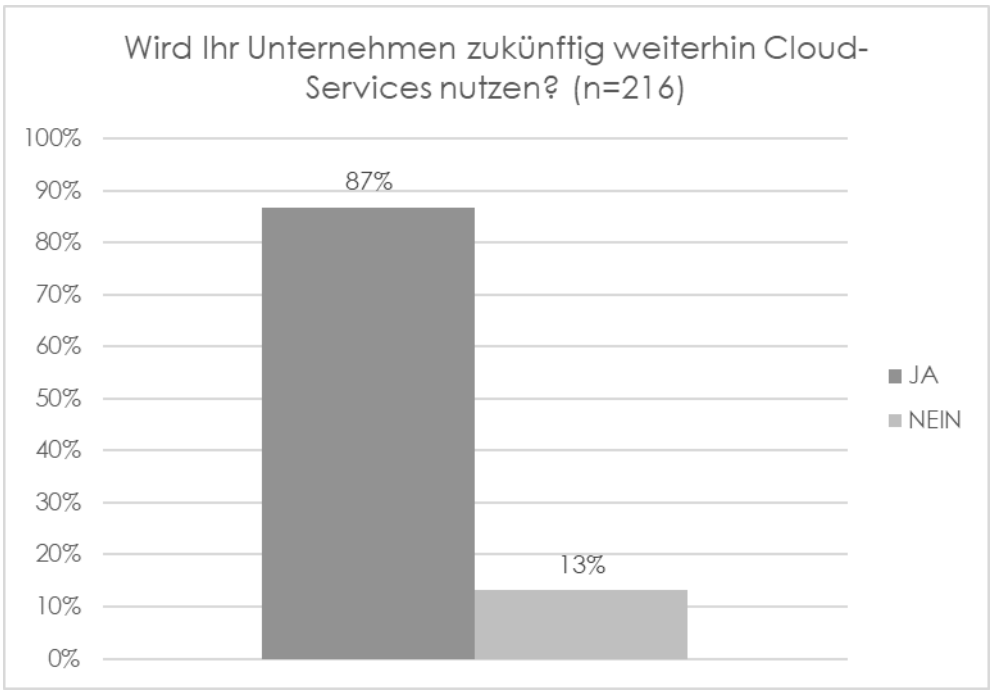


Abbildung 33 - Zukünftige Nutzung von Cloud-Services

Durch die korrelierten Daten konnten noch weitere Erkenntnisse identifiziert werden. Wenn man die Branchen betrachten, die in Zukunft weiterhin auf Cloud-Services setzen, dann kann man einen durchschnittlichen Rückgang von Cloud-Services pro Branche um einen Prozentpunkt betrachten. Bei genauerer Betrachtung stellt man fest, dass sich die Cloud-Service-Nutzung in der Branche „Gesundheit und Soziales“ um 50 Prozent reduziert hat. Diese Reduktion kann durch nicht DSGVO-konforme Services dargestellt werden. Diese Betrachtung wird in der Abbildung 34 grafisch dargestellt.

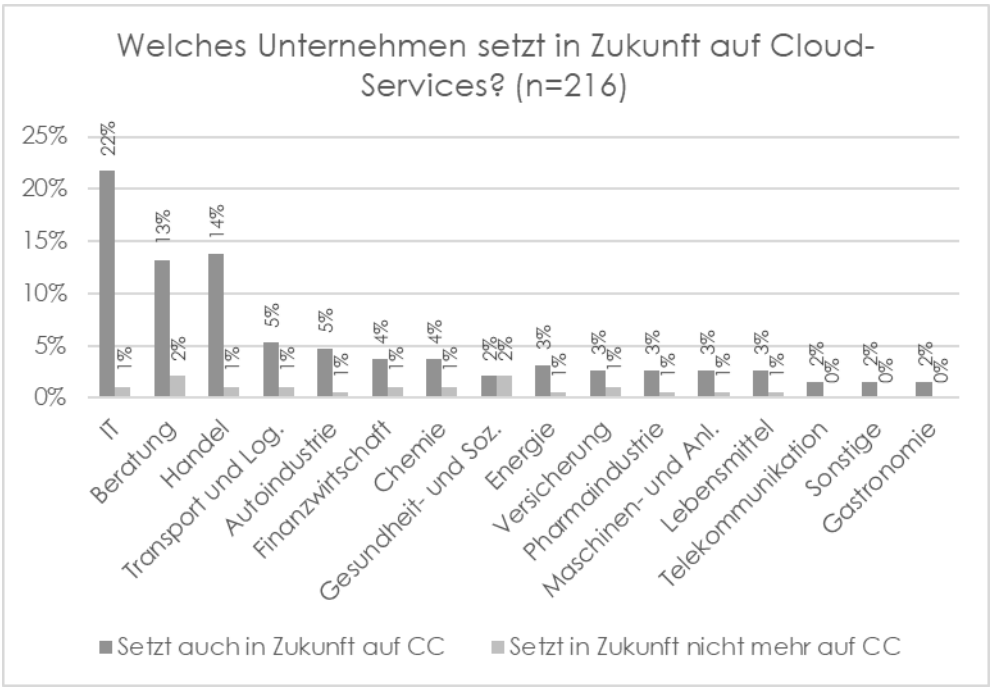


Abbildung 34 - Zukünftige CC-Nutzung pro Branche

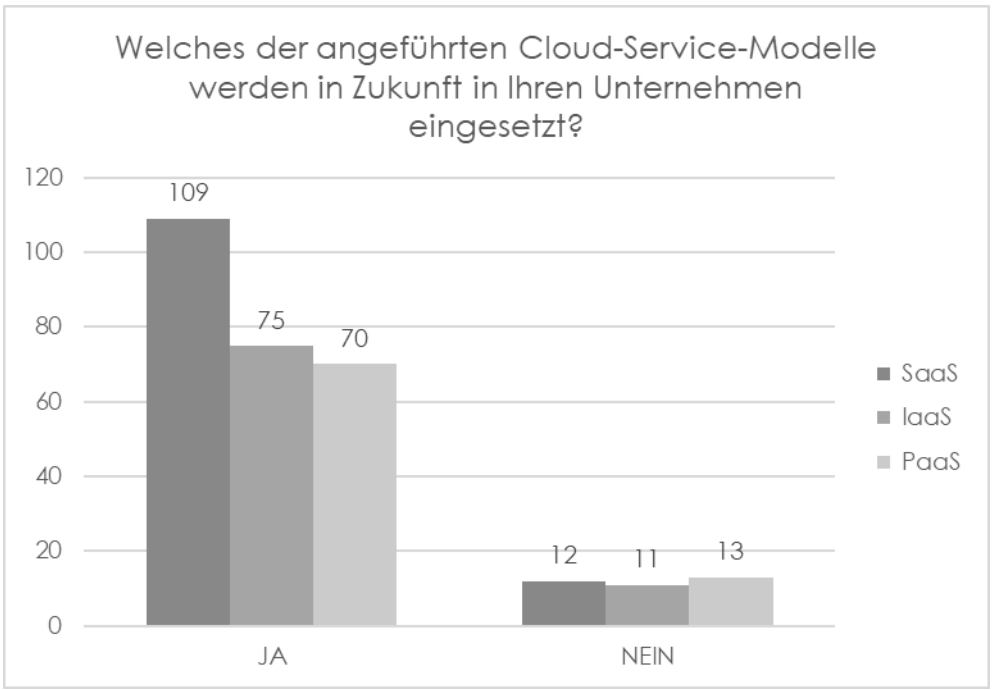


Abbildung 35 - Zukünftige Cloud-Service-Modelle

Des Weiteren konnte durch die Korrelation der Forschungsergebnisse der Trend der Cloud-Service-Modelle dargestellt werden. Bei allen drei beschriebenen Cloud-Service-Modellen gab einen zweistelligen Rückgang. Wobei das Software-as-a-Service-Modell weiterhin das häufigste Cloud-Service-Modell darstellt. Die untersuchten KMUs setzten weiterhin verstärkt auf das Software-as-a-Service-Modell, um Applikationen und Software aus der Cloud zu beziehen. Dieser Verlauf wird in der Abbildung 35 dargestellt. Dieser Trend wird durch ein Whitepaper von „Cisco Systems“ verstärkt. Der Trend von SaaS-Modellen setzt sich, laut Cisco Systems, weiterhin fort. [Ci18]

4.4 Zusammenfassung

In diesem Kapitel wurde die empirische Studie im Detail erläutert. Dabei wurde der Fokus auf die Methodik der Befragung, auf den Aufbau des Onlinefragebogens sowie auf die Analyse und Interpretation der Forschungsergebnisse gelegt. Die Methodik beschrieb die Vorgehensweise der empirischen Forschung. Dabei wurden die einzelnen Schritte der Vorgehensweise beschrieben und erläutert. Des Weiteren wurde die Begründung einer quantitativen Befragung bestärkt und untermauert. Ein wesentlicher Teil dieses Kapitels beschäftigte sich mit der Erstellung und dem Aufbau des Onlinefragebogens. Der Onlinefragebogen wurde über eine externe Onlineplattform bereitgestellt und verfügte über vier Rubriken mit insgesamt 24 Fragen. Die Analyse und Interpretation der 24 Fragen wurde anhand von grafischen Darstellungen sowie Erläuterungen durchgeführt. Die wesentlichen Forschungsergebnisse für die Beantwortung der Forschungsfrage werden im nächsten Kapitel 5 im Detail erläutert.

5. FAZIT

Im fünften Kapitel werden die Erkenntnisse aus den vorherigen Kapiteln erläutert und zusammengefasst. Des Weiteren dient das Kapitel 5 zur Beantwortung der vorliegenden Forschungsfrage, die im Kapitelabschnitt 1.2 erläutert wurde. Zur Beantwortung der Forschungsfrage werden die untersuchten Forschungsergebnisse der empirischen Untersuchung sowie die vorhandene Literatur herangezogen.

5.1 Beantwortung der Forschungsfrage

Im Rahmen dieser Arbeit wurde eine Studie durchgeführt, die kleine und mittlere Unternehmen auf die Cloud-Service-Nutzung vor und nach Inkrafttreten der DSGVO untersuchte. Der Kapitelabschnitt 5.1 dient zur Beantwortung der Forschungsfrage. Die Forschungsfrage soll anhand der gewonnenen Forschungsergebnisse, die im Kapitelabschnitt 4.3 erläutert wurden, beantworten werden. Folgend werden die Ergebnisse erläutert, die für eine Steigerung der Cloud-Service-Nutzung sprechen.

Im Zuge dieser Arbeit wurden 312 Probanden befragt. Von diesen 312 Probanden waren 222 kleine und mittelständische Unternehmen. Diese 222 KMUs sind der definierten Zielgruppe zuzuordnen. Die untersuchten kleinen und mittelständischen Unternehmen haben nach Inkrafttreten der Datenschutz-Grundverordnung den Einsatz der Cloud-Services erhöht. Die Abbildung 14 stellt eine Steigerung von 1,9 Prozent grafisch dar. Das bedeutet, dass nach Inkrafttreten der DSGVO 216 KMUs Cloud-Services im Einsatz haben. Diese Steigerung kann durch den vorherrschenden Cloud-Computing-Trend dargestellt werden. Durch dieses Ergebnisse kann ein fortlaufender Trend, trotz des Inkrafttreten der DSGVO, bestätigt werden. [DH18]

Bei 84 Prozent dieser 216 untersuchten KMUs hat sich die Cloud-Service-Nutzung nach Inkrafttreten der DSGVO verändert. Diese Veränderung der Cloud-Service-Nutzung wurde in der Abbildung 29 grafisch dargestellt. Das bedeutet, dass sich nach Inkrafttreten der DSGVO bei 181 der untersuchten 216 KMUs die Cloud-Service-Nutzung verändert hat. Um die Forschungsfrage zu beantworten, wurden die 181 KMUs im Detail untersucht. Dabei wurde untersucht, wie sich die Nutzung verändert hat. Die Steigerung beziehungsweise die Senkung der Cloud-Service-Nutzung wurde in der Abbildung 30 grafisch dargestellt. 75 Prozent der 181 KMUs haben nach Inkrafttreten der DSGVO ihre Cloud-Service-Nutzung gesteigert. Das bedeutet, dass 136 der 181 untersuchten KMUs die Nutzung ihrer Cloud-Services gesteigert haben. Als Hauptgrund für die Steigerung der Cloud-Service-Nutzung gaben 116 KMUs an, dass der CSP die gewünschten Cloud-Services DSGVO-konform zur Verfügung stellen konnte. Dieser Grund galt auch für 44 untersuchte KMUs als Hauptgrund für die Einschränkung der Cloud-Service-Nutzung. Die Ergebnisse werden in der Tabelle 6 zusammengefasst.

Dieser Trend ist nicht nur in Österreich erkennbar. Die Cloud-Service-Nutzung steigt trotz Inkrafttreten der DSGVO in ganz Europa. Laut einer Statistik des „Statistischen Amt der Europäischen Union“ (kurz Eurostat) benutzte im Jahr 2018 jedes vierte europäische Unternehmen mindestens ein Cloud-Service. Des Weiteren geht aus dem Eurostat Report hervor, dass die IT-Branche den höchsten Anteil an Unternehmen mit Cloud-Services aufweist. Durch diesen Report können die Forschungsergebnisse hinsichtlich der gestiegenen Cloud-Service-Nutzung und der Branchenverteilung bekräftigt werden. [KS18]

Statistik	Anzahl	Prozent
Untersuchte Unternehmen	312	100
Untersuchte KMUs	222	71
KMUs die vor Inkrafttreten der DSGVO Cloud-Services einsetzten	212	95
KMUs die nach Inkrafttreten der DSGVO Cloud-Services einsetzen	216	97
KMUs die nach Inkrafttreten der DSGVO keine Cloud-Services einsetzen	4	2
KMUs bei denen sich die Cloud-Service-Nutzung nach Inkrafttreten der DSGVO verändert hat	181	84
KMUs bei denen die Cloud-Service-Nutzung nach Inkrafttreten der DSGVO gestiegen ist	136	75
KMUs bei denen die Cloud-Service-Nutzung nach Inkrafttreten der DSGVO gesunken ist	45	25

Tabelle 6 - Zusammenfassung der Untersuchungen

Aus diesen gewonnenen Forschungsergebnissen kann die gesetzte Forschungsfrage folgendermaßen beantwortet werden:

Die Nutzung der Cloud-Services wurde nach Inkrafttreten der DSGVO von 75 Prozent (136 von 181 KMUs) der untersuchten KMUs gesteigert. Lediglich 25 Prozent (45 von 181 KMUs) haben nach Inkrafttreten der DSGVO ihr Cloud-Service-Nutzung eingeschränkt. Mit den dargestellten Ergebnissen kann die gesetzte Forschungsfrage beantwortet werden.

Durch die analysierten Ergebnisse können noch weitere Erkenntnisse über die untersuchten Unternehmen abgeleitet werden. Durch die Erkenntnisse können Rückschlüsse auf die Cloud-Compliance der Unternehmen gezogen werden. Von den 222 untersuchten KMUs definierten lediglich 47 Prozent der KMUs das Thema Datenschutz als „eher wichtig“ bis „sehr wichtig“ (Abbildung 22). Des Weiteren haben nur 51 Prozent der befragten KMUs die gesetzliche Einhaltung

mit einer Priorität von „eher wichtig“ bis „sehr wichtig“ beantwortet (Abbildung 23). Das bedeutet, dass mehr als 50 Prozent der untersuchten KMUs die Einhaltung des Datenschutzes nur mit einer Priorität von „sehr unwichtig“ bis „neutral“ verfolgen.

Diese Ergebnisse spiegeln sich in den Bereichen DSGVO-Schulung, Auftragsverarbeitervertrag mit CSP sowie den TOMs des CSP wieder. Lediglich in 52 Prozent der untersuchten KMUs wurden die Mitarbeiter hinsichtlich der DSGVO geschult (Abbildung 25). Die Sensibilisierung beziehungsweise die Schulung der Mitarbeiter hinsichtlich der DSGVO sind wesentliche Aspekte der Artikel 37, 39 sowie 47 der DSGVO. Des Weiteren haben lediglich 51 Prozent der Unternehmen einen AVV mit dem Cloud-Service-Provider abgeschlossen (Abbildung 27). Die technischen und organisatorischen Maßnahmen des CSP sind nur 46 Prozent der untersuchten KMUs bekannt (Abbildung 28).

Die Cloud-Strategie wurde nach Inkrafttreten der DSGVO um elf Prozent gesteigert. Somit verfolgen 87 Prozent der untersuchten KMUs eine Cloud-Strategie (Abbildung 20). Des Weiteren haben 70 Prozent der untersuchten KMUs den Aspekt „Sicherheit“ als wichtigsten Treiber für die Cloud-Nutzung gewählt (Abbildung 17). Bei der Auswahl von Cloud-Services wählten 85 Prozent der untersuchten KMUs den Aspekt „Datenschutz“ als wichtigstes Auswahlkriterium (Abbildung 19).

Die untersuchten KMUs legen bei der Auswahl von Cloud-Services beziehungsweise des CSP großen Wert auf Datenschutz und Sicherheit (Abbildung 19), was sich jedoch in der internen Organisation der Unternehmen nicht wiederfindet. Die Ziele der DSGVO sind rund 74 Prozent der untersuchten KMUs bekannt (Abbildung 21). Trotz allem zeigen die Ergebnisse, dass sich nur knapp die Hälfte der untersuchten Unternehmen, die ihre Daten in der Cloud speichern oder verarbeiten, an die gesetzlichen Anforderungen der DSGVO

halten. Diese Erkenntnisse werden aus den Abbildungen 25, 26, 27 und 28 abgeleitet.

Um die Qualität der Antworten zu überprüfen wurden im Fragebogen zwei Kontrollen eingebaut. Die erste Kontrolle prüft, ob die Teilnehmer alle Fragen des Fragenbogens beantwortet haben. 99 Prozent der Teilnehmer haben alle Fragen des Fragebogens beantwortet. Eine weitere Kontrolle wurde in den Fragen 5 und 22 eingebaut. Die Summe der KMUs die nach Inkrafttreten der DSGVO Cloud-Services im Einsatz haben muss mit der Summe der Antworten der Frage 22 übereinstimmen. Das bedeutet, dass bei 216 KMUs die nach Inkrafttreten der DSGVO Cloud-Service im Einsatz hatten, auch die Cloud-Service-Nutzung verändert haben muss. Durch die Übereinstimmung dieser Summen kann eine weitere vollständige Durchgängigkeit der Antworten belegt werden. Die Übereinstimmung liegt bei 100 Prozent. Die Qualität der Antworten kann somit belegt werden.

Durch diese Forschungsergebnisse und den abgeleiteten Erkenntnissen konnte die Forschungsfrage beantwortet werden. Der folgende Kapitelabschnitt gibt einen Ausblick und soll den Nutzen dieser Arbeit erläutern.

5.2 Ausblick und Nutzen

Cloud-Computing hat sich in den letzten Jahren von einem Trend zu einer fest etablierten Technologie entwickelt. Durch die Digitalisierungsoffensiven der Unternehmen sowie durch die Cloud-Strategien der Hersteller reist der Hype um Cloud-Computing beziehungsweise Cloud-Service nicht ab. Unternehmen setzen vermehrt auf Cloud-Computing um Kostenvorteile zu nutzen sowie eine höhere Servicequalität zu erreichen. Die größten Herausforderungen der Cloud-Service-Provider ist und bleiben die Sicherheitsbedenken der Kunden. Die Kunden besitzen noch immer ein gewisse Hemmschwelle ihre Daten in Cloud-Umgebungen auszulagern. Diese Hemmschwelle kann nur durch Awareness-

Maßnahmen der CSP verringert werden. Des Weiteren müssen die CSP auf DSGVO-konforme Services setzten. Die angebotenen Services müssen den technischen sowie den organisatorischen Anforderungen der DSGVO entsprechen. Auftragsverarbeitervertrag und die Auflistung der TOMs müssen vom CSP direkt bei Vertragsabschluss an den Kunden übermittelt werden. Wenn sich die Awareness bei den Kunden durchgesetzt hat und die CSP die Services DSGVO-konform anbieten, dann kann das bestehende Wachstum von Cloud-Services noch weiter gesteigert werden.

In speziellen Unternehmensbereichen wird es immer Ausnahmen geben. In Bereichen wir „Forschung und Entwicklung“ oder im „Public Sektor“ werden Public-Cloud-Services auch in Zukunft nur schwer Einzug halten können. Dort können CSP beziehungsweise Anbieter auf Private-Cloud-Modelle setzten. Diese Modelle eignen sich speziell für abgeschottete und dezidierte Umgebungen. Die Datenhoheit liegt dabei zu 100 Prozent beim Kunden, rein der Betrieb der Infrastruktur wird an den Provider beziehungsweise Anbieter ausgelagert. Der Trend Cloud-Computing wird sich trotz allen rechtlichen Vorgaben weiter fortsetzen. Durch neue digitale Innovationen profitieren Unternehmen sowie Private Haushalte.

Die Arbeit richtet sich an Unternehmen aber auch an Cloud-Service-Provider beziehungsweise Cloud-Anbieter. Unternehmen können sich an den theoretischen Erkenntnissen dieser Arbeit orientieren. Die Arbeit soll eine Hilfe für die Einführung sowie den Betrieb von Cloud-Services sein. Des Weiteren können sich Unternehmen über die Anforderungen der DSGVO in Bezug auf Cloud-Services informieren. Durch die Forschungsergebnisse können CSP sowie Cloud-Anbieter Verbesserungen ableiten und somit ihre Services weiterentwickeln. Durch die Weiterentwicklung können in Zukunft die Kundenbedürfnisse besser erfüllt werden und damit höhere Umsätze generiert werden. Im nächsten und somit letzten Kapitelabschnitt dieser Arbeit wird die gesamte Arbeit zusammengefasst.

5.3 Zusammenfassung

Die vorliegende Arbeit hat sich das Ziel gesetzt, die Cloud-Service-Nutzung von kleinen und mittleren Unternehmen vor und nach Inkrafttreten der Datenschutz-Grundverordnung zu untersuchen. Die Zusammenfassung dient zur Erläuterung der einzelnen Kapitel dieser Arbeit und zur Konsolidierung der Ergebnisse aus der empirischen Untersuchung.

Im ersten Kapitel „Einleitung" wurde die Zielsetzung sowie die Motivation dieser Arbeit beschrieben. Aus dieser Zielsetzung leitete sich folgende Forschungsfrage ab:

„Wie hoch ist die Bereitschaft zur Cloud-Service-Nutzung bei KMUs vor und nach Inkrafttreten der DSGVO?"

Des Weiteren wurde im Kapitel 1 der grundlegende Aufbau dieser Arbeit sowie die ausgewählte Forschungsmethode zur Untersuchung der Forschungsfrage erläutert. Der Autor entschied sich bewusst für die empirische Forschung mittels einer quantitativen Befragung. Durch die quantitative Befragung war es möglich, in kurzer Zeit eine hohe Anzahl von standardisierten Befragungen durchzuführen. Des Weiteren war die quantitative Befragung eine kostengünstige Variante und bot den Probanden volle Anonymität bei der Beantwortung der Fragen. Der letzte Kapitelabschnitt des ersten Kapitels beschrieb die Abgrenzung dieser Arbeit zu vergleichbaren Arbeiten und grenzte die Forschung auf kleine und mittelständische Unternehmen ein. Großunternehmen wurden in der Studie nicht berücksichtigt.

Das Kapitel 2 beschrieb die theoretischen Grundlagen, die zur Beantwortung der Forschungsfrage dienten. Aus diesem Grund wurden in diesem zweiten Kapitel die Begrifflichkeiten „Cloud-Computing", „Datenschutz-Grundverordnung" und „kleine und mittelständische Unternehmen" theoretisch beschrieben und erläutert. Im Kapitelabschnitt „Cloud-Computing" wurden die aktuellen Service-

Modelle sowie die Betriebsmodelle theoretisch erläutert. Auf diese beschriebenen Service-Modelle wurde anschließend in der empirischen Studie verwiesen. Des Weiteren wurden in diesem Kapitelanschnitt die „Cloud-Service-Kriterien“ im Detail erläutert, um das „Trusted-Cloud-Label“ zu erreichen. Diese Cloud-Service-Kriterien unterstützen die Nutzer bei der Auswahl von Cloud-Service-Provider. Die Cloud-Service-Kriterien decken die Bereiche Datensicherheit, Datenschutz-Grundverordnung (DSGVO), Rechtskonformität, Integrierbarkeit und Investitionssicherheit ab. Zudem wurden in diesem Kapitelabschnitt die Anwendungsbereiche von Cloud-Services dargestellt. Aus diesen Anwendungsbereichen wurden die Vor- und Nachteile von Cloud-Services abgeleitet und im Kapitelabschnitt 2.1.7 erläutert. Der Kapitelabschnitt „Datenschutz-Grundverordnung“ beschrieb die DSGVO anhand von Begriffsdefinitionen und leitete aus dem geschichtlichen Hintergrund weitere Fakten über die DSGVO ab. Ein weiterer Fokus wurde auf die Kernziele der DSGVO sowie die Anwendungsbereiche der DSGVO gelegt. Zudem wurden in diesem Kapitelabschnitt essenzielle Begrifflichkeiten der Datenschutz-Grundverordnung erläutert. Des Weiteren wurden die gesetzlichen Anforderungen der technischen und organisatorischen Maßnahmen dargestellt. Die rechtlichen Grundlagen dieser TOMs wurden im Kapitelabschnitt „Cloud-Compliance“ in die Praxis umgelegt. Abschließend wurde im Kapitelabschnitt „DSGVO“ auf die Datenschutzbehörde und auf die möglichen Strafen bei der Nichteinhaltung der gesetzlichen Anforderungen verwiesen. Im letzten Kapitelabschnitt des Kapitels 2 wurden die kleinen und mittelständischen Unternehmen behandelt. Die KMUs sind ein wesentlicher Bestandteil der Forschung und wurden aus diesem Grund theoretisch untersucht. Der Kapitelabschnitt „kleine und mittelständische Unternehmen“ beschrieb anhand einer Begriffsdefinition die KMUs und wies anhand von Statistiken auf die Verteilung der KMUs in Österreich hin. Die gesammelten theoretischen Erkenntnisse des Kapitels 2 sind ein wichtiger Bestandteil des Kapitels 3.

Das dritte Kapitel stand im Fokus der „Cloud-Compliance“. Die Cloud-Compliance steht für die Einhaltung gesetzlicher, vertraglicher sowie sonstigen Regularien. Gemäß dem „Cloud-Kompass“ besteht die Cloud-Compliance aus den Bereichen „vertragliche Rahmenbedingungen“, „IT-Servicemanagement“, „Informationssicherheit“ sowie „Datenschutz“. Diese vier Teilbereiche wurden im Kapitel 3 ausführlich beschrieben und auf die Cloud-Compliance bezogen. Des Weiteren wurde im dritten Kapitel der „Life-Cycle-Cloud-Computing“ erläutert. Dieser Life-Cycle besteht aus den Phasen „Planung“, „Umsetzung und -Migration“, „Betrieb“ sowie aus der Phase „Beendigung“. Diese vier Phasen entsprechen dem PDCA-Zyklus, wie er auch in der Informationssicherheit gemäß ISO/IEC 27001, im IT-Servicemanagement gemäß ITIL sowie auch im Datenschutz gemäß DSGVO eingesetzt wird. Der Kapitelabschnitt 3.5 erläuterte die Bedrohungen von Cloud-Services. Die Bedrohungen wurden in die Bereiche „Cloud-Provider-Infrastruktur“, „Nutzung von Cloud-Services“ sowie „Einführung von Cloud-Services“ unterteilt. Zu jedem dieser Bereiche wurden Bedrohungen evaluiert und erläutert. Anhand dieser evaluierten Bedrohungen wurden im nächsten Kapitelabschnitt des dritten Kapitels Empfehlungen und möglichen Gegenmaßnahmen abgeleitet. Diese Maßnahmen wurden in organisatorische und technische Maßnahmen unterteilt. Die Maßnahmen referenzieren sich auf die zuvor beschriebenen theoretischen Grundlagen der Cloud-Compliance. Nach der Ausarbeitung dieser empfohlenen Maßnahmen schloss das Kapitel 3 und somit den theoretischen Teil dieser Arbeit ab.

Mit dem Kapitel 4 startete der praktische Teil dieser Arbeit. In diesem Kapitel wurden die Forschungsmethodik und das Fragebogendesign beschrieben. Des Weiteren wurden die erhobenen Forschungsergebnisse analysiert, aufbereitet und interpretiert. Der Autor dieser Arbeit hat sich bei der Forschungsmethodik auf die empirische Untersuchung anhand eines Online-Fragebogens gestützt. Anhand dieser Methode war es möglich, eine große Anzahl an Probanden durch einen standardisierten Fragebogen zu befragen. Die Befragung war anonymisiert

und wurde über ein Onlineportal durchgeführt. Der Online-Fragebogen bestand aus vier Rubriken mit insgesamt 24 Fragen. Die vier Rubriken bestanden aus „Organisation“, „Cloud-Computing“, „Datenschutz-Grundverordnung“ und „Nutzungsverhalten“. Die vier Rubriken und die darin enthaltenen Fragen leiteten sich aus der Forschungsfrage ab. Die Fragen aus der Rubrik „Organisation“ zielten auf die Größe des Unternehmens, die Stelle der Probanden sowie auf die Branche des Unternehmens ab. Mit den Rubriken „Cloud-Computing“ und „Datenschutz-Grundverordnung“ wurden die Probanden nach den eingesetzten Cloud-Services sowie nach den Erfahrungen mit der DSGVO befragt. Die letzte Rubrik „Nutzungsverhalten“ sollte zusammenfassend zu den vorherigen Rubriken die Antwort auf die Forschungsfrage liefern. Die Ergebnisse aus den 24 Fragen wurden im Kapitelabschnitt 4.3 grafisch dargestellt und interpretiert. Durch die quantitative Onlinebefragung konnten 373 Aufrufe des Fragebogens verzeichnet werden. Aus diesen 373 Aufrufen konnten 312 vollständige Ergebnisse gewonnen werden. Der Befragungszeitraum betrug 40 Tage. Aus den Ergebnissen ging hervor, dass von den untersuchten 312 Unternehmen 222 Unternehmen der Zielgruppe entsprachen. Damit konnten 71 Prozent der befragten Unternehmen der Zielgruppe „kleinen und mittelständischen Unternehmen“ zugeordnet werden. Des Weiteren ging aus den Ergebnissen der Forschung hervor, dass aktuell 216 der untersuchten KMUs Cloud-Services einsetzen. Damit entsprachen 216 KMUs der gesuchten Zielgruppe. Nach der eindeutigen Identifizierung der Zielgruppe konnten die Interpretation der Ergebnisse auf diese identifizierten Unternehmen abzielen. Abschließend wurde in diesem Kapitelabschnitt das Nutzungsverhalten der Unternehmen interpretiert. Die Analyse der Ergebnisse hat gezeigt, dass sich bei 182 der untersuchten 216 KMUs die Cloud-Service-Nutzung verändert hat. Das bedeutet, dass sich die Cloud-Service-Nutzung bei 84 Prozent der KMUs verändert hat. Um die Forschungsfrage ganzheitlich zu beantworten, wurden die KMUs aufgefordert, die veränderte Cloud-Service-Nutzung darzustellen. Aus diesen Ergebnissen ging hervor, dass bei 137 KMUs die Cloud-Service-Nutzung

gestiegen ist. Lediglich bei 45 KMUs ist die Nutzung nach Inkrafttreten der DSGVO gesunken. Der letzte Abschnitt des Kapitelabschnittes 4.3.4 erläuterte die Gründe der Steigerung sowie die Gründe für die Einschränkung der Cloud-Service-Nutzung.

Im Kapitel 5 wurde die Forschungsfrage beantwortet sowie die Zusammenhänge der gewonnen Erkenntnissen aus den Forschungsergebnissen erläutert. Die Forschungsergebnisse zeigten, dass die untersuchten KMUs die Cloud-Service-Nutzung nach Inkrafttreten der DSGVO gesteigert haben. Des Weiteren konnte Datenschutz und Sicherheit als größter Treiber sowie als wichtigstes Auswahlkriterium identifiziert werden. Die Cloud-Strategie wurde bei den untersuchten KMUs gesteigert. Nur rund 50 Prozent der untersuchten KMUs können die vertraglichen und gesetzlichen Anforderungen hinsichtlich der Cloud-Compliance abbilden. Im Anschluss wurde ein Ausblick sowie der Nutzen der Arbeit erläutert.

II. ANHANG


FERDINAND PORSCHE
FERN FH

0% ausgefüllt

Herzlich Willkommen zu meiner Umfrage

Im Rahmen meiner Masterarbeit in Wirtschaftsinformatik an der Ferdinand Porsche FernFH möchte ich herausfinden, wie sich die Nutzung von Cloud-Services bei KMUs unter Berücksichtigung der DSGVO verändert hat.

Ihre Antworten werden natürlich **vertraulich** behandelt und **anonym** elektronisch verarbeitet.

Der Zeitaufwand beträgt max. 10 Minuten.

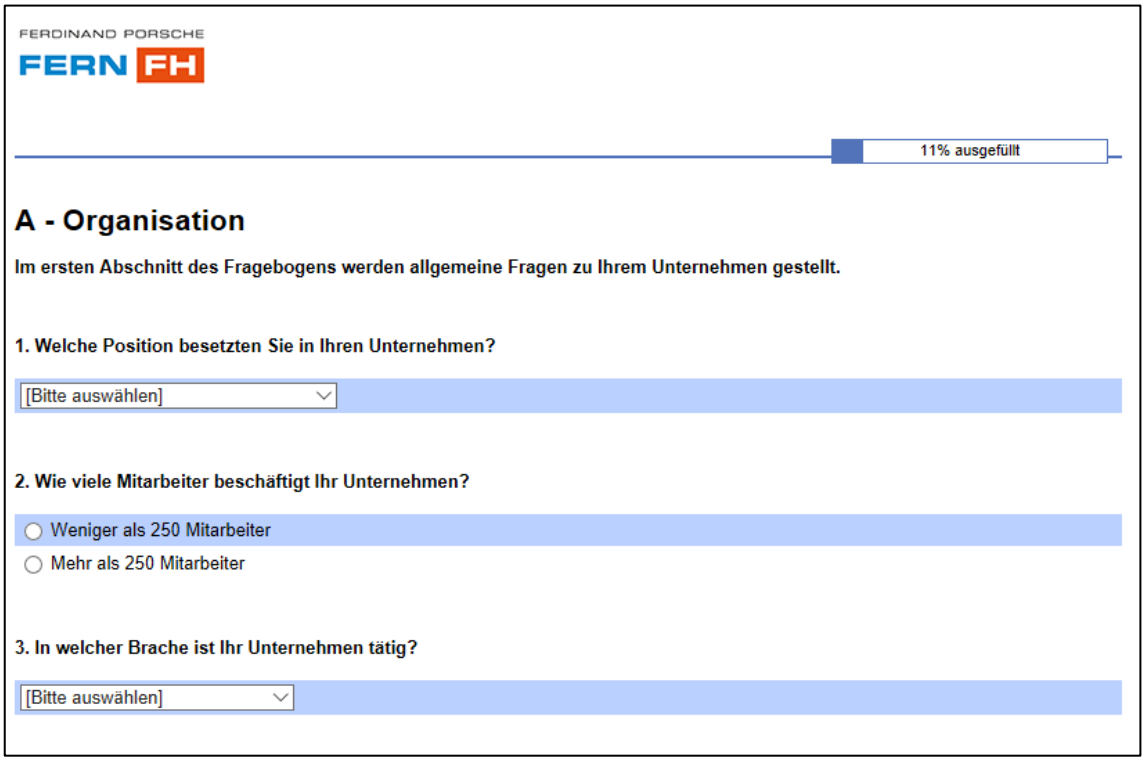
Für Fragen und Anregungen stehe ich Ihnen sehr gerne zur Verfügung.

Sie erreichen mich unter folgender E-Mail-Adresse: Andreas.Kaufmann@mail.fernfh.ac.at

Vielen Dank für Ihre Unterstützung!

Andreas Kaufmann, BA

Anhang Abbildung 1 - Fragebogen Einleitung


FERDINAND PORSCHE
FERN FH

11% ausgefüllt

A - Organisation

Im ersten Abschnitt des Fragebogens werden allgemeine Fragen zu Ihrem Unternehmen gestellt.

1. Welche Position besetzten Sie in Ihren Unternehmen?

[Bitte auswählen]

2. Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?

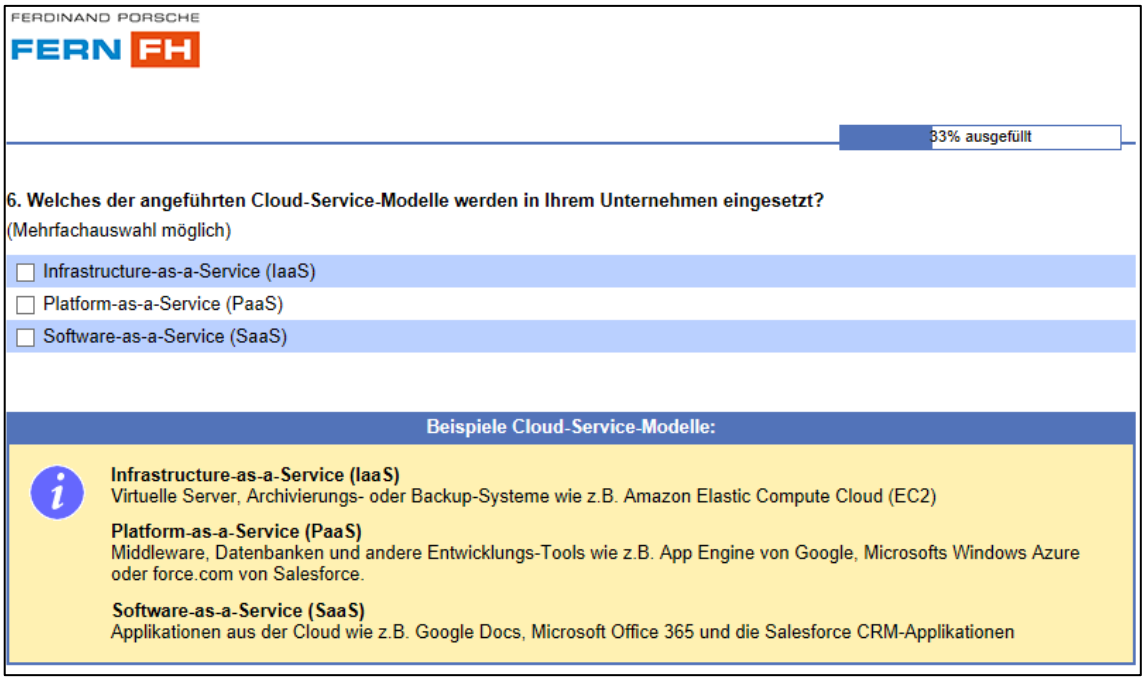
- ○ Weniger als 250 Mitarbeiter
- ○ Mehr als 250 Mitarbeiter

3. In welcher Brache ist Ihr Unternehmen tätig?

[Bitte auswählen]

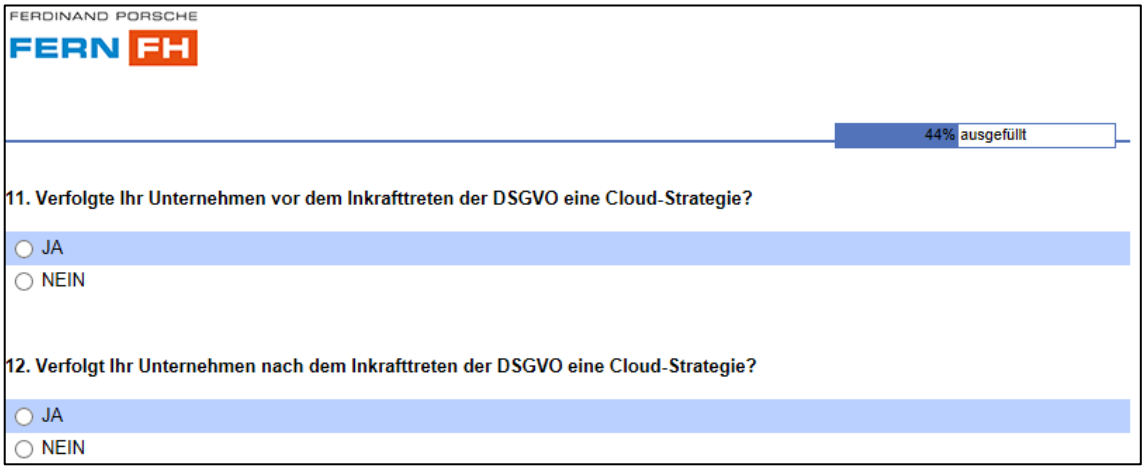
Anhang Abbildung 2 - Fragebogen Rubrik „Organisation“

Anhang Abbildung 3 - Fragebogen Rubrik "Cloud-Computing" 1/4

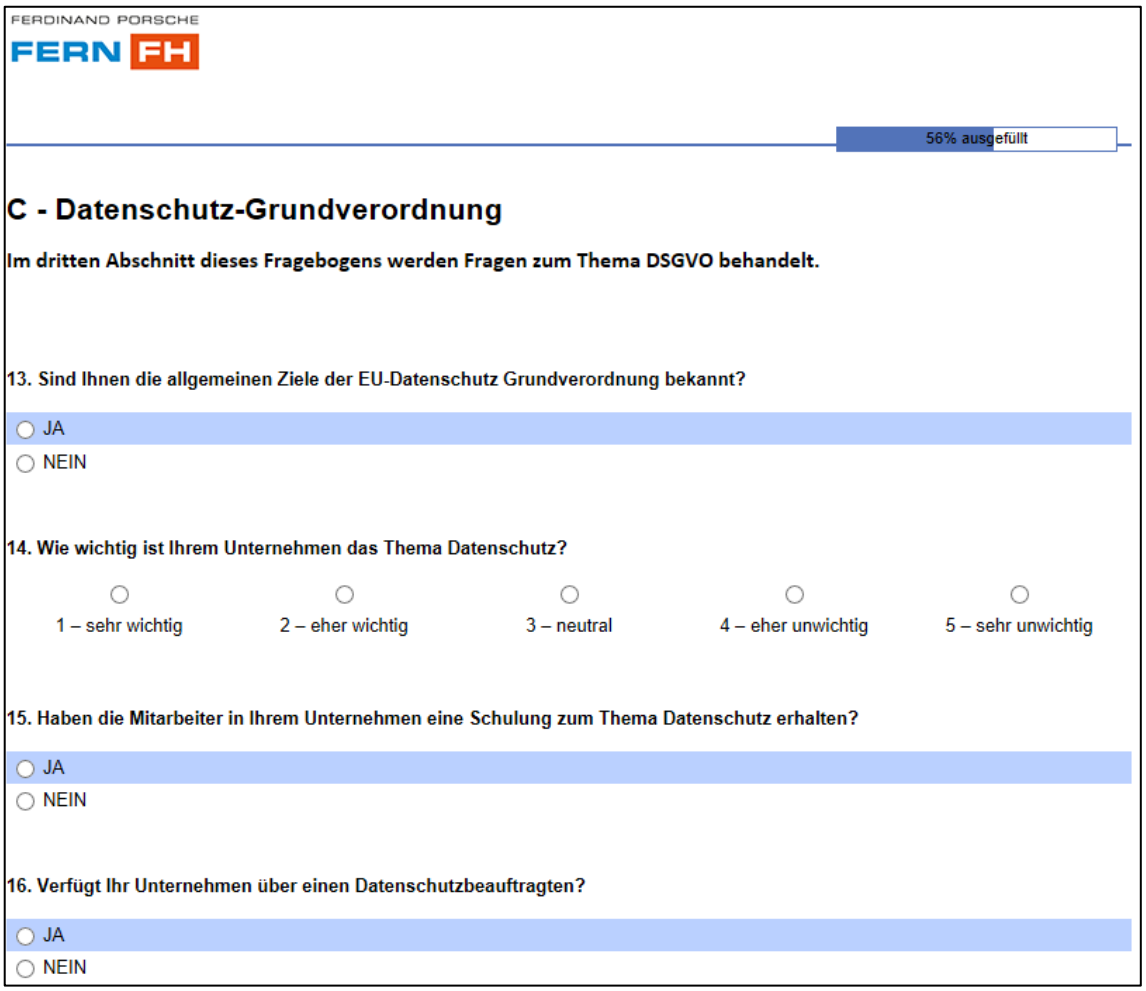


Anhang Abbildung 4 - Fragebogen Rubrik "Cloud-Computing" 2/4

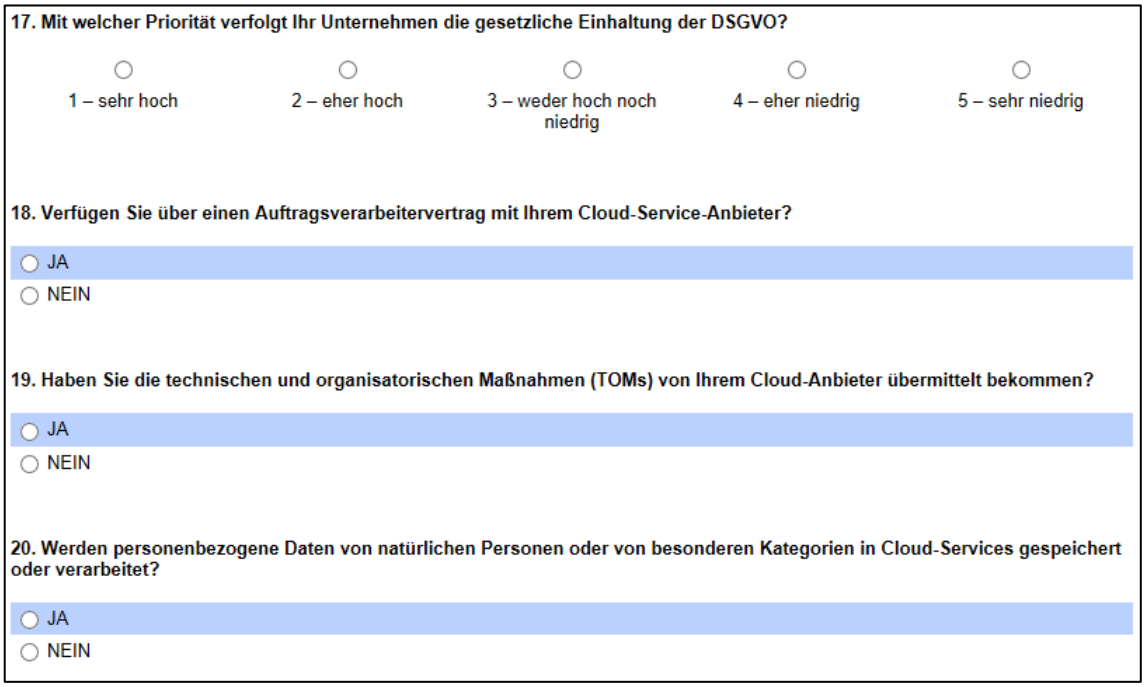
Anhang Abbildung 5 - Fragebogen Rubrik "Cloud-Computing" 3/4



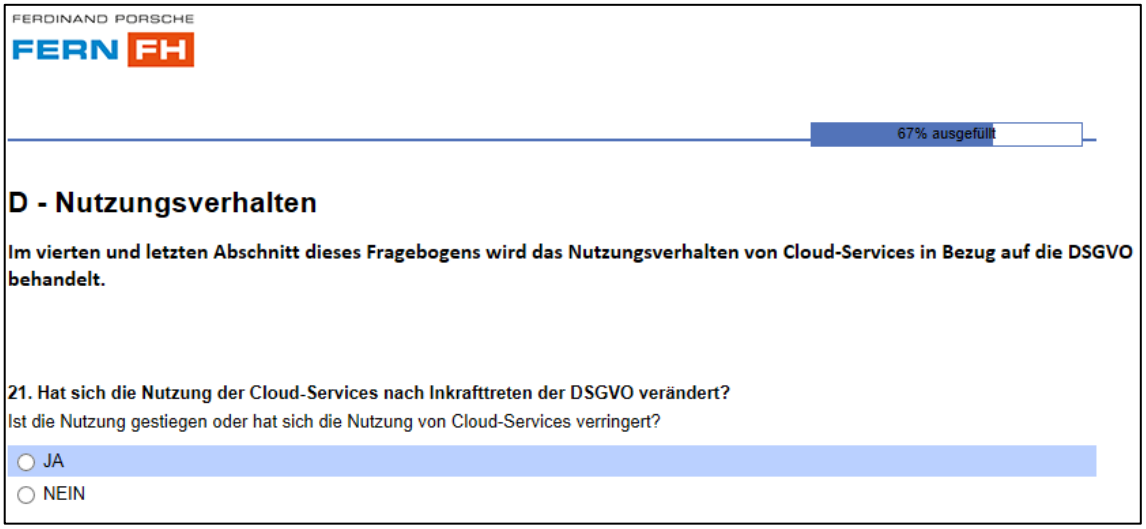
Anhang Abbildung 6 - Fragebogen Rubrik "Cloud-Computing" 4/4



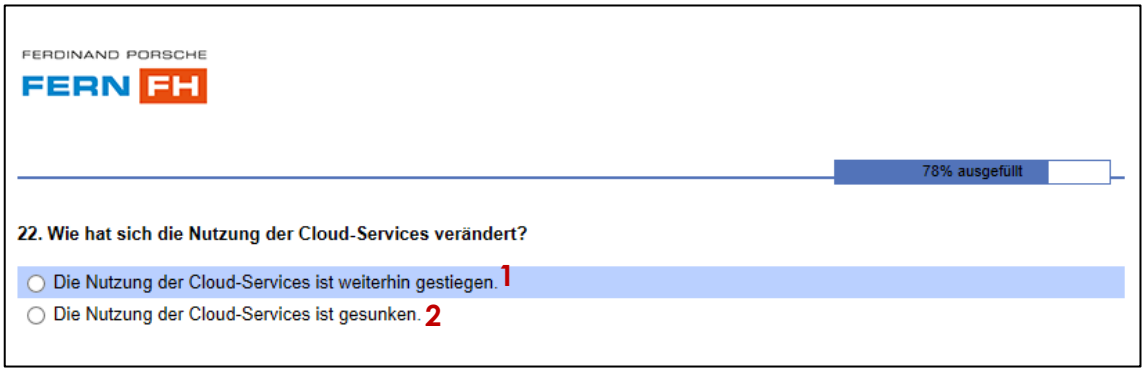
Anhang Abbildung 7 - Fragebogen Rubrik " DSGVO " 1/2



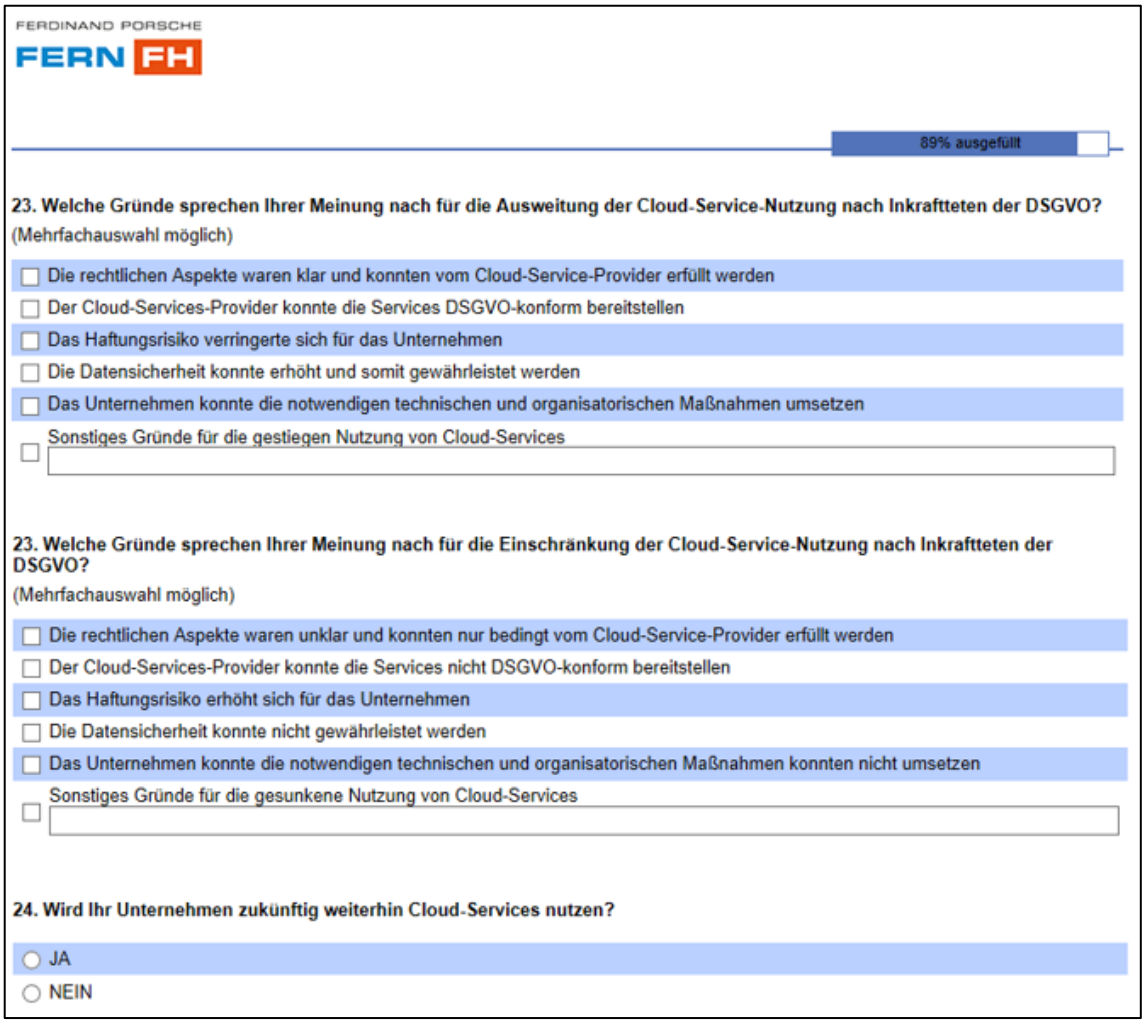
Anhang Abbildung 8 - Fragebogen Rubrik "DSGVO " 2/2



Anhang Abbildung 9 - Fragebogen Rubrik "Nutzungsverhalten" 1/3



Anhang Abbildung 10 - Fragebogen Rubrik "Nutzungsverhalten" 2/3



Anhang Abbildung 11 - Fragebogen Rubrik "Nutzungsverhalten" 3/3

III. ABBILDUNGSVERZEICHNIS

Abbildung 1 - Grafische Gliederung der Arbeit 10

Abbildung 2 - NIST Definition Cloud-Computing [MG11, S. 2f.].....17

Abbildung 3 - Faktoren von Cloud-Computing [Ba14, S. 42] 18

Abbildung 4 - Cloud-Service-Architektur [HY10, S. 11] 22

Abbildung 5 - Cloud-Service-Betriebsmodelle.....23

Abbildung 6 - Grundsätze der DSGVO [Ra16, S. 17f.].....43

Abbildung 7 - Definition KMUs in Österreich [GB19] 60

Abbildung 8 - Cloud-Compliance 63

Abbildung 9 - Life-Cycle-Cloud-Computing [De10, S. 73] 67

Abbildung 10 - Vorgehensweise d. empirischen Studie.....93

Abbildung 11 - Mitarbeiteranzahl der Unternehmen.....99

Abbildung 12 - Position des Probanden..... 100

Abbildung 13 - Unternehmensbranchen 101

Abbildung 14 - Cloud-Service-Einsatz..... 103

Abbildung 15 - Cloud-Service-Modelle..... 104

Abbildung 16 - Cloud-Service-Provider..... 105

Abbildung 17 - Cloud-Service-Treiber..... 106

Abbildung 18 - Cloud-Service-Herausforderungen..... 107

Abbildung 19 - Cloud-Service-Kriterien 108

Abbildung 20 - Cloud-Strategie 109

Abbildung 21 - Ziele der DSGVO 110

Abbildung 22 - Wichtigkeit DSGVO 111

Abbildung 23 - Priorisierung gesetzlicher Anforderungen 112

Abbildung 24 - Verarbeitung von personenbezogenen Daten 112

Abbildung 25 - Datenschutzschulung 113

Abbildung 26 - Datenschutzbeauftragten 114

Abbildung 27 – Auftragsverarbeitervertrag 115

Abbildung 28 – TOMs 115

Abbildung 29 - Veränderung der Cloud-Service-Nutzung 117

Abbildung 30 - Cloud-Service-Nutzungsveränderung 118

Abbildung 31 - Gründe für die Einschränkung der Cloud-Services 119

Abbildung 32 - Gründe für die Erweiterung der Cloud-Services 120

Abbildung 33 - Zukünftige Nutzung von Cloud-Services 121

Abbildung 34 - Zukünftige CC-Nutzung pro Branche 122

Abbildung 35 - Zukünftige Cloud-Service-Modelle 122

Anhang Abbildung 1 - Fragebogen Einleitung 135

Anhang Abbildung 2 - Fragebogen Rubrik „Organisation“ 135

Anhang Abbildung 3 - Fragebogen Rubrik "Cloud-Computing" 1/4 136

Anhang Abbildung 4 - Fragebogen Rubrik "Cloud-Computing" 2/4 136

Anhang Abbildung 5 - Fragebogen Rubrik "Cloud-Computing" 3/4 137

Anhang Abbildung 6 - Fragebogen Rubrik "Cloud-Computing" 4/4 138

Anhang Abbildung 7 - Fragebogen Rubrik " DSGVO " 1/2 138

Anhang Abbildung 8 - Fragebogen Rubrik "DSGVO " 2/2 139

Anhang Abbildung 9 - Fragebogen Rubrik "Nutzungsverhalten" 1/3 139

Anhang Abbildung 10 - Fragebogen Rubrik "Nutzungsverhalten" 2/3 140

Anhang Abbildung 11 - Fragebogen Rubrik "Nutzungsverhalten" 3/3 140

IV. TABELLENVERZEINIS

Tabelle 1 – SaaS-Bereiche und -Anbieter.....31

Tabelle 2 - Statistische KMU-Daten aus Österreich (Stand 2016) [GB19] 61

Tabelle 3 - ITIL-Prozesse aus der Verantwortlichen-Sicht [BÜ16] 66

Tabelle 4 - Cloud-Provider-Zertifizierungen [Tr16, S. 6] 81

Tabelle 5 - Rücklauf-Statistik 98

Tabelle 6 - Zusammenfassung der Untersuchungen..... 126

V. LITERATURVERZEICHNIS

[A-18] A-SIT Zentrum für sichere Informationstechnologie – Austria: Identitätsdiebstahl. https://www.onlinesicherheit.gv.at/service/cybermonitor/identitaetsdiebstahl/135064.html, abgerufen am 26.02.2018.

[AK18] Alsabah, N.; Krösmann, C.: Fast ein Drittel der Unternehmen verzeichnet Cyberangriffe. https://www.bitkom.org/Presse/Presseinformation/Fast-ein-Drittel-der-Unternehmen-verzeichnet-Cyberangriffe.html, abgerufen am 04.03.2018.

[Ba11] Badger, L. et al.: US Government Cloud Computing Technology Roadmap. https://www.nist.gov/sites/default/files/documents/itl/cloud/SP_500_293_volumeII.pdf, abgerufen am 01.02.2019.

[Ba14] Barton, T.: E-Business mit Cloud Computing. Grundlagen, Praktische Anwendungen, verständliche Lösungsansätze. Springer Vieweg, Wiesbaden, 2014.

[Be18] Bergauer, C.: Personenbezogene Daten. Begriff und Kategorien. In LexisNexis, 2018, 2018; S. 12–14.

[BGS14] Bourgeas, V.; Giannakouris, K.; Smihily, M.: Nutzung von IKT in Unternehmen im Jahr 2014. Jedes fünfte Unternehmen in der EU28 nutzt Cloud Computing Dienst. http://ec.europa.eu/eurostat/documents/2995521/6208102/4-09122014-AP-DE.pdf/4a3fdeb8-d389-41a2-92cc-db541a45646e, abgerufen am 29.09.2018.

[Bl14] BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.: IT-Strategie – Digitale Agenda für Deutschland. Deutschland zum Digitalen Wachstumsland entwickeln. https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Positionen/BITKOM-legt-IT-Strategie-vor/BITKOM-IT-Strategie.pdf, abgerufen am 04.02.2019.

[Bl16] BITKOM: Was muss ich wissen zur EU-Datenschutz Grundverordnung? https://www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2016/160909-EU-DS-GVO-FAQ-03.pdf, abgerufen am 04.03.2019.

[Bo17] Boegelein, L.: Sichere Passwörter. Paradigmenwechsel bei Passwortsicherheit. https://it-service.network/blog/2017/10/23/sichere-passwoerter-passwortsicherheit/, abgerufen am 12.08.2019.

[Br15] Breitenreuter, D.: Diese 3 Branchen nutzen die Cloud noch (zu?) wenig. https://www.cancom.info/2015/05/diese-3-branchen-nutzen-die-cloud-noch-zu-wenig/, abgerufen am 05.05.2019.

[Bu12] Bundesamt für Sicherheit in der Informationstechnik: Sicherheitsempfehlung für Cloud Computing Anbieter. Mindestanforderungen in der Informationssicherheit. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile&v=7, abgerufen am 28.02.2019.

[Bu14] Bundesamt für Sicherheit in der Informationstechnik: IT-Grund-schutz-Ka-ta-lo-ge. Einführung in das Cloud Management. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzK

ataloge/Inhalt/_content/m/m04/m04446.html, abgerufen am 01.02.2019.

[Bu16] Bundesamt für Sicherheit in der Informationstechnik: Sichere Nutzung von Cloud-Diensten. Schritt für Schritt von der Strategie bis zum Vertragsende. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=10, abgerufen am 26.02.2019.

[BÜ16] Büst, R.: IT-Servicemanagement als Bestandteil der Public Cloud-Strategie. https://www.crisp-research.com/it-servicemanagement-als-bestandteil-der-public-cloud-strategie/, abgerufen am 19.02.2019.

[Bu17] Bundesamt für Sicherheit in der Informationstechnik: Anforderungskatalog Cloud Computing (C5). Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf?__blob=publicationFile&v=3, abgerufen am 04.03.2019.

[Bu17] Bundesministerium für Finanzen et al.: Cloud Computing Kompass. Eine Orientierungshilfe für Cloud-Service-Kunden, abgerufen am 19.02.2019.

[Bu18] Bundesministerium für Wirtschaft und Energie: Kriterienkatalog für Cloud Services. https://www.trusted-cloud.de/sites/default/files/tc_kriterienkatalog_v2_final_1.pdf, abgerufen am 02.02.2019.

[Ci18] Cisco Systems: Cisco Global Cloud Index. Forecast and Methodology, 2016-2021. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf, abgerufen am 11.05.2019.

[De10] Dehmel, S. et al.: Cloud Computing – Was Entscheider wissen müssen. Ein ganzheitlicher Blick über die Technik hinaus Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance. https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2010/Leitfaden/Leitfaden-Cloud-Computing-Was-Entscheider-wissen-muessen/BITKOM-Leitfaden-Cloud-Computing-Was-Entscheider-wissen-muessen.pdf, abgerufen am 19.02.2019.

[DH18] Djhangiri, N.; Hassl, G.: Unternehmen mit Nutzung folgender Cloud Services 2018. https://www.statistik.at/web_de/statistiken/energie_umwelt_innovation_mobilitaet/informationsgesellschaft/ikt-einsatz_in_unternehmen/105100.html, abgerufen am 10.05.2019.

[DH18] Djhangiri, N.; Hassl, G.: Jedes vierte Unternehmen nutzt Cloud Services. http://www.statistik.at/web_de/statistiken/energie_umwelt_innovation_mobilitaet/informationsgesellschaft/ikt-einsatz_in_unternehmen/119330.html, abgerufen am 15.05.2019.

[Ec06] Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg, München, 2006.

[GB19] Gavac, K.; Bachinger, K.: KMU-Daten. https://www.kmuforschung.ac.at/zahlen-fakten/kmu-daten/, abgerufen am 17.02.2019.

[He12] Herfert, M.: Über die Sicherheit von Cloud-Speicherdiensten. https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_ManagementSummary.pdf, abgerufen am 04.04.2018.

[He16] Herrmann, W.: Desktop-as-a-Service. Wann lohnt sich der Einsatz? https://www.computerwoche.de/a/desktop-as-a-service-wann-lohnt-sich-der-einsatz,3313102, abgerufen am 28.02.2019.

[He19] Heidkamp, P. et al.: Cloud-Monitor 2018. Strategien für eine zukunftsorientierte Cloud Security und Cloud Compliance. https://hub.kpmg.de/cloud-monitor-2018, abgerufen am 18.02.2019.

[Ho12] Hoepman, J.-H.: Privacy Design Strategies. https://www.cs.ru.nl/~jhh/publications/pdp.pdf, abgerufen am 07.04.2019.

[HY10] Harms, R.; Yamartino, M.: THE ECONOMICS OF THE CLOUD. https://news.microsoft.com/download/archived/presskits/cloud/docs/The-Economics-of-the-Cloud.pdf, abgerufen am 08.04.2019.

[Jo18] Jost, T. et al.: Datenschutz-Audit. Recht - Organisation - Prozess - IT der Praxisleitfaden zur Datenschutz-Grundverordnung. LexisNexis Verlag GmbH, Wien, 2018.

[Ke16] Kersten, H. et al.: IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls. Springer Vieweg, Wiesbaden, 2016.

[Ko03] Kommission der europäischen Gemeinschaft: EMPFEHLUNG DER KOMMISSION vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. K(2003) 1422. http://wko.at/Statistik/kmu/Defintion_KMU_Empfehlung2003-361-EG.pdf, abgerufen am 17.02.2019.

[Ko07] Kornmeier, M.: Wissenschaftstheorie und wissenschaftliches Arbeiten. Eine Einführung für Wirtschaftswissenschaftler. Physica-Verlag Heidelberg, Heidelberg, 2007.

[KS18] Kaminska, M.; Smihily, M.: Cloud computing - statistics on the use by enterprises. https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights, abgerufen am 05.05.2019.

[La18] LaPalme, J.: Cloud-Nutzung und DSGVO in Einklang bringen. https://www.cloudcomputing-insider.de/cloud-nutzung-und-dsgvo-in-einklang-bringen-a-678492/, abgerufen am 29.29.2018.

[LBD14] Lissen, N.; Brünger, C.; Damhorst, S.: IT-Services in der Cloud und ISAE 3402: Ein praxisorientierter Leitfaden für eine erfolgreiche Auditierung. Springer Science and Business Media, Place of publication not identified, 2014.

[Mc18] McLaughlin, P.: Die DSGVO – eine Weiterentwicklung der Datenschutzrichtlinie von 1995. https://blogs.oracle.com/de-cloud/dsgvo-weiterentwicklung-der-datenschutzrichtlinie-von-1995, abgerufen am 02.02.2019.

[MG11] Mell, P.; Grance, T.: The NIST Definition of Cloud Computing. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, abgerufen am 29.09.2018.

[Mo06] Moos, F.: Datenschutzrecht. Schnell erfasst. Springer, Berlin, Heidelberg, 2006.

[MPR15] Münzl, G.; Pauly, M.; Reti, M.: Cloud Computing als neue Herausforderung für Management und IT. Springer Vieweg, Berlin, 2015.

[MRV11] Metzger, C.; Reitz, T.; Villar, J.: Cloud computing. Chancen und Risiken aus technischer und unternehmerischer Sicht. Hanser, München, 2011.

[MÜ09] Münzl, G. et al.: Cloud Computing - Evolution in der Technik. Revolution im Business. https://www.cloud-finder.ch/fileadmin/Dateien/Studien/BITKOM-Leitfaden-CloudComputing.pdf, abgerufen am 02.02.2019.

[Ös19] Österreichische Datenschutzbehörde: Österreichische Datenschutzbehörde. https://www.dsb.gv.at/, abgerufen am 15.02.2019.

[Pr14] Pröhl, T. et al.: IT-Servicemanagement im Cloud Computing. https://link.springer.com/article/10.1007/BF03340752, abgerufen am 19.02.2019.

[Ra16] Rat der Europäischen Union: Standpunkt des Rates in erster Lesung im Hinblick auf den Erlass der VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-

Grundverordnung).
https://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1-ADD-1/de/pdf, abgerufen am 02.02.2019.

[Ro16] Rouse, M.: Storage as a Service (SaaS).
https://www.computerweekly.com/de/definition/Storage-as-a-Service-SaaS, abgerufen am 28.02.2019.

[Sc18] Schweiger, T.: Was sind „TOMs“? (technische und organisatorische Maßnahmen) iSd DSGVO?
https://www.wko.at/branchen/information-consulting/finanzdienstleister/toms-muster.pdf, abgerufen am 07.04.2019.

[St16] Statista: Nutzung von Cloud Computing in Unternehmen in Deutschland im Jahr 2016 nach Unternehmensgröße.
https://de.statista.com/statistik/daten/studie/305563/umfrage/einsatz-von-cloud-computing-in-deutschen-unternehmen-nach-groesse/, abgerufen am 29.09.2018.

[Ta14] Taylor, C.: Backup as a Service: To BaaS or Not to BaaS. Cloud-based Backup as a Service may or may not be a good choice for your business, depending on cost and management factors.
https://www.datamation.com/cloud-computing/backup-as-a-service-to-baas-or-not-to-baas-1.html, abgerufen am 28.02.2019.

[TL16] Tonweber, G.; Lukac, D.: Die Haftungspflicht des Managements und Cyberversicherungen. In Zeitschrift für Finance und Controlling, 2016, 2016; S. 253–254.

[Tr16] Trusted Cloud Kompetenznetzwerk e.V.: Cloud-Standards und Zertifizierungen im Überblick. Was "Cloud-spezifisch" beachtet

werden sollte. https://www.trusted-cloud.de/sites/default/files/beitrag-cloud-standards_und_zertifizierungen_im_ueberblick.pdf, abgerufen am 04.03.2019.

[VB18] Voigt, P.; Bussche, A. v. d.: EU-Datenschutz-Grundverordnung (DSGVO). Praktikerhandbuch. Springer, Berlin, Germany, 2018.

[VHH13] Vossen, G.; Haselmann, T.; Hoeren, T.: Cloud-Computing für Unternehmen. Technische, wirtschaftliche, rechtliche und organisatorische Aspekte. dpunkt-Verl., Heidelberg, 2013.

[Wi18] Wirtschaftskammer Österreich: EU-Datenschutz-Grundverordnung (DSGVO). Überblick zum Datenschutz in Österreich. https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html, abgerufen am 02.02.2019.

[Wi19a] Wikipedia: Cloud database. https://en.wikipedia.org/wiki/Cloud_database, abgerufen am 28.02.2019.

[Wi19b] Wikipedia: Everything as a Service. https://de.wikipedia.org/wiki/Everything_as_a_Service#Weitere_Ansätze, abgerufen am 02.02.2019.

[WZ14] Wachter, S.; Zaelke, T.: Systemkonsolidierung und Datenmigration als geschäftskritische Erfolgsfaktoren. https://link.springer.com/article/10.1365/s40702-014-0023-2, abgerufen am 05.01.2019.