Wirtschaftlichkeitsbetrachtung zur EU-Datenschutz-Grundverordnungs-Compliance in der österreichischen stationären Krankenversorgung

Analyse der Chancen und Herausforderungen sowie des wirtschaftlichen Umgangs im Zuge ihrer Erfüllung

Master Thesis zur Erlangung des akademischen Grades

Master of Business Administration (MBA)

an der Universität für Weiterbildung (Donau-Universität Krems)

und der Technischen Universität Wien, Continuing Education Center

eingereicht von

Ing. Mag. Christina Haas

BetreuerIn

RA Dr. Lukas Feiler, SSCP, CCIPP/E

Wien, 19.09.2017

Eidesstattliche Erklärung

Ich, ING. MAG. CHRISTINA HAAS

geboren am 22.12.1981, in Wels

erkläre, hiermit

1. dass ich meine Master Thesis selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfen bedient habe,

2. dass ich meine Master Thesis bisher weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe,

3. dass ich, falls die Arbeit mein Unternehmen betrifft, meine/n ArbeitgeberIn über Titel, Form und Inhalt der Master Thesis unterrichtet und sein Einverständnis eingeholt habe.

Wien, 19.09.2017

Ort, Datum

.....

Unterschrift

Danksagung

Ein MBA Studium bringt herausfordernde Zeiten mit sich und es verändert einen, was auch ich erleben durfte. Oft stößt man an seine Grenzen und meistert die Dinge dann aber doch, um schlussendlich daran zu wachsen. Es war eine sehr herausfordernde Zeit, aber eine lehrreiche Zeit auf vielen Ebenen die ich keinesfalls missen möchte.

Allen voran möchte ich mich bei meinem Mann bedanken, der immer an mich glaubt und mich auch zu diesem Studium motiviert hat. Ohne deine Unterstützung, deine Liebe und deinen Glauben an mich wäre ich im Leben nicht da wo ich heute bin – Danke dafür!

Mein weiterer Dank geht an meine Familie und meine Freunde. Danke, dass Ihr immer für mich da seid und Euch stetig darum bemüht, mich auch mal auf andere Gedanken zu bringen.

Vielen lieben Dank auch an meinen Betreuer für Ideen, Ratschläge und Feedback und dass ich von Ihrem großen Fachwissen im Bereich der EU-DSGVO profitieren durfte. Danke ebenso der Studiengangs-Betreuung für immer prompte, verlässliche und freundliche Unterstützung bei kleinen und größeren Herausforderungen aller Art, sei es organisatorischer aber auch inhaltlicher Natur.

Ein großer Dank gilt meinem Arbeitgeber, vor allem für viel Flexibilität, was ich sehr zu schätzen weiß.

Herzlichen Dank an meine Interviewpartner! Ich habe mich sehr über Ihr Interesse und über Ihr Engagement gefreut. Schön, dass Sie dieses Thema so interessant finden wie ich. Ich würde mich freuen, wenn wir dazu weiterhin in Kontakt blieben.

Und ich möchte auch meinen Studienkollegen danken. Dafür, dass wir so eine gute Zeit miteinander hatten und uns gegenseitig motiviert haben, auch wenn wir wussten, dass Freunde und Familie ihre Freizeit am Wochenende gerade ohne uns genießen mussten und es für uns am Montag gleich wieder ins Büro ging.

Vielen Dank an Euch alle – ohne Euch würde diese Arbeit nicht existieren!

Kurzbeschreibung

Die EU-Datenschutz-Grundverordnung ist derzeit ein viel diskutiertes Thema. In erster Linie deshalb, weil ab 25.05.2018 die Strafen für Datenschutzverletzungen exorbitant erhöht werden. Bei Verstößen ist, je nach Vergehen, mit Geldbußen von bis zu € 10 Mio. oder € 20 Mio. bzw. 2% oder 4% des internationalen Konzernumsatzes des Vorjahres zu rechnen.

Das Gesundheitswesen ist von der EU-DSGVO besonders betroffen. Ein Großteil der Verarbeitungstätigkeiten betrifft personenbezogene Daten und zwar Gesundheitsdaten, die im Sinne der EU-DSGVO nach Artikel 9 unter „besondere Kategorien personenbezogener Daten“ fallen, was umfangreiche technische und organisatorische Herausforderungen zur Erfüllung der EU-DSGVO-Compliance mit sich bringt. Beim stetigen Kostendruck in diesem Sektor ist dies keine einfache Aufgabe und eine gewisse Rechtsunsicherheit verkompliziert dies zusätzlich.

In dieser Arbeit werden die angesprochenen Herausforderungen untersucht und es wird betrachtet, ob die Unternehmen, neben der Vermeidung des Strafrisikos, weitere Chancen aus der EU-DSGVO-Compliance heraus erkennen konnten. Weiters ist von Interesse, ob für diese Chancen eine monetäre Nutzenbewertung durchgeführt wird bzw. ob Kosten und Nutzen im Sinne einer Wirtschaftlichkeitsbetrachtung gegenübergestellt werden.

Diese Fragestellungen wurden im Rahmen einer empirischen Untersuchung mit sieben Experten beleuchtet. Die Experteninterviews wurden anschließend einer qualitativen Inhaltsanalyse unterzogen. Im Ergebnis zeigt sich, dass die Unternehmen sich auf die Vermeidung der Strafen konzentrierten und bisher keine bahnbrechenden weiteren Chancen erkennen konnten. Auch eine monetäre Nutzenbewertung bzw. Wirtschaftlichkeitsbetrachtung im Zusammenhang mit der EU-DSGVO-Compliance wurde in der Praxis nicht durchgeführt.

Abstract

The European General Data Protection Regulation is much discussed in recent days. Primarily, because the penalties for data breaches will be raised exorbitantly from May 25, 2018. Offenses against the GDPR are punished with money sentences, depending on the type of offense, in the amount of € 10 m or € 20 m or 2% or 4% of the international group revenue of the last year.

The healthcare sector is particularly affected by the GDPR. A substantial part of the data processing activities concerns personal health data. They are covered by Article 9 GDPR as “special categories of personal data”. Thus, fulfilling the GDPR requirements, causes many technical and organizational challenges. This is no easy task, considering that the healthcare sector is under constant cost pressure, and legal uncertainty complicates the issue.

This study draws attention to mentioned challenges and to the question, if companies are only focused on avoiding penalties or if they can find additional opportunities out of the GDPR-Compliance. There is further interest, whether a monetary assessment of the benefits of these chances was conducted, and whether costs and benefits were compared regarding a profitability assessment.

These questions were analyzed in an empirical study with seven experts. With the help of methods of qualitative content analysis, the expert interviews were examined. The outcome shows that companies have focused on the avoidance of sentencing and that they have not yet determined any additional chances. In practice, no monetary assessments of the benefits and no profitability assessments have been conducted regarding GDPR-Compliance.

Inhaltsverzeichnis

DANKSAGUNG ..... **I**

KURZBESCHREIBUNG ..... **II**

ABSTRACT ..... **III**

INHALTSVERZEICHNIS ..... **IV**

VERZEICHNIS FÜR ABBILDUNGEN ..... **VII**

VERZEICHNIS FÜR TABELLEN ..... **VIII**

VERZEICHNIS FÜR ABKÜRZUNGEN ..... **IX**

EXECUTIVE SUMMARY ..... **X**

1. EINLEITUNG **1**

1.1 AUSGANGSSITUATION UND PROBLEMSTELLUNG 1

1.2 ZIELSETZUNG UND FORSCHUNGSFRAGE 3

1.2.1 Abgrenzung der Arbeit *4*

1.3 METHODISCHE VORGEHENSWEISE 5

1.4 AUFBAU DER ARBEIT 6

1.4.1 Hinweis zur sprachlichen Gleichbehandlung *7*

2. BEGRIFFSDEFINITIONEN UND ZUSAMMENHÄNGE **8**

2.1 EINFÜHRUNG IN RELEVANTE EU-DSGVO BEGRIFFLICHKEITEN 8

2.1.1 Betroffene *8*

2.1.2 Sensible Daten *8*

2.1.3 Gesundheitsdaten *9*

2.1.4 Verantwortliche *9*

2.1.5 Auftragsverarbeiter *9*

2.2 ZWECK, ZIEL, ANWENDUNGSBEREICH UND STRAFAUSMAß DER EU-DSGVO 9

2.2.1 Zweck und Ziel der EU-DSGVO *10*

2.2.2 Anwendungsbereich der EU-DSGVO *14*

2.2.3 Strafausmaß *18*

2.3 BEGRIFFSDEFINITION UND ABGRENZUNG DER COMPLIANCE 20

2.3.1 Governance *20*

2.3.2 Compliance *22*

2.3.3 Einordnung des Datenschutzes im Rahmen der Compliance *23*

2.4 BEDEUTUNG VON COMPLIANCE IM GESUNDHEITSWESEN 24

2.5 DER NUTZEN VON COMPLIANCE 26

2.6 DIE KOSTEN VON COMPLIANCE 28

2.7 ERFOLGREICHE UMSETZUNG VON COMPLIANCE-VORHABEN 30

2.8 Erläuterung des Wirtschaftlichkeitsprinzips 31
2.9 Zusammenfassung 33

3. HERAUSFORDERUNGEN UND CHANCEN, KOSTEN UND NUTZEN 35

3.1 Herausforderungen 35
3.1.1 Datenschutzbeauftragter 37
3.1.2 Register der Verarbeitungstätigkeiten 39
3.1.3 Datenschutz-Folgeabschätzung / Privacy-Impact-Assessment 42
3.1.4 Erfüllung der Betroffenenrechte 44
3.1.5 Melden von Datenschutzvorfällen 49
3.1.6 Informationssicherheit nach dem Stand der Technik 51
3.1.7 Datenschutz durch Technikgestaltung und datenschutzfreundliche Vorsteinstellungen 56
3.2 Kosten und Budgets 58
3.3 Chancen und Nutzen 60
3.3.1 Vermeidung von Strafen 61
3.3.2 Hebung weiterer Chancen aus der Erfüllung der EU-DSGVO 62
3.4 Zusammenfassung 66

4. EMPIRISCHER FORSCHUNGSTEIL 68

4.1 Der empirische Forschungsprozess 68
4.2 Das Experteninterview 69
4.2.1 Interviewleitfaden 71
4.2.2 Datenquelle 74
4.3 Die qualitative Inhaltsanalyse 79

5. ERGEBNISSE 82

5.1 Darstellung und Interpretation der Ergebnisse 82
5.1.1 Kategorie „Rahmenbedingungen“ 82
5.1.2 Kategorie „Herausforderungen“ 89
5.1.3 Kategorie „Budget“ 96
5.1.4 Kategorie „Chancen“ 99
5.1.5 Kategorie „Nutzen“ 102
5.1.6 Kategorie „Wirtschaftlichkeit“ 104
5.2 Erkannte mögliche Korrelationen 106
5.2.1 Korrelation Management-Awareness und Management-Commitment 106
5.2.2 Korrelation Strafausmaß und Commitment 106

6. FAZIT 108

6.1 Zusammenfassung 108
6.2 Ausblick und persönliche Meinung 110
6.3 Beitrag der Arbeit und mögliche weiterführende Forschungen 112

7. LITERATUR 113

7.1 Selbstständige Werke 113

7.2 BEITRÄGEN IN SAMMEL- UND NACHSCHLAGEWERKEN 114
7.3 AUFSÄTZE IN ZEITSCHRIFTEN 116
7.4 INTERNET-QUELLEN 117
7.5 RECHTSQUELLEN 120

Verzeichnis für Abbildungen

ABBILDUNG 1: DIE QUELLEN DER COMPLIANCE 22
ABBILDUNG 2: IT-GESTÜTZTE COMPLIANCE VS. IT-COMPLIANCE....24
ABBILDUNG 3: IT-COMPLIANCE WIRKT AUF LEISTUNGSFÄHIGKEIT....29
ABBILDUNG 4: EINFLUSS DER IT-COMPLIANCE AUF WERTBEITRAG DER IT 29
ABBILDUNG 5: DIE GRÖßTEN SCHWACHSTELLEN IN DER DATENSICHERHEIT....55
ABBILDUNG 6: DIE TOP-BEDENKEN IM BERIECH INFORMATIONSSICHERHEIT 55
ABBILDUNG 7: DAS JÄHRLICHE BUDGET UM DIE ÄNDERUNGEN DER REGULATORISCHEN ANFORDERUNGEN ZU ADRESSIEREN....59
ABBILDUNG 8: ZEITPUNKT DER BUDGETENTSCHEIDUNGEN BZGL. DER REGULATORISCHEN ÄNDERUNGEN 60
ABBILDUNG 9: ABLAUFMODELL ZUSAMMENFASSENDER INHALTSANALYSE....80

Verzeichnis für Tabellen

TABELLE 1: ANGABEN ZUM INTERVIEWPARTNER 76
TABELLE 2: ANGABEN ZUM BETREFFENDEN UNTERNEHMEN DER INTERVIEWPARTNER 78
TABELLE 3: ANGABEN ZU DEN BETREFFENDEN EU-DSGVO PROJEKTEN DER JEWEILIGEN UNTERNEHMEN 79
TABELLE 4: KONNEX ZWISCHEN DEM KATEGORIENSYSTEM UND DEN SUBFORSCHUNGSFRAGEN 81
TABELLE 5: VARIABLEN DER KATEGORIE "RAHMENBEDINGUNGEN" 82
TABELLE 6: BEWERTUNG DER ERFOLGSKRITERIEN FÜR ERFOLGREICHE COMPLIANCE-EINFÜHRUNGEN AN DEN 7 EXPERTENINTERVIEWS 89
TABELLE 7: VARIABLEN DER KATEGORIE "HERAUSFORDERUNGEN" 90
TABELLE 8: TECHNISCHE HERAUSFORDERUNGEN LAUT DER INTERVIEWPARTNER 90
TABELLE 9: ORGANISATORISCHE HERAUSFORDERUNGEN LAUT DER INTERVIEWPARTNER 91
TABELLE 10: DIE DREI GRÖßTEN HERAUSFORDERUNGEN 93
TABELLE 11: VARIABLEN DER KATEGORIE "BUDGET" 96
TABELLE 12: AUFGETRETENE MERKMALAUSPRÄGUNGEN ZUM BUDGETRAHMEN 97
TABELLE 13: VARIABLEN DER KATEGORIE "CHANCEN" 99
TABELLE 14: VARIABLEN DER KATEGORIE "NUTZEN" 103
TABELLE 15: VARIABLEN DER KATEGORIE "WIRTSCHAFTLICHKEIT" 104

Verzeichnis für Abkürzungen

DSMS	Datenschutz-Management-System
EU-DSGVO	Europäische Datenschutz-Grundverordnung
HIPPA	Health Insurance Portability and Accountability Act
ISMS	Informationssicherheits-Management-System
KIS	Krankenhausinformationssystem
OGD	Open Government Data
PIA	Privacy Impact Assessment
PET	Privacy-Enhancing-Technologie
TOM	technische und organisatorische Maßnahmen

Executive Summary

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) regelt EU-weit die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen, wobei persönliche Daten jegliche Informationen bezogen auf eine Person umfassen. Anwendbar ist die EU-DSGVO ab dem 25. Mai 2018. Bis dahin müssen alle Datenanwendungen in den Unternehmen an die neue Rechtslage angepasst werden. Die neue Grundverordnung ist vor allem deshalb ein viel diskutiertes Thema, weil ab dem gesetzlichen Stichtag die Strafen für Datenschutzverletzungen exorbitant erhöht werden. Bei Verstößen sind zukünftig, je nach Vergehen, Geldbußen von bis zu € 10 Mio. oder € 20 Mio. bzw. 2% oder 4% des internationalen Konzernumsatzes des Vorjahres nicht ausschließbar.

Die mit der EU-DSGVO verbundenen Herausforderungen für österreichische Unternehmen sind seit Juni 2017 bekannt, da der österreichische Gesetzgeber zu diesem Zeitpunkt das korrespondierende Datenschutz-Anpassungsgesetz 2018 verabschiedet hat. Auf diese vermeidlich rechtssichere Situation haben viele Unternehmen gewartet, um ihre Vorhaben zur Herstellung der EU-DSGVO-Compliance zu starten. Neuerungen wie das Führen eines Verarbeitungsregisters, die Durchführung von Datenschutz-Folgeabschätzungen oder die Umsetzung der Anforderungen bzgl. des Rechts auf Vergessenwerden, stellen Herausforderungen im organisatorischen sowie technischen Sinne für Unternehmen dar. Das Gesundheitswesen ist von der EU-DSGVO besonders betroffen. Ein Großteil ihrer Verarbeitungstätigkeiten betreffen personenbezogene Daten und zwar Gesundheitsdaten, die im Sinne der EU-DSGVO nach Artikel 9 unter „besonderer Kategorien personenbezogener Daten“ fallen, weshalb umfangreiche technische und organisatorische Herausforderungen zur Erfüllung der EU-DSGVO-Compliance mit sich bringt. Beim stetigen Kostendruck in diesem Sektor ist dies keine einfache Aufgabe und eine gewisse Rechtsunsicherheit verkompliziert dies zusätzlich.

Daher stellt sich die Frage, ob die Unternehmen neben der Vermeidung von Nachteilen, auch weitere Chancen aus der Herstellung der EU-DSGVO-Compliance erkennen können. Denn wenn ein zusätzlicher Nutzen generiert werden kann, der dazu beiträgt das Vorhaben kostendeckend umzusetzen, dann könnte sich das Vorhaben wirtschaftlich decken und damit, über die Vermeidung von Nachteilen hinaus, rechtfertigen lassen. Daher ist von

Interesse, ob die betroffenen Unternehmen weitere Chancen erkennen, ob sie diese einer monetären Nutzenbewertung unterziehen bzw. Kosten und Nutzen im Sinne einer Wirtschaftlichkeitsbetrachtung gegenüberstellen.

Die Forschungsfrage lautet daher wie folgt:
Welchen Herausforderungen und Chancen begegnen österreichische Verantwortliche und Auftragsverarbeiter im Sinne des Art. 4 EU-DSGVO in der stationären Krankenversorgung bei der Herbeiführung der EU-DSGVO-Compliance bis zum 25. Mai 2018 und wie werden die damit verbundenen Kosten und Nutzen im Sinne des Wirtschaftlichkeitsprinzips gegenübergestellt?

In diesem Zusammenhang soll auf die folgenden Unterfragen zur Forschungsfrage eingegangen werden:

(1) Wie stellen Unternehmen mit Verantwortung für Gesundheitsdaten aus der österreichischen stationären Krankenversorgung die erfolgreiche Umsetzung eines Vorhabens zur Erfüllung der EU-DSGVO-Compliance bis Mai 2018 sicher?
(2) Welchen technischen und organisatorischen Herausforderungen begegnen diese Unternehmen dabei?
(3) Welchen Aufwand kalkulieren die untersuchten Unternehmen um den Herausforderungen gerecht zu werden?
(4) Liegt der Nutzen in der Herbeiführung der EU-DSGVO-Compliance nur in der Vermeidung von Nachteilen aus Datenschutzverletzungen oder erkennen die untersuchten Unternehmen weitere Chancen?
(5) Wie planen die untersuchten Unternehmen den erkannten Nutzen zu realisieren und kann der erkannte Nutzen die entstehenden Aufwände decken?
(6) Versuchen die untersuchten Unternehmen einen wirtschaftlichen Mehrwert dabei zu generieren, sollen rein die Kosten gedeckt werden oder wird dies nicht betrachtet?

Um dieses Thema zu bearbeiten wurde zuerst eine Literaturrecherche und eine Studie der EU-DSGVO durchgeführt. Es wurden die gesetzlichen Grundlagen aufgearbeitet, sowie theoretische Konzepte zu den Themen Compliance und Wirtschaftlichkeit bearbeitet. Anschließend wurden die technischen und organisatorischen Herausforderungen aus der EU-DSGVO-Compliance heraus erarbeitet, eine Studie zu den anberaumten Budgets zur Herstellung der EU-DSGVO-Compliance aufgearbeitet und vorhersehbare Chancen laut

Literatur erläutert. Dabei bestand das Bemühen den Konnex zum Gesundheitswesen jeweils herzustellen.

Anschließend wurden aus den Sub-Forschungsfragen sowie anhand der Erkenntnisse aus der literarischen Aufarbeitung, Fragen für einen Interviewleitfaden zur Durchführung von Experteninterviews erarbeitet. Diese Fragestellungen wurden im Rahmen einer empirischen Untersuchung mit sieben Experten beleuchtet. Dabei wurden die Interviewpartner so ausgewählt, dass diese Expertise im Umgang mit Gesundheitsdaten im Sinne der Verarbeitung und Verantwortung mitbrachten. Dazu fanden sich Experten die als Berater, Verantwortliche und/oder Auftragsverarbeiter für den stationären Bereich des Gesundheitswesens tätig sind. Die Experteninterviews wurden anschließend einer qualitativen Inhaltsanalyse unterzogen.

Im Ergebnis zeigt sich, dass bei sechs von sieben Unternehmen ein volles Management-Commitment zur Erreichung der EU-DSGVO-Compliance zu verzeichnen ist und dass in der Regel ein angemessenes Budget zur Umsetzung des Vorhabens zur Verfügung gestellt wird. Die Analyseergebnisse deuten darauf hin, dass die Begründung dafür im hohen drohenden Strafausmaß liegt. Daher fokussieren die Unternehmen sich auch auf die Vermeidung der Nachteile, vor allem der Strafen, aber auch des Imageverlustes. Weitere Chancen konnten in den Interviews zwar erkannt werden, aber kein Interviewpartner konnte bahnbrechende Erkenntnisse nennen. Auch eine monetäre Nutzenbewertung bzw. eine Wirtschaftlichkeitsbetrachtung im Zusammenhang mit der EU-DSGVO-Compliance wird in der Praxis nicht durchgeführt.

Deutlich erkennbar ist, dass es viel Ungewissheit und Unsicherheiten bzgl. der Auslegung der EU-DSGVO gibt. Zentrale Vorgaben und klare Handlungsempfehlungen fehlen den Unternehmen. Dies geht so weit, dass Projektziele nicht klar formuliert werden und folglich Unklarheit darüber herrscht, wann sie erfüllt sind bzw. wie man den Nachweis für die Wirksamkeit ergriffener Maßnahmen erbringen kann.

Viele Herausforderungen sowohl im technischen als auch organisatorischen Themenbereichen wurden in der Literatur erkannt und in den Interviews genannt. Im Ergebnis zeigt sich aber, dass sich viele der vom Interview betroffenen Unternehmen noch in frühen Phasen der Umsetzungsvorhaben zur Herstellung der EU-DSGVO-Compliance befinden. Es war daher ersichtlich, dass die Experten dazu, abhängig von der jeweiligen Projektphase

einen unterschiedlichen Erkenntnisstand hatten. Eine besondere Herausforderung nannten aber fünf von sieben Experten, nämlich die technische Umsetzung des Rechts auf Vergessenwerden.

Es bleibt daher zu hoffen, dass die EU-DSGVO auch im Gesundheitswesen dennoch Vorteile mit sich bringen wird. Mancher Experte deutete in den Interviews bereits an, dass davon ausgehen ist, dass in einem zweiten Schritt mit der Generierung eines zusätzlichen Nutzens zu rechnen ist. Jetzt liegt der Fokus der Unternehmen aber klar darauf Schaden zu vermeiden und die Kosten dafür werden in Kauf genommen.

1. Einleitung

Im Folgenden wird die Ausgangssituation und Problemstellung erklärt, die zur Stellung der Forschungsfrage als Basis dieser Arbeit diente. Weiters werden das methodische Vorgehen im Zuge der Arbeit sowie der Aufbau der Arbeit erläutert.

1.1 Ausgangssituation und Problemstellung

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) ist am 14. April 2016 durch das EU-Parlament beschlossen und am 04. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht worden. Sie regelt EU-weit die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen, wobei persönliche Daten jegliche Informationen bezogen auf eine Person umfassen. Es spielt dabei keine Rolle ob sich diese Daten auf das private, berufliche oder öffentliche Leben der Person beziehen. Anwendbar ist die EU-DSGVO ab dem 25. Mai 2018. Bis dahin müssen alle Datenanwendungen in den EU-Mitgliedsstaaten an die neue Rechtslage angepasst werden sowie neue organisatorische Prozesse eingeführt werden.[1]

Die EU-DSGVO ist zwar als EU-Verordnung in jedem EU-Mitgliedstaat unmittelbar anwendbar, sie enthält jedoch zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume. Das ist auch der Grund weshalb sie als eine „hinkende Verordnung“ bezeichnet wird[2]. In Österreich wird diese Verordnung durch das Datenschutz-Anpassungsgesetz 2018 ausgestaltet. Das Vorliegen des geänderten österreichischen Datenschutzgesetzes unter Berücksichtigung der Datenschutz-Grundverordnung wird die konkrete Gesetzeslage ab 25. Mai 2018 bestimmen.[3] Das bisher gültige DSG 2000, das auf der EU-Datenschutzrichtlinie 95/46/EG (DSRL) basierte wird dadurch aufgehoben und durch das Datenschutz-Anpassungsgesetz 2018 ersetzt.

Die mit der EU-DSGVO verbundenen Herausforderungen, aber auch Chancen, für österreichische Unternehmen sind daher seit spätestens Juni 2017[4] bekannt. Auf diese ver-

[1] vgl Wirtschaftskammer Österreich (2017): EU-Datenschutz-Grundverordnung, Kurzüberblick und Zeitplan, https://www.wko.at/Content.Node/Service/Wirtschaftsrecht-und-Gewerberecht/Verwaltungs--und-Verfassungsrecht/Datenschutz/EU-Datenschutz-Grundverordnung.html, Abfragedatum 05.02.2017
[2] vgl Kastelitz, M. (2016a): Die Datenschutz-Grundverordnung im Gesundheitsbereich – ein erster Überblick, JMG 0-2016, S. 71
[3] vgl Wirtschaftskammer Österreich (2017)
[4] Verabschiedung des Datenschutz-Anpassungsgesetzes 2018 mit 29. Juni 2017 im Nationalrat

meidlich rechtssichere Situation haben viele Unternehmen gewartet, um ihre Vorhaben zur Erfüllung der EU-DSGVO-Compliance umzusetzen. Neuerungen wie das Führen eines Verarbeitungsregisters, die Durchführung von Datenschutz-Folgeabschätzungen oder die Umsetzung der Anforderungen bzgl. des Rechts auf Vergessenwerden, stellen Herausforderungen im organisatorischen sowie technischen Sinne an Unternehmen dar, vor allem da das Strafausmaß bei Datenschutzverletzungen durch die EU-DSGVO dramatisch ansteigen wird. Strafen können zukünftig bis max. EUR 20 Mio. oder 4% des globalen Konzernumsatzes betragen. Dies gilt sowohl für Klein-/Kleinstunternehmer als auch international agierende Konzerne.[5]

Im Zuge der Schaffung technischer und organisatorischer Voraussetzungen zur Erfüllung der Vorgaben der EU-DSGVO ergeben sich vielleicht auch neu erkannte Chancen für die Unternehmen. Es ist zu erwarten, dass Missstände in Systemen, Prozessen und Daten erkannt und behoben werden, ein besserer Überblick über alle zum Kunden bzw. Mitarbeiter gespeicherten Daten entsteht und auch die Weichen für erfolgreiche Digitalisierungsvorhaben zielgerichteter gestellt werden können. Im Kontext der Digitalisierung ergeben sich auch aus Schlagworten wie Big Data, Profiling und Open Data sowie damit verbundenen Geschäftsmodellen Fragen an die Begünstigung oder Benachteiligung dieser Themen durch die EU-DSGVO.

In dem verbleibenden Jahr gilt es daher für betroffene österreichische Unternehmen, viele Vorkehrungen zu treffen. Vor allem im Gesundheitswesen wird eine Vielzahl an sensiblen, personenbezogenen Daten verarbeitet. Die Prozesse, Datenflüsse und IT-Architekturen in Gesundheitseinrichtungen, vor allem im Bereich der stationären Krankenversorgung, weisen häufig einen hohen Komplexitätsgrad auf. Es wird für Unternehmen im Gesundheitswesen, sowohl für Verantwortliche als auch für Auftragsverarbeiter im Sinne des Art. 4 EU-DSGVO, daher eine besondere Herausforderung darstellen, organisatorisch sowie technisch den Anforderungen der EU-DSGVO bis Mai 2018 gerecht zu werden. Dies wird auch mit beachtlichen Kosten verbunden sein. Budgets von bis zu € 500.000, -- sind nicht unüblich, wie Studien und auch Interviews zu dieser Arbeit bestätigten.

[5] vgl Knyrim, R., Trieb, G. (2014): Das künftige EU-Datenschutzrecht / Neue Anforderungen an die unternehmerische Compliance, http://www.preslmayr.at/tl_files/Publikationen/2014/Das%20kuenftige%20EU-Datenschutzrecht%20-%20Neue%20Anforderungen%20an%20die%20unternehmerische%20Compliance_Knyrim_Trieb.pdf, Abfragedatum 05.02.2017

Wirtschaftlich agierende Unternehmen stellen den Wertbeitrag eines Vorhabens wie diesem in der Regel seinen Kosten gegenüber. Dem ökonomischen Grundsatz folgend sind Unternehmen bemüht ein bestimmtes Ergebnis mit dem geringstmöglichen Mitteleinsatz (Minimalprinzip) bzw. mit einem bestimmten Mitteleinsatz den größtmöglichen Erfolg (Maximalprinzip) zu erzielen oder einen optimalen Weg daraus zu erarbeiten (Optimalprinzip)[6].

In dieser Arbeit wird die Fragestellung behandelt, ob sich die betroffenen Unternehmen im Untersuchungsbereich mit den mit der EU-DSGVO-Compliance verbundenen Chancen und Nutzen auseinandersetzen oder ob der einzige Nutzen in der Vermeidung von Risiken, wie Strafen oder Reputationsverlusten, verstanden wird. Weiters stellt sich die Frage, welche Kosten durch das Meistern der neuen Herausforderungen anfallen werden und ob der jeweils erkannte Nutzen die Aufwände rechtfertigt. Und ob die EU-DSGVO-Compliance bei Unternehmen im Untersuchungsbereich nach Wirtschaftlichkeitsaspekten betrachtet herbeigeführt wird.

1.2 Zielsetzung und Forschungsfrage

Aus der beschriebenen Ausgangssituation und Problemstellung abgeleitet soll es Ziel dieser Arbeit sein, die Herausforderungen und Chancen sowie damit verbunden die Kosten und den Nutzen im Rahmen der Herbeiführung einer EU-DSGVO-Compliance im Bereich der stationären österreichischen Krankenversorgung zu erheben. Weiters ist zu analysieren, ob diese Betriebe dabei anstreben einen wirtschaftlichen Mehrwert zu generieren oder nur versuchen das notwendige Maß an Compliance herbeizuführen, um das Risiko einer drohenden Strafe größtmöglich zu reduzieren. Die Master‘s Thesis beschäftigt sich daher mit der Beantwortung folgender Forschungsfrage:

Welchen Herausforderungen und Chancen begegnen österreichische Verantwortliche und Auftragsverarbeiter im Sinne des Art. 4 EU-DSGVO in der stationären Krankenversorgung bei der Herbeiführung der EU-DSGVO-Compliance bis zum 25. Mai 2018 und wie werden die damit verbundenen Kosten und Nutzen im Sinne des Wirtschaftlichkeitsprinzips gegenübergestellt?

In diesem Zusammenhang soll auf die folgenden Unterfragen zur Forschungsfrage eingegangen werden:

[6] vgl Gabler Wirtschaftslexikon (2017c): Wirtschaftlichkeitsprinzip, http://wirtschaftslexikon.gabler.de/Definition/wirtschaftlichkeitsprinzip.html, Abfragedatum 21.05.2017

(1) Wie stellen Unternehmen mit Verantwortung für Gesundheitsdaten aus der österreichischen stationären Krankenversorgung die erfolgreiche Umsetzung eines Vorhabens zur Erfüllung der EU-DSGVO-Compliance bis Mai 2018 sicher?
(2) Welchen technischen und organisatorischen Herausforderungen begegnen diese Unternehmen dabei?
(3) Welchen Aufwand kalkulieren die untersuchten Unternehmen um den Herausforderungen gerecht zu werden?
(4) Liegt der Nutzen in der Herbeiführung der EU-DSGVO-Compliance nur in der Vermeidung von Nachteilen aus Datenschutzverletzungen oder erkennen die untersuchten Unternehmen weitere Chancen?
(5) Wie planen die untersuchten Unternehmen den erkannten Nutzen zu realisieren und kann der erkannte Nutzen die entstehenden Aufwände decken?
(6) Versuchen die untersuchten Unternehmen einen wirtschaftlichen Mehrwert dabei zu generieren, sollen rein die Kosten gedeckt werden oder wird dies nicht betrachtet?

1.2.1 Abgrenzung der Arbeit

Da vorausgehend die Zielsetzung der Arbeit erklärt wurde, soll an dieser Stelle auch abgegrenzt werden womit sich die Arbeit aus welchem Grund nicht beschäftigt:

(1) Stationäre vs. nicht stationäre Krankenversorgung

Der Fokus der Arbeit wird auf den Bereich der stationären Krankenversorgung eingeschränkt, weil bei Unternehmen aus dem nicht stationären Bereich, wie z.B. bei niedergelassen Ärzten davon auszugehen ist, dass diese aufgrund ihrer Größe (Einzelpersonen oder kleine gemeinschaftlich geführte Arztpraxen) mit anders gelagerten, vor allem organisatorischen Problemen konfrontiert sind. So wie sich beispielsweise auch die Aufbewahrungsfristen für personenbezogene Daten im stationären Bereich von denen im ambulanten Bereich unterscheiden, was daher auch zu anderen Herausforderungen in der Behandlung dieser Daten führt.

(2) Das österreichische Datenschutz-Anpassungsgesetz 2018

Zu jenem Zeitpunkt als das Thema der Arbeit eingereicht wurde war noch nicht absehbar, ob der österreichische Nationalrat das Datenschutz-Anpassungsgesetz 2018 noch vor der parlamentarischen Sommerpause 2017 beschließen wird. Der Fokus der Arbeit wurde daher auf die EU-DSGVO als europäische Grundverordnung, anstatt auf das Datenschutz-Anpassungsgesetzt 2018, als korrespondierende nationale Norm gelegt.

(3) Regelungen zur internationalen Datenübermittlung bzw. zu Aufsichtsbehörden

Regelungen dieser Art werden auch in der EU-DSGVO behandelt. Da es in der Bearbeitung des Themas weder bei der theoriegeleiten Grundlagenforschung noch im Rahmen der Empirie Berührungspunkte gab wurde in weiterer Folge nicht vertiefend darauf eingegangen. Es ist auch nicht Ziel der Arbeit eine vollständige Beleuchtung der EU-DSGVO Regelungen durchzuführen, sondern die Chancen und Herausforderungen daraus, die das österreichische Gesundheitswesen derzeit maßgeblich beschäftigen, zu thematisieren.

1.3 Methodische Vorgehensweise

Über eine Literaturrecherche bzw. auf Basis der vorliegenden Gesetzestexte wurden Begriffsdefinitionen und –erläuterungen, sowie Abgrenzungen von Anwendungsbereichen vorgenommen. Ebenso wurden die Themen Kosten und Nutzen von Compliance sowie die Aspekte der Wirtschaftlichkeit anhand von Literatur erarbeitet. Weiters wurden Zweck, Ziel und Anwendungsbereich der EU-DSGVO analysiert und die Neuerungen durch die EU-DSGVO, in Form technischer sowie organisatorischer Vorgaben bzw. Herausforderungen und vorhersehbare Chancen und benötigtes Budget über Literatur und Studien erklärt.

Weiters wurden Methoden der qualitativen Sozialforschung angewandt. Dabei wurden Experteninterviews (Leitfadeninterviews) mit Verantwortlichen aus dem österreichischen Gesundheitswesen mit Verantwortung über personenbezogene Daten aus dem stationären Gesundheitswesen aus den Bereichen Gesundheitsbetreiber/Krankenhausträger, Sozialversicherung, Lehre und Forschung, IT-Dienstleistung sowie einer Vertreterin aus der Rechtsberatung geführt. Dabei wurden die Rahmenbedingungen zu EU-DSGVO-Compliance-Vorhaben, erkannte Herausforderungen und Aufwände sowie Chancen und Nutzen diskutiert und aus den Umsetzungsprojekten zur EU-DSGVO-Compliance aus Perspektive der Praktiker beleuchtet. Weiters haben die Interviewpartner Ihren Eindruck über die wirtschaftliche Handhabung des Themas in ihrer Organisation bzw. bei ihren Klienten erläutert. Anschließend wurde eine qualitative Inhaltsanalyse nach Mayring durchgeführt um die Ergebnisse zu erheben und zu interpretieren.

Die Ergebnisse der Arbeit basieren somit auf der Analyse von Gesetzestexten, Literaturrecherchen, Studien sowie Experteninterviews und deren qualitative Inhaltsanalyse bzw. folglich der Interpretation der Ergebnisse.

1.4 Aufbau der Arbeit

Im Einleitungskapitel wird die Relevanz des Themas hervorgehoben und die Forschungsfrage erläutert, sowie die Vorgehensweise in der Bearbeitung und Beantwortung der Forschungsfrage erklärt.

Im zweiten Kapitel werden die zentralen Begriffe und ihre Verwendung im Rahmen der Arbeit für die theoretischen Grundlagen erklärt. Neben Zweck, Zielsetzung und Anwendungsbereich der EU-DSGVO wird auch auf das Strafausmaß bei Datenschutzverletzungen eingegangen. Dies führt zur Erklärung und Abgrenzung des Begriffs Compliance und zur Evaluierung des Nutzens von Compliance und dem Stellenwert von Compliance im Gesundheitswesen. Weiters wird auf das Wirtschaftlichkeitsprinzip und damit verbunden die Gegenüberstellung von Kosten und Nutzen eingegangen und auf die Thematik von Wirtschaftlichkeit im Sinne der EU-DSGVO-Compliance hingeführt.

Im dritten Kapitel wird auf Herausforderungen und Kosten bzw. Chancen und Nutzen, im Zuge der Umsetzung der EU-DSGVO-Compliance eingegangen. Dazu werden zuerst die organisatorischen und technischen Anforderungen, die die EU-DSGVO mit sich bringt erläutert. Dies betrifft Themen, wie der Einführung und Ausgestaltung der Rolle des Datenschutzbeauftragten, dem Aufbau von zentralen Verarbeitungsregistern und der Durchführung von Datenschutz-Folgeabschätzungen u.v.m. Weiters sind die technischen Herausforderungen von Bedeutung, z.B. mit welchem technischen Sicherheitsniveau die untersuchten Betriebe im Gesundheitswesen in die Projekte hineingehen und was nachzuholen ist. Weiters soll erklärt werden, welche Herausforderungen Neuerungen wie Privacy-by-Design und Privacy-by-Default an die Unternehmen stellen.
Auf Basis aktueller Studien soll ermittelt werden, welche Budgets Unternehmen für derartige Projekte in der Regel zur Verfügung stellen.
Weiters wird in diesem Kapitel auch erklärt, welche denkbaren Chancen durch die Schaffung der Voraussetzungen über die Umsetzung der Anforderungen laut EU-DSGVO sich für Unternehmen, die Daten im Gesundheitswesen verantworten, ergeben können. Denn durch die Konsolidierung von Daten, sowie die technischen Errungenschaften im Bereich von Big Data Analysen und Profiling ergeben sich neue Möglichkeiten. Auch das Schlagwort „Open Data“ im Zusammenhang mit dem zur Verfügung stellen von Behandlungsergebnissen im gemeinnützigen Sinne ist eine weitere Chance für Entwicklung im Gesundheitswesen.

Andererseits wird in diesem Abschnitt der Arbeit auch auf den Nutzen einer Risikoreduktion hinsichtlich des Eintretens einer Datenschutzverletzung und der damit zusammenhängenden Vermeidung von Risiken, wie Strafen und Reputationsschäden, eingegangen.

Im Kapitel 4 wird erläutert wie der empirische Teil dieser Arbeit durchgeführt wird. Es wird die verwendete Erhebungs- und Auswertungsmethode erläutert sowie das Untersuchungsdesign und die ausgewählten Untersuchungsteilnehmer beschrieben.

Im Kapitel 5 werden dann die Ergebnisse der empirischen Untersuchung präsentiert und interpretiert.

Im abschließenden 6. Kapitel erfolgt dann eine Zusammenfassung, in der die Beantwortung der Forschungsfrage sowie der sinnstiftende Zweck dieser Arbeit dargestellt wird. Hier sind auch persönliche Bemerkungen und ein Ausblick zu finden.

1.4.1 Hinweis zur sprachlichen Gleichbehandlung

Aus Gründen der besseren Lesbarkeit wird in dieser Arbeit auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Begriffe gelten gleichermaßen für beiderlei Geschlecht.

2. Begriffsdefinitionen und Zusammenhänge

In diesem Kapitel sollen die zentralen Begriffe und ihre Verwendung im Rahmen dieser Arbeit für die theoretischen Grundlagen erläutert werden. Neben Zweck, Zielsetzung und Anwendungsbereich der EU-DSGVO wird auch auf das Strafausmaß bei Datenschutzverletzungen eingegangen. Dies führt weiter zur Erklärung und Abgrenzung des Begriffs Compliance, des Stellenwerts von Compliance im Gesundheitswesen und zur Evaluierung des Nutzens sowie der Kosten von Compliance. Anschließend wird auf das Wirtschaftlichkeitsprinzip und damit verbunden die Gegenüberstellung von Kosten und Nutzen eingegangen und auf die Thematik von Wirtschaftlichkeit im Sinne der EU-DSGVO-Compliance hingeführt.

2.1 Einführung in relevante EU-DSGVO Begrifflichkeiten

Bevor im Detail darauf eingegangen werden kann, welchen Sinn und Zweck die Verordnung verfolgt, müssen in diesem Zusammenhang relevante Begriffe erläutert werden:

2.1.1 Betroffene

Der Betroffene (oder auch, die betroffene Person) ist im Sinne der Verordnung eine identifizierte oder identifizierbare natürliche Person.[7] Wann eine Person als identifizierbar gilt wird im Kapitel 2.2.2 Anwendungsbereich der EU-DSGVO noch genauer erläutert.

2.1.2 Sensible Daten

Im Art. 9 EU-DSGVO wird die „Verarbeitung besonderer Kategorien personenbezogener Daten“ erläutert, welche auch als „sensible Daten“[8] bezeichnet werden.[9] Art. 9 Abs. 1 EU-DSGVO zählt auf, welche Datenarten konkret darunter verstanden werden: rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Gesundheitsdaten, das Sexualleben oder die sexuelle Orientierung betreffende Daten.[10]

[7] vgl Feiler, L., Forgó, N. (2017): EU-DSGVO: EU-Datenschutz-Grundverordnung, Wien, Verlag Österreich, S. 3
[8] Synonyme Verwendung im Erwägungsgrund Nr. 10 zur EU-DSGVO in: Pollirer, H.-J., Weiss, E., Knyrim, R., Haidinger, V. (Hrsg) (2017): DSGVO: Datenschutz-Grundverordnung, Wien, Manz, S.4
[9] vgl Bergauer, C. (2016): Personenbezogene Daten: Begriff und Kategorien, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S.56
[10] vgl VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 2016/119, S. 38, vgl Feiler, L., Forgó, N. (2017), S.3

Auch jene Daten die zur Identifizierung eines Betroffen verwendet und verarbeitet werden, wie die Sozialversicherungsnummer oder biometrische Daten wie z.B. Fingerabdrücke und Gesichtsbilder, zählen zu den sensiblen Daten.[11]

2.1.3 Gesundheitsdaten

Gesundheitsdaten, welche zu den sensiblen Daten zählen, werden im Art. 4 Z. 15 definiert. Sie beziehen sich auf die körperliche und geistige Gesundheit einer natürlichen Person. Dies schließt auch die Erbringung von Gesundheitsdienstleistungen mit ein, wenn daraus Informationen über den Gesundheitszustand ableitbar sind.[12]

2.1.4 Verantwortliche

Der Verantwortliche im Sinne der Verordnung, ist die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle. Den Verantwortlichen zeichnet aus, dass er alleine oder auch gemeinsam mit anderen (dies erklärt den ebenso verwendeten Begriff der „gemeinsam Verantwortlichen"; man nennt dies auch pluralistische Kontrolle) über Zweck und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[13]

2.1.5 Auftragsverarbeiter

Der Auftragsverarbeiter im Sinne der Verordnung, ist die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet. Charakteristisch ist dabei, dass der Auftragsverarbeiter nicht selbst über den Zweck und die Mittel der Datenverarbeitung entscheidet, denn er führt die Datenverarbeitung im Auftrag des Verantwortlichen durch.[14]

2.2 Zweck, Ziel, Anwendungsbereich und Strafausmaß der EU-DSGVO

Im Folgenden soll vermittelt werden, welchen Zweck und welche Ziele die EU-DSGVO verfolgt und für wen, was und wo diese Verordnung Anwendung findet bzw. mit welchen Sanktionen bei Nichteinhaltung zu rechnen ist.

---

[11] vgl Feiler, L., Forgó, N. (2017), S. 3
[12] vgl VO (EU) 2016/679 ABl L 2016/119, S.34
[13] vgl Horn, B. (2016): Gemeinsam für die Verarbeitung Verantwortliche, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S.153,155, vgl Feiler, L., Forgó, N. (2017), S. 3
[14] vgl Bogendorfer, R.J. (2016): Der Dienstleister wird zum Auftragsverarbeiter: Und was ändert sich für Dienstleister mit der DSGVO noch?, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S.69f, vgl Feiler, L., Forgó, N. (2017), S. 3

2.2.1 Zweck und Ziel der EU-DSGVO

Der Gegenstand und das Ziel der EU-DSGVO werden dabei im Art. 1 dieser Verordnung definiert:

„(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.[15]“

Der Zweck die natürliche Person im Rahmen von Verarbeitungstätigkeiten hinsichtlich der Geheimhaltung ihrer personenbezogenen Daten und folglich ihrer Privatsphäre zu schützen, auch im Vergleich zum DSG 2000, ist nichts Neues. Um dem gerecht zu werden richtet sich die Verordnung mit Pflichten an den Verantwortlichen und den Auftragsverarbeiter. Dazu wurden Vorgaben für die rechtmäßige Verarbeitung personenbezogener Daten im Kapitel II, in Art. 5-11 der EU-DSGVO definiert. Dies teilt sich in die Grundsätze (Art. 5) sowie die Rechtmäßigkeit (Art. 6-11) der Verarbeitung.

Grundsätze der Verarbeitung personenbezogener Daten

Folgende Grundsätze, welche auch als „allgemeine Grundsätze“ bezeichnet werden, werden dabei im Allgemeinen in Art. 5 aufgezählt[16]:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a),
- Zweckbindung (Art. 5 Abs. 1 lit. b),
- Datenminimierung (Art. 5 Abs. 1 lit. c),
- Richtigkeit (Art. 5 Abs. 1 lit. d),
- Speicherbegrenzung (Art. 5 Abs. 1 lit. e),
- Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f),
- Rechenschaftspflicht (Art. 5 Abs. 2)

[15] vgl VO (EU) 2016/679 ABl L 2016/119, S.32

[16] vgl Kastelitz, M. (2016): Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 5-11 DSGVO), in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S.99f, vgl VO (EU) 2016/679 ABl L 2016/119, S.35f

In den Grundsätzen findet sich ebenfalls einiges Bekanntes, da diese Grundsätze auf dem Art. 6 Abs. 1 der DSRL aufbauen, der in Österreich im § 6 Abs. 1 des DSG 2000 Berücksichtigung findet. Tatsächlich neu dazugekommen sind der Grundsatz auf „Integrität und Vertraulichkeit“ sowie die „Rechenschaftspflicht“.[17]

Im Grundsatz der **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz** wird geregelt, dass eine rechtmäßige Datenverarbeitung nur auf der Basis einer zulässigen Rechtsgrundlage erfolgen darf, sofern eine ausreichende rechtliche Befugnis bzw. Zuständigkeit des Verantwortlichen für die Datennutzung gegeben ist. Unter „Treu und Glauben“ ist zu verstehen, dass es für den Betroffenen möglich ist in Erfahrung zu bringen, dass eine Verarbeitung seiner personenbezogenen Daten erfolgt und dass er der Form entsprechend über die Bedingungen der Erhebung informiert wird. Der Grundsatz der Transparenz, welcher in dieser Verordnung im Unterschied zur DSRL hinsichtlich seiner Begrifflichkeit neu hinzugefügt wurde, gibt dem Verantwortlichen vor, dass er dem Betroffenen leicht verständlich, leicht zugänglich und präzise erklärt Informationen über die Erhebung, hinsichtlich Art und Umfang, von personenbezogenen Daten des Betroffenen zur Verfügung stellen muss. Weiters muss auch die weitere Verwendung dieser Daten erklärt werden.[18]

Der Grundsatz der **Zweckbindung** besagt, dass eine eindeutige und möglichst genaue Festlegung des Zwecks der Datenerhebung notwendig ist. Weiters muss der Zweck legitim, also rechtmäßig sein. Abweichend vom ursprünglichen Zweck, darf eine Verarbeitung nur dann erfolgen, wenn eine Zustimmung eines Betroffenen vorliegt oder eine Weiterverarbeitung im öffentlichen Interesse für wissenschaftliche, historische oder statistische Zwecke gegeben ist, Unionsrecht oder nationales Recht dies erlauben oder ein durchzuführender „Kompatibilitätstest“ eine Vereinbarkeit bestätigt. Beim Kompatibilitätstest, werden die sogenannten fünf Kompatibilitätskriterien geprüft, die im Art. 6 Abs. 4 EU-DSGVO zu finden sind.[19]

Der Grundsatz der **Datenminimierung** fordert, dass die Verarbeitung der personenbezogenen Daten auf das notwendige Maß beschränkt sein muss. Weiters muss sie für den Zweck angemessen und erheblich sein.[20] In dieser Regelung spiegelt sich die daten-

[17] vgl Kastelitz, M. (2016), S. 104f
[18] vgl Kastelitz, M. (2016), S. 100f
[19] vgl Kastelitz, M. (2016), S. 101 u. 103
[20] vgl VO (EU) 2016/679 ABl L 2016/119, S.35

schutzrechtliche Ausgestaltung des allgemeinen Verhältnismäßigkeitsprinzips wieder. Würde man beispielsweise, um zu dokumentieren wie groß das Datenvolumen ist, das durch einen Mitarbeiter verbraucht wird, auch zusätzlich dokumentieren wann der Download der jeweiligen Dateien stattgefunden hat und wie die Benennung der Dateien lautete, dann wäre von einem Datenerhebungsexzess die Rede und das Verhältnismäßigkeitsprinzip verletzt.[21]

Die **Richtigkeit** bedeutet, dass personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen. Das bedeutet auch, dass diese Daten korrigiert oder unverzüglich gelöscht werden müssen, falls eine Unrichtigkeit erkannt wird.[22]

Die **Speicherbegrenzung** bedeutet, dass die personenbezogenen Daten nur solange in einer Form gespeichert werden dürfen, welche die Identifikation eines Betroffenen ermöglicht, solange eine Notwendigkeit basierend auf einer gesetzlichen Grundlage gegeben ist. Wenn die Frist abgelaufen ist, dann sind die Daten wieder zu löschen oder zu anonymisieren.[23] Der Sinn der Regelung ist der, dass Betroffene einen Anspruch geltend machen können, dass sie wünschen das betreffende Daten gelöscht werden müssen und daher nicht mehr zur Verwendung des Verantwortlichen zur Verfügung stehen, wenn die Verarbeitung nicht mehr aufgrund der Grundsätze der Rechtmäßigkeit und Zweckmäßigkeit der Verarbeitungstätigkeit entsprechend EU-DSGVO beruht. Nur wenn eine weitere Speicherung dieser Daten auf rechtlichen Verpflichtungen wie Aufbewahrungsdauern beruht, ist dies auch weiterhin gerechtfertigt.[24] Würde aber ein Unternehmer eine Dokumentation zu einem Vertrag mit einem Kunden über die möglichen rechtlichen, durch den Vertrag gegebenen Anspruchsfristen hinaus aufbewahren, um einen allfälligen Anspruch des Kunden abzuwehren, dann wäre nach der Verjährung der Fristen die weitere Speicherung nicht mehr mit der EU-DSGVO vereinbar.[25]

Die **Integrität und Vertraulichkeit** bedeutet, dass für die personenbezogenen Daten ein angemessenes Sicherheitsniveau durch geeignete technische und organisatorische Maß-

[21] vgl Feiler, L., Forgó, N. (2017), S. 9
[22] vgl VO (EU) 2016/679 ABl L 2016/119, S.35
[23] vgl Feiler, L., Forgó, N. (2017), S. 9, vgl VO (EU) 2016/679 ABl L 2016/119, S.36
[24] vgl Pachinger, M. M., Beham, G. (Hrsg) (2016): Datenschutz-Audit: Recht - Organisation - Prozess – IT: Der Praxisleitfaden zur Datenschutz-Grundverordnung, Wien, LexisNexis, S. 29f
[25] vgl Feiler, L., Forgó, N. (2017), S. 9f

nahmen gewährleistet werden muss.[26] Das angemessene Niveau und die geeigneten Maßnahmen werden auch im Art. 32 der EU-DSGVO durch den Gesetzgeber thematisiert. Dabei wird auf den Stand der Technik verwiesen. Dieser ist unter Berücksichtigung der Implementierungskosten sowie Art und Umfang, Umstände und Zweck der Verarbeitung und unter Anbetracht der unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für den Betroffenen, hinsichtlich der Rechte und Freiheiten der natürlichen Person, zu betrachten. Um dann in weiterer Folge die geeigneten technischen und organisatorischen Maßnahmen wählen zu können.[27] Dabei ist auch anzumerken, dass obwohl der Grundsatz „Integrität und Vertraulichkeit" heißt, er genauso auf den Schutz der Verfügbarkeit sowie Rechtmäßigkeit der Verarbeitung eingeht.[28]

Und die Klammer über all das Genannte, zieht die im Art. 5 Abs. 2 EU-DSGVO geforderte **Rechenschaftspflicht** (auch als „Accountability" bekannt). Dabei wird der Verantwortliche dazu verpflichtet, die Einhaltung der eben beschriebenen Grundsätze nach Art. 5 Abs. 1 EU-DSGVO jederzeit nachweisen zu können.[29]

Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Die Grundsätze der Verarbeitung werden ergänzt, um die im Art. 6 Abs. 1 EU-DSGVO geregelte Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Denn dies ist, auch unter Einhaltung der Grundsätze, nur dann der Fall, wenn jedenfalls eine der im Folgenden aufgezählten Bedingungen erfüllt ist[30]:

- Die Einwilligung des Betroffenen liegt für den Zweck vor (lit. a)
- Ein Vertrag mit dem Betroffenen liegt dazu vor oder eine vorvertragliche Maßnahme macht es notwendig, die vom Betroffenen angefragt wurde (lit. b)
- Eine rechtliche Verpflichtung des Verantwortlichen liegt vor (lit. c)
- Es ist zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen Person erforderlich (lit. d)
- Eine, dem Verantwortlichen übertragene Aufgabe des öffentlichen Interesses oder im Rahmen der Ausübung öffentlicher Gewalt erfordert es (lit. e)
- Die Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten macht es erforderlich, wenn nicht die Interessen oder Grundrechte des Betroffenen überwiegen, besonders dann, wenn Kinder betroffen sind (lit. f)

[26] vgl VO (EU) 2016/679 ABl L 2016/119, S.36
[27] vgl Pachinger, M. M., Beham, G. (Hrsg) (2016), S.30
[28] vgl Feiler, L., Forgó, N. (2017), S. 10
[29] vgl VO (EU) 2016/679 ABl L 2016/119, S.36
[30] vgl Kastelitz, M. (2016), S. 105

Wenn die rechtmäßige Verarbeitung von Daten auf einer Einwilligung basiert, dann sind dafür die, entsprechend Art. 7 EU-DSGVO gemachten Bedingungen für die Einwilligung einzuhalten. Beispielsweise muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form, in klarer und einfacher Sprache formuliert sein. Weiters hat ein Betroffener das Recht seine Einwilligung jederzeit zu wiederrufen:

„Die Einwilligung sollte durch eine eindeutige beständige Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung."[31]

Damit fällt Stillschweigen als eine mögliche Form der Einwilligung weg. Eine konkludente Einwilligung ist daher zukünftig schwer nachweisbar, da sie wohl nicht als „eindeutig bestätigende Handlung" gewertet werden kann.

Im Art. 8 der EU-DSGVO werden weitere Regelungen für Minderjährige gemacht. Dabei wird die Altersgrenze für die Zustimmungsfähigkeit bei Angeboten von Diensten der Informationsgesellschaft, mit der Vollendung des 16. Lebensjahres eingeführt. Wobei diese Altersgrenze durch den nationalen Gesetzgeber über die dafür vorgesehene Öffnungsklausel (max. bis zur Vollendung des 13. Lebensjahr) abgesenkt werden kann.[32]

Ebenfalls zusätzlich geregelt sind Verarbeitungsbedingungen für besondere Kategorien personenbezogener Daten inkl. strafrechtsrelevanter Daten in den Art. 9 und 10 der EU-DSGVO[33]. Sowie die Klarstellung im Art. 12 EU-DSGVO, dass dann, wenn für die Verarbeitungstätigkeit für den Verantwortlicher die Identifizierung einer Person nicht notwendig ist, keine zusätzlichen Informationen zum Betroffenen erhoben werden müssen, um der EU-DSGVO zu entsprechen, z. B. dann wenn der Betroffene das Auskunftsrecht geltend macht.[34]

2.2.2 Anwendungsbereich der EU-DSGVO

Der Anwendungsbereich der EU-DSGVO wird in einen persönlichen, sachlichen und einen räumlichen Anwendungsbereich unterschieden und wird im Folgenden näher erläutert.

[31] Erwägungsgrund Nr. 32 zur EU-DSGVO in: Pollirer, H.-J., Weiss, E., Knyrim, R., Haidinger, V. (Hrsg) (2017), S.32
[32] vgl Kastelitz, M. (2016), S. 111
[33] für die Definition sensibler Daten siehe Kapitel 2.1.2 Sensible Daten.
[34] vgl Kastelitz, M. (2016), S. 113

Wobei sich der sachliche Anwendungsbereich sich im Vergleich zum DSG 2000 nicht signifikant verändert hat. Hingegen hat sich der räumliche Anwendungsbereich des Datenschutzes stark ausgedehnt. Die Regelungen treffen nun auch Verantwortliche und Auftragsverarbeiter mit Niederlassung außerhalb der EU, wenn von deren Datenverarbeitungstätigkeiten Personen in der EU betroffen sind.[35]

Persönlicher Anwendungsbereich der EU-DSGVO

Die EU-DSGVO richtet sich an Verantwortliche und Auftragsverarbeiter. In der DSRL hatte der Auftragsverarbeiter nur untergeordnete regulatorische Pflichten zu erfüllen. Mit der EU-DSGVO ändert sich seine Stellung. Er ist nun gemeinsam mit dem Verantwortlichen primärer Normenadressat.[36]

Sachlicher Anwendungsbereich der EU-DSGVO

Der sachliche Anwendungsbereich regelt, welche Datenverarbeitungsaktivitäten erfasst sind. Im Art. 2 Abs. 1 der EU-DSGVO heißt es:

„Die Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[37]“

Darin finden sich mehrere Begriffe die es im Folgenden zu erklären gilt:
Im Art. 4 Abs. 1 EU-DSGVO ist definiert, was unter **personenbezogenen Daten** zu verstehen ist:

„[…] „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;[38] […]“

Identifizierbar im Sinne der EU-DSGVO ist eine natürliche Person dann, wenn eine Person direkt oder indirekt identifiziert werden kann indem ihr z.B. eine Kundennummer, Standortdaten oder Merkmale die z.B. auf die physische, wirtschaftliche oder soziale Identität der Person schließen lassen, zuordnet.[39] Beispielsweise kann über die „physische Identität“ die durch die Körpergröße, das Körpergewicht oder das Erscheinungsbild einer Person bestimmt wird, diese identifiziert werden. So wie beispielsweise auch über „wirtschaftliche

[35] vgl Hldjk, J. (2016): Sachlicher und räumlicher Anwendungsbereich der DSGVO, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S.42
[36] vgl Feiler, L., Forgó, N. (2017), S. 5
[37] vgl VO (EU) 2016/679 ABl L 2016/119, S.32
[38] vgl VO (EU) 2016/679 ABl L 2016/119, S.33
[39] vgl VO (EU) 2016/679 ABl L 2016/119, S.33

Identität“, die durch Einkommen, Vermögen, Eigentum etc. bestimmbar ist.[40] Der Begriff ist generell sehr weit gefasst. Die EU-DSGVO ist bereits anwendbar, sobald die Person einer Information auf irgendeine Weise zugeordnet werden kann und damit ein Personenbezug herstellbar ist. Dies umfasst beispielsweise Information wie Name, Adresse, Telefonnummer, Autokennzeichen oder IP-Adresse einer Person.[41]
Weiters ist in dieser Regelung erkennbar, dass sie sich nicht nach der Staatsangehörigkeit der Person oder ihren Aufenthaltsort abgegrenzt. Und sie findet keine Anwendung auf juristische Personen.[42]

Im Art. 4 Abs. 2 EU-DSGVO ist definiert, was unter der **Verarbeitung** zu verstehen ist:

„[…] „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verarbeitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;[43] […]“

Auch der Verarbeitungsbegriff der EU-DSGVO ist weit gefasst und regelt jeglichen Umgang mit personenbezogenen Daten. Der Gesetzgeber legt den Bestimmungen weiters das Gedankengut zugrunde, dass der Schutz personenbezogener Daten technologieneutral zu erfolgen hat. Daher gilt der Schutz für die **manuelle** Verarbeitung genauso wie für die **(teilweise) automatisierte Verarbeitung**.[44] Von einer teilweisen automatisierten Verarbeitung ist dann die Rede, wenn die Datenverarbeitungsschritte nicht ausschließlich manuell (vom Menschen ohne IT-Unterstützung, z.B. das Führen handschriftlicher Aufzeichnungen) durchgeführt werden, sondern wenn mindestens ein Verarbeitungsschritt maschinell (d.h. programmgesteuert / mikroprozessorgestützt) durchgeführt wird. Ganz automatisiert ist die Verarbeitung dann, wenn alle Verarbeitungsschritte maschinell erfolgen.[45]

---

[40] vgl Bergauer, C. (2016), S.55
[41] vgl Dr. Datenschutz (2017): Sachlicher Anwendungsbereich: Die DSGVO gilt, wenn ..., https://www.datenschutzbeauftragter-info.de/sachlicher-anwendungsbereich-die-dsgvo-gilt-wenn/, Abfragedatum 30.05.2017
[42] vgl Ennöckl, D. (2017): Die Verarbeitung von personenbezogenen Gesundheitsdaten nach der DSGVO, Heft 3/2017, Manz, S.90, vgl Hldjk, J. (2016), S.39
[43] vgl VO (EU) 2016/679 ABl L 2016/119, S.33
[44] vgl Hldjk, J. (2016), S.39f
[45] vgl Bergauer, C. (2016), S.44f

Im Sinne der EU-DSGVO ist ein **Dateisystem** laut Art. 4 Abs. 6 wie folgt zu verstehen:

„[…] „Dateisystem" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;[46] […]"

Die EU-DSGVO ist jedenfalls dann anwendbar, wenn die personenbezogenen Daten in einer elektronischen Datei gespeichert sind oder werden. Weiters ist sie auch dann anwendbar, wenn personenbezogene Daten manuell in einem Akt oder einer Aktensammlung (d.h. in der Regel in Form einer Papierablage) verwaltet werden, sofern ihre Deckblätter nach bestimmten Kriterien geordnet sind.[47] Folglich sind handschriftliche Aufzeichnungen personenbezogener Daten in der Regel nicht von der EU-DSGVO betroffen, mit einer Ausnahme. Nämlich mit der, dass diese Daten (ggf. auch mit der Absicht dies zu einem späteren Zeitpunkt zu tun) nach personenbezogenen Kriterien geordnet und in einem Karteisystem organisiert werden.[48] Ein Beispiel aus dem Gesundheitswesen dazu, wäre die Aufbewahrung von Patientenakten in Form einer sortierten Karteiablage im Archiv eines Krankenhauses.

Es gibt ein paar wenige Ausnahmen von der Regelung. Beispielsweise, wenn die Verarbeitung im Rahmen einer Tätigkeit erfolgt, die nicht in das Unionsrecht fällt, wie die nationale Sicherheit betreffende Tätigkeiten. Oder wenn die Verarbeitung durch Familienmitglieder ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt.[49]

Räumlicher Anwendungsbereich der EU-DSGVO

Im räumlichen Anwendungsbereich der UE-DSGVO finden sich sowohl Niederlassungen in als auch solche außerhalb der EU. Wenn die Verarbeitung personenbezogener Daten durch eine Niederlassung erfolgt, die für einen Verantwortlichen oder einen Auftragsverarbeiter **innerhalb der EU tätig wird**, egal ob die tatsächliche Verarbeitung in der EU oder außerhalb der EU erfolgt, dann findet die EU-DSGVO Anwendung.[50]

[46] vgl VO (EU) 2016/679 ABl L 2016/119, S.33
[47] vgl Feiler, L., Forgó, N. (2017), S. 4, vgl Hldjk, J. (2016), S.40
[48] vgl Bergauer, C. (2016), S.46, vgl Feiler, L., Forgó, N. (2017), S. 4
[49] vgl Hldjk, J. (2016), S.40
[50] vgl Hldjk, J. (2016), S.40f

Die EU-DSGVO findet aber auch dann Anwendung, wenn der Verantwortliche oder Auftragsverarbeiter für den die personenbezogenen **Daten von Betroffenen mit Aufenthaltsort in der EU** verarbeitet werden, eine der beiden folgenden Voraussetzungen erfüllt[51]:

- Die Datenverarbeitung dient dazu, um Betroffenen in der EU Waren oder Dienstleistungen entgeltlich oder auch unentgeltlich anzubieten.
- Die Datenverarbeitung dient dazu das Verhalten von Betroffenen in der EU zu beobachten.

Dem ist deshalb so, weil die EU-DSGVO dadurch sicherstellen möchte, dass die internationale Konkurrenz die am europäischen Markt tätig wir, aber keine Niederlassung in Europa hat, ebenfalls den europäischen Wettbewerbsbedingungen unterliegt.[52]

Beispiele:

- Wenn ein US-amerikanischer Onlinebuchhändler einem Schweden Bücher online zum Kauf anbietet, dann fällt dies in den Anwendungsbereich der EU-DSGVO (ersichtlich ist er Wille der Onlinehändlers beispielsweise dadurch, dass die Seite auch auf Schwedisch angeboten wird[53]).
- Wenn Google aufgrund aktivierter Standortdienste am Smartphone die Aufenthaltszeiten kanadischer Staatsbürger mit Aufenthaltsort in Wien an bestimmten Lokationen sammelt und analysiert, dann unterliegt diese Verarbeitungstätigkeit der EU-DSGVO.

2.2.3 Strafausmaß

Weiters ist in der Verordnung geregelt, wie die Einhaltung der Vorschriften gewährleistet werden soll und welche Sanktionen bei Verstößen zu verhängen sind. Die Geldbußen im Falle von Datenschutzverletzungen sind nach der EU-DSGVO sehr hoch, vor allem da die Strafe am weltweiten Gesamtkonzernumsatz bemessen wird.[54]

Es werden zwei Kategorien von Strafausmaßen unterschieden[55]:

(1) 10 Millionen Euro oder 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres bei einem Unternehmen, je nachdem was höher ist.

[51] vgl Hldjk, J. (2016), S.41
[52] vgl Feiler, L., Forgó, N. (2017), S. 6
[53] vgl Hldjk, J. (2016), S.41
[54] vgl Feiler, L., Forgó, N. (2017), S. 40
[55] vgl Feiler, L., Forgó, N. (2017), S. 38f

(2) 20 Millionen Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres bei einem Unternehmen, je nachdem was höher ist.

Das unter (1) beschriebene Strafausmaß gilt für folgende Fälle[56]:

- Art. 8 EU-DSGVO: Pflicht zur Einhaltung der Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft,
- Art. 11 EU-DSGVO: Pflichten im Zusammenhang mit der Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist,
- Art. 25 EU-DSGVO: Pflicht zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Privacy-by-Design und Privacy-by-Default),
- Art. 26 EU-DSGVO: Pflicht zur vertraglichen Regelung der Aufgabenverteilung zwischen gemeinsamen Verantwortlichen,
- Art. 27 EU-DSGVO: Pflichten zur Benennung eines Vertreters für nicht in der Union niedergelassene Verantwortliche bzw. Auftragsverarbeiter,
- Art. 28 EU-DSGVO: Pflichten beim Einsatz eines Auftragsverarbeiters,
- Art. 29 EU-DSGVO: Verbot der eigenmächtigen Verarbeitung durch Auftragsverarbeiter oder Personen, die Auftragsverarbeitern oder Verantwortlichen unterstellt sind,
- Art. 30 EU-DSGVO: Pflicht zur Führung des Verzeichnisses von Verarbeitungstätigkeiten,
- Art. 31 EU-DSGVO: Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde,
- Art. 32 EU-DSGVO: Pflicht zur Sicherstellung der Sicherheit der Verarbeitung,
- Art. 33 EU-DSGVO: Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Data-Breach Notification),
- Art. 34 EU-DSGVO: Pflicht zur Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen (Data-Breach Notification),
- Art. 35 EU-DSGVO: Pflicht zur Datenschutz-Folgeabschätzung (Privacy Impact Assessment)
- Art. 36 EU-DSGVO: Pflicht zur vorherigen Konsultation,
- Art. 37-39 EU-DSGVO: Pflicht zur Einhaltung der Bestimmungen (Benennung, Stellung und Aufgaben) über den Datenschutzbeauftragten und

[56] vgl Feiler, L., Forgó, N. (2017), S. 38f, vgl Illibauer, U. (2016): Geldbußen und andere Sanktionen, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 340f

- Art. 41-43 EU-DSGVO: Pflicht zur Einhaltung der Bestimmungen über genehmigte Verhaltensregeln und Zertifizierungen (gelten für Verantwortliche und Auftragsverarbeiter sowie Zertifizierungs- und Überwachungsstellen).

Das unter (2) beschriebene Strafausmaß gilt für folgende Fälle[57]:

- Art. 5, 6, 7, und 9 EU-DSGVO: Pflicht zur Einhaltung der Grundsätze der Datenverarbeitung und Voraussetzungen für ihre Rechtmäßigkeit mit Ausnahme der Bedingungen für die Einwilligung eines Kindes,
- Art. 12-22 EU-DSGVO: Pflicht zur Einhaltung der Betroffenenrechte einschließlich Informationspflicht des Verantwortlichen sowie Beschränkungen automatisierter Entscheidungen und Profiling,
- Art. 44-49 EU-DSGVO: Pflicht zur Einhaltung von Bestimmungen über internationale Datenübermittlungen,
- Art. 58 Abs. 1 lit. e und f EU-DSGVO: Einhaltung der Verpflichtung, der Aufsichtsbehörde Zugang zu gewähren,
- sowie die Rechtsvorschriften der Mitgliedstaaten, auf Grundlage von Art. 85 bis 91 (Vorschriften für besondere Verarbeitungssituationen einschließlich des Beschäftigungskontextes).

2.3 Begriffsdefinition und Abgrenzung der Compliance

Gesetzen muss bekanntlich entsprochen werden, denn andernfalls führt dies womöglich zu Strafen wie sie im vorangegangenen Abschnitt beschrieben wurden. Wenn dieser rechtskonforme Zustand angestrebt wird, dann wird in Unternehmensumfeld häufig vom Begriff „Compliance“ gesprochen. Im Folgenden wird erklärt was darunter zu verstehen ist und wie dieser Begriff zu dem, in diesem Kontext ebenfalls häufig verwendeten Begriff „Governance“ abzugrenzen ist bzw. wie das Thema Datenschutz in der Compliance einzuordnen ist.

2.3.1 Governance

Die Begriffe „Compliance“ und „Governance“ stammen ursprünglich aus der Politikwissenschaft. Sie wurden in das Feld der Wirtschaftswissenschaften übernommen.[58] Häufig werden die beiden Begriffe im gemeinsamen Kontext genannt. Es ist dabei aber wichtig zu

[57] vgl Feiler, L., Forgó, N. (2017), S. 39, vgl Illibauer, U. (2016), S. 341
[58] Rath, M., Sponholz, R. (2014): IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen, 2. Aufl, Berlin, Erich Schmidt Verlag, S.27

wissen, dass damit zwei unterschiedliche Dinge gemeint sind, die jedoch ineinandergreifen. Gemeinsam ist aber sowohl der Compliance als auch der Corporate Governance, das vorrangige Ziel das Unternehmen präventiv vor Schäden zu schützen bzw. Schadensbegrenzung herbei zu führen. Letzteres wird durch die Erfüllung von Organisationspflichten sowie der Möglichkeit Regelverletzungen frühzeitig zu erkennen, möglich.[59]

Durch die **Corporate Governance** (gelegentlich auch als Enterprise Governance bezeichnet) wird ein Unternehmen geführt und kontrolliert. Dieser Begriff steht für ein System, welches die Verteilung der Rechte und Pflichten sowie die Regeln und Verfahren zur Entscheidungsfindung im Unternehmen festlegt. Dadurch können entsprechend der Regeln die Unternehmensziele festgelegt werden, die Mittel zur Erreichung der Ziele bereitgestellt und die Messung und Kontrolle der Performance vereinbart werden.[60]

Vom der Corporate Governance abgeleitet kann man die IT-Governance unterscheiden. Dabei ist die eben angeführte Erklärung auch auf den Begriff **IT Governance** umlegbar bzw. eingrenzbar. Auch hier spricht man von einem System, durch das die IT in einem Unternehmen gelenkt und kontrolliert wird. Durch die IT-Governance-Struktur wird die Verteilung von Rechten und Pflichten definiert. Regeln und Verfahren werden vereinbart um die Entscheidungen im IT-Bereich herbeiführen zu können und es werden IT-Ziele, Mittel zur Erreichung dieser sowie Mittel zur Kontrolle der Performance definiert. Weill und Woodham definieren IT-Governance wie folgt:

„We define IT governance as specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT."[61]

Zusammengefasst kann man sagen, dass Governance allgemein vom Sinn her die Ausweitung von Regelsystemen bewirkt, denn sie macht Regeln und Verfahren zur Vorgabe. Die jeweilige Organisation hat folglich die Einhaltung der Regelsysteme sicherzustellen. D.h. sie muss Compliance gewährleisten. Daher kann Compliance als Teilaspekt der Governance gesehen werden.[62]

---

[59] vgl Rath, M., Sponholz, R. (2014), S.25
[60] vgl Dierlamm, J. (2011): IT Governance und IT Compliance – die wichtigsten Normen und Regelwerke, Köln, TÜV Media, S.3f, European Central Bank, 2004, Annual Report: 2004, ECB, Frankfurt, Glossary. https://www.ecb.europa.eu/pub/pdf/annrep/ar2004en.pdf?4cc01c9b5ba4f31492c002bd7b5c954e, Abfragedatum 04.07.2017
[61] vgl Weill, P., Woodham, R. (2002): Don't Just Lead, Govern: Implementing Effective IT Governance (April 2002). MIT Sloan Working Paper No. 4237-02. https://ssrn.com/abstract=317319 or http://dx.doi.org/10.2139/ssrn.317319, Abfragedatum 17.07.2017, S.1
[62] vgl Rath, M., Sponholz, R. (2014), S.29

2.3.2 Compliance

Compliance liegt, einer Definition von Klotz nach, dann vor, wenn alle für ein Unternehmen verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.[63]

Dabei ist zum einen von gesetzlichen Verbindlichkeiten die Rede, wie von Gesetzen und der aktuellen Rechtsprechung, aber auch von Verträgen. Aber es zählen beispielsweise auch Normen oder branchenübliche Standards zu den, von einem Unternehmen anerkannten und als verbindlich geltenden Vorgaben, die von außerhalb des Unternehmens kommen. Weiters definieren Unternehmen intern ihre eigenen Vorgaben, zu deren Einhaltung sie sich bekennen, wie Richtlinien und Verfahrensanweisungen[64]:

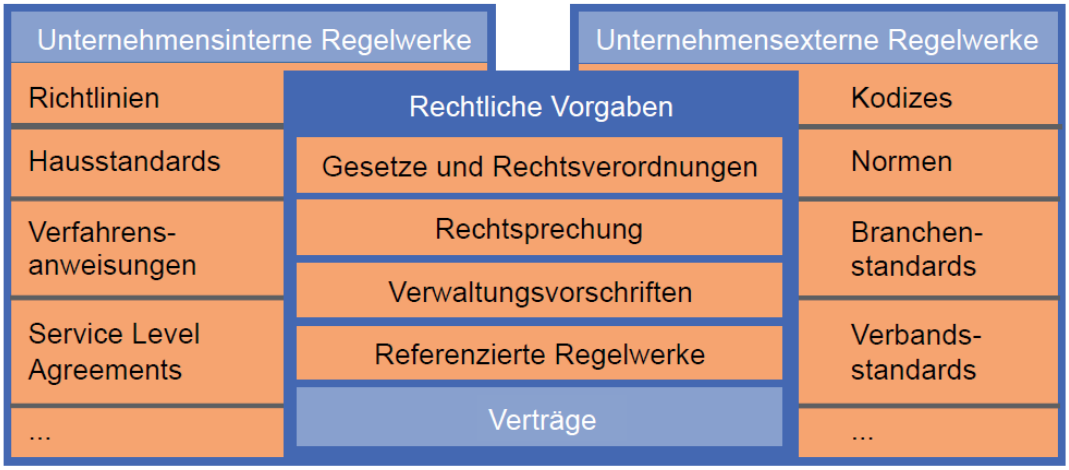

Abbildung 1: Die Quellen der Compliance[65]

Ein weiterer Aspekt der Definition ist der Begriff der „Nachweisbarkeit“ (im englischen auch „Accountability“). Nachweisbarkeit hat sich vor allem im Zusammenhang mit der Corporate Governance zu einem wesentlichen Aspekt der Compliance entwickelt, da das Management dafür Sorge zu tragen hat, dass vorgegebene Regeln eingehalten werden.[66] Dies muss nachweislich - und das bedeutet in der Regel „dokumentiert“ - erfolgen.

IT-Compliance kann nach Rath und Sponholz wie folgt definiert werden:

„(IT)-Compliance bezeichnet die Kenntnis und Einhaltung sämtlicher regulatorischer Vorgaben und Anforderungen an das Unternehmen, die Initiierung und die Einrichtung entsprechender Prozesse und die Schaffung eines Bewusstseins der Mitarbeiter für die

[63] vgl Klotz, M. (2009): IT-Compliance: Ein Überblick, Heidelberg, dpunkt.verlag, S.3
[64] vgl Klotz, M. (2009), S.4
[65] Abbildung entnommen aus: Klotz, M. (2009), S.4
[66] Rath, M., Sponholz, R. (2014), S.26

Regelkonformität, sowie die Kontrolle und Dokumentation der Einhaltung der relevanten Bestimmungen gegenüber internen und externen Adressaten."[67]

Auch hier fällt uns auf, dass diese Definition wenig IT-lastig sondern sehr generell für Compliance gilt, da auch der Begriff der IT-Compliance ein abgeleiteter ist. In dieser Definition finden sich aber zwei weitere Aspekte der Compliance:

Zum einen wird darin die **Einrichtung von Prozessen** zur Einhaltung regulatorischer Vorgaben und Anforderungen angesprochen. Dies ist relevant, dass die Herbeiführung von Compliance nicht ein einmaliges Ereignis sein kann. Dieser Zustand muss aufrechterhalten werden und erfordert daher einen laufenden Prozess.

Weiters wird die Notwendigkeit der **Schaffung eines Bewusstseins der Mitarbeiter** für die Regelkonformität thematisiert. Denn auch wenn alle anderen Aspekte der Compliance gut ausgestaltet wurden, ist doch das Verhalten der Menschen letztendlich entscheidend. Das Handeln der Mitarbeiter ist als Risiko zu sehen, sofern das Unternehmen nicht in der Lage ist den Menschen darin zu vermitteln, dass selbstständiges regelkonformes Handeln entscheidend sein kann und die Voraussetzungen dafür schafft.[68]

Für die Einhaltung der IT-Compliance ist es im Übrigen unerheblich ob die IT von einem externen Partner oder intern betrieben wird.[69]

2.3.3 Einordnung des Datenschutzes im Rahmen der Compliance

Im Zusammenhang mit IT-Compliance ist die Unterscheidung zwischen IT-Compliance und der **IT-gestützten Compliance** relevant. Dabei ist die IT einmal Anforderungsträger und einmal Unterstützer zur Erfüllung der Compliance, da IT-Mittel zu ihrer Erreichung eingesetzt werden. Dies kann sich gleichermaßen auf die Corporate Compliance als auch auf die IT-Compliance beziehen.[70]

[67] Rath, M., Sponholz, R. (2014), S.27
[68] Rath, M., Sponholz, R. (2014), S.25f
[69] vgl Klotz, M. (2009), S.6
[70] vgl Klotz, M., Dorn, D.-W. (2008): IT-Compliance – Begriff, Umfang und relevante Regelwerke, In: HMD – Praxis der Wirtschaftsinformatik, 2008, Jg. 45, Heft 263, S.9

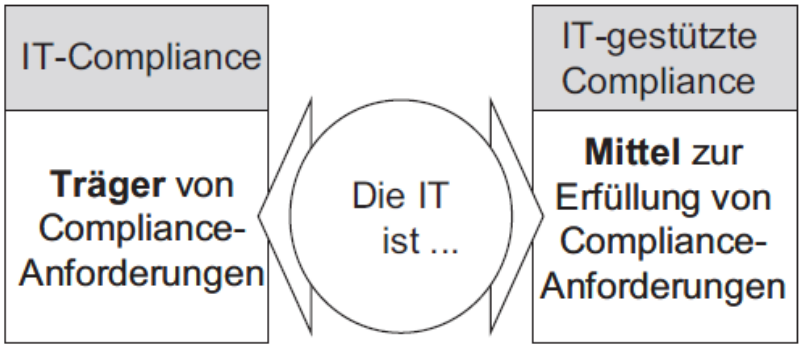

Abbildung 2: IT-gestützte Compliance vs. IT-Compliance[71]

Die EU-DSGVO macht es sich nicht zum Hauptzweck die Datensicherheit im Unternehmen zu regeln, sondern den Schutz der Person bzgl. ihrer Privatsphäre, welche durch einen mangelnden Schutz personenbezogener Daten zu dieser Person gefährdet sein könnte. Dabei sind viele organisatorische Themen, wie die Einhaltung von Betroffenenrechten oder die Erstellung des Verarbeitungsregisters für die Aufsichtsbehörde notwendig. Vor allem in großen Organisationen wird man vielen Anforderungen nur mit Unterstützungsleistung der IT gerecht werden können, weshalb **IT-gestützte Compliance** hier in erster Linie ein Thema ist.
Andererseits gibt sie die Einhaltung von Datensicherheit nach Stand der Technik und durch entsprechende technische und organisatorische Maßnahmen vor, wodurch sie auch die IT zum Anforderungsträger macht und somit **IT-Compliance** einfordert.

Die IT ist daher hinsichtlich EU-DSGVO sowohl als Anforderungsträger, als auch als Erfüllungsgehilfe gefordert. Ein Großteil der Themen die es aber im Rahmen der Herbeiführung der EU-DSGVO-Compliance zu behandeln gibt, und das wird vor allem auch im Rahmen der empirischen Untersuchung deutlich, sind organisatorischer anstatt technischer Natur.

2.4 Bedeutung von Compliance im Gesundheitswesen

Dies führt uns weiter zur Evaluierung des Stellenwerts von Compliance im Gesundheitswesen. Das Gesundheitswesen umfasst drei Bereiche: die Krankenversorgung, die Gesundheitsförderung und die Prävention.[72] Die Leistungen der Krankenversorgungen umfassen ärztliche Hilfe, Spitalspflege, medizinische Rehabilitation, medizinische Hauskrankenpflege und Leistungen von Hebammen, Psychotherapie und klinisch-

[71] Abbildung entnommen aus: Klotz, M., Dorn, D.-W. (2008), S.9
[72] vgl Öffentliches Gesundheitsportal Österreich (2017): Gesundheitswesen, https://www.gesundheit.gv.at/gesundheitssystem/gesundheitswesen/inhalt, Abfragedatum 17.07.2017

psychologische Diagnostik, Behandlungen durch medizinisch-technische Dienste, Mutter-Kind-Pass-Untersuchungen sowie Gesunden- und Vorsorgeuntersuchungen.[73] Dabei unterscheidet man zwischen ambulanter und stationärer Behandlung, sowie öffentlich (gesetzlich) oder privat krankenversicherten Patienten.[74] Der Fokus dieser Arbeit richtet sich auf den Bereich der Krankenversorgung im Rahmen des stationären Gesundheitswesens, weil hier die Aufbewahrungspflichten für Daten längere sind als im ambulanten Bereich und die Einrichtungen in der Regel auch deutlich größer sind. Daher werden betroffene Unternehmen mit anderen Herausforderungen konfrontiert sein, was es im Rahmen der Studie zu berücksichtigen und daher abzugrenzen gilt.

Generell bekommt das Thema Compliance einen zunehmend wachesenden Stellenwert im Gesundheitswesen. Es gibt viele Anwendungsbereiche im Gesundheitswesen, auf welche sich Compliance Aktivitäten konzentrieren, wie Abrechnungsbetrug (z.B. Abrechnung nicht erbrachter Leistungen), Bevorzugung von Patienten (z.B. rasche Behandlung gegen Zuwendung), Korruption (z.B. sogenannte Einweiser-Prämien) etc.[75]

Aus der Auseinandersetzung mit dem Gesetz hat sich die Erkenntnis ergeben, dass die EU-DSGVO-Compliance im Bereich der stationären Krankenversorgung aus zwei Gründen besonders wichtig wird:

(1) In diesem Bereich wird mit großen Mengen an sensiblen personenbezogenen Daten gearbeitet.
(2) In diesem Bereich herrscht ein stetiger hoher Kostendruck.

Zum einen führt (1) dazu, dass das Gesundheitswesen von organisatorischen und technischen Maßnahmen zur Herstellung der EU-DSGVO-Compliance betroffen sein wird, da z.B. eine voraussichtlich große Menge an Verarbeitungstätigkeiten ein hohes Risiko für den Patienten im Sinne des Schutzes seiner Privatsphäre mit sich bringen wird. Und man sieht sich im Gesundheitswesen immer im Konflikt zwischen der ärztlichen Schweigepflicht

[73] vgl Öffentliches Gesundheitsportal Österreich (2017a): Das Gesundheitswesen im Überblick, https://www.gesundheit.gv.at/gesundheitssystem/gesundheitswesen/gesundheitssystem, Abfragedatum 17.07.2017
[74] Gabler Wirtschaftslexikon (2017), Stichwort: Gesundheitswesen, http://wirtschaftslexikon.gabler.de/Archiv/55801/gesundheitswesen-v9.html, Springer Gabler Verlag (Hrsg), Abfragedatum 30.06.2017
[75] vgl Döring, S., Heintz, L. (2012): Compliance im Gesundheitswesen: Krankenhäuser stärker im Blick, http://www.pwc.de/de/gesundheitswesen-und-pharma/compliance-im-gesundheitswesen-krankenhaeuser-staerker-im-blick.html, Abfragedatum 14.07.2017, vgl Ittensohn, D. (2013): Compliance im Gesundheitswesen: "Wandel von der Schuldkultur über die Fehlerkultur zur Sicherheitskultur", eHealth Summit 2013, https://www.eiseverywhere.com/file_uploads/6694b88b292804fcea7a871a0fa437fe_Ittensohn_ComplianceimGesundheitswesen.pdf, Abfragedatum 14.07.2017

sowie dem Datenschutz auf der einen Seite und einem möglichst raschen, flexiblen Zugriff der Ärzteschaft auf Gesundheitsdaten um Patienten die bestmögliche Behandlung basierend auf möglichst vielen Informationen zum Behandlungskonzept bzw. der Vorgeschichte des Patienten zukommen zu lassen.[76]

Und (2) hat seinen Grund darin, dass die österreichische Krankenversorgung aufgrund von steigenden Kosten und sinkenden Beitragsleisten sozusagen „knapp bei Kasse" ist. Dazu führt vor allem eine Überalterung der Gesellschaft, aber auch eine veränderte Einkommensstruktur, das steigende Bildungsniveau und alternative Familienmodelle nehmen darauf Einfluss.[77] Darin findet man wohl auch die Begründung, weshalb das Gesundheitswesen in puncto Datensicherheit hinterherhinkt. Einer KPMG Studie aus dem Jahr 2015 zufolge, liegt das Gesundheitswesen im Vergleich zu anderen Industriesektoren, hinsichtlich technischer Kompetenz im Schutz von IT-Infrastruktur und elektronischer Gesundheitsdaten deutlich zurück. Dies wird erkennbar durch den Einsatz von veralteten klinischen Technologien, unsicheren netzwerkfähigen medizinischen Devices und einem generellen Mangel an Informationssicherheits-Management-Prozessen bzw. entsprechenden Zertifizierungen.[78]

Auf Basis dieser Argumente ist ein klarer Handlungsbedarf für das Gesundheitswesen zum Thema Datenschutz und Datensicherheit ableitbar.

2.5 Der Nutzen von Compliance

Compliance, ganz allgemein, kann einen klaren Nutzen für Unternehmen generieren. Dabei können zwei Arten von Nutzen unterschieden werden[79]:

(1) Vermeidung von Nachteilen

(2) Generierung von Vorteilen

Hinsichtlich (1) kann festgehalten werden, dass Compliance dazu beiträgt, dass drohende **Strafrisiken** reduziert werden. Beispiele im Sinne der IT-Compliance bzw. IT-gestützten

[76] vgl Meyer, S. (2017): Datenschutz-Grundverordnung - eine sinnvolle Herausforderung oder Provokation für Kliniken und Krankenhäuser, BvD-News Ausgabe 2/2017, Berlin, S.30
[77] vgl Schmalzer, T., ua: Die dritte Säule im Österreichischen Gesundheitssystem: Eine Studie für den Raum Graz am Beispiel des Ärzte-Center Graz, http://wko.at/wien/drittesauele.pdf, Abfragedatum 17.07.2017
[78] vgl KPMG (2015): Health Care and Cyber Security: Increasing Threats Require Increased Capabilities, https://www.kpmg-institutes.com/content/dam/kpmg/healthcarelifesciencesinstitute/pdf/2015/cyber-healthcare-survey.pdf, Abfragedatum 17.07.2017, S.1
[79] vgl Klotz, M. (2009), S. 19

Compliance wäre ein Verhindern von Strafen aufgrund nicht eingehaltener Dokumentations- und Archivierungspflichten. Bei diesem denkbaren Schaden, ist nicht nur vom monetären Strafausmaß die Rede, denn auch das Risiko eines möglichen **Imageverlusts** gilt es zu bewerten. Dadurch könnten im Rahmen von Ausschreibungen Nachteile entstehen bzw. könnten auch Bestandskunden verloren gehen.[80]

Hinsichtlich (2) kommt man zu der Erkenntnis, dass Compliance auch einen echten wirtschaftlichen Vorteil generieren kann. Am Beispiel der IT-Compliance, könnten positive Effekte die Erhöhung **der Sicherheit, IT-Qualität** und **Produktivität** sein. Beispiele wären Standardisierungen die in der Regel durch die einhergehende Reduktion der Komplexität auch zu einer Erhöhung der Qualität der IT-Betriebsführung führen, effektivere Prozesse durch Kontrollen, Automatisierungen (oft eine Folge von Standardisierungen) sowie Zeit- und Kostenreduktion im Rahmen z.B. im Rahmen von Wartungs- und Administrationstätigkeiten.[81]

Weitere Argumente können in der Literatur exemplarisch gefunden werden:

- Häufig müssen Unternehmen Zertifizierungen vorweisen, welche durch die Umsetzung der Compliance-Anforderungen erreichbar werden, um überhaupt in **Ausschreibungen** berücksichtigt zu werden. [82]
- Hinsichtlich **Haftungsreduktion** bieten sich weitere Vorteile, denn Haftungsentlastungen wie Versicherungen können nur abgeschlossen werden bzw. bleibt deren Versicherungsschutz bei Versäumnissen nur dann aufrecht, wenn Compliance gegeben ist. Z.B. bei der Versicherung gegen IT-Risiken unter Einhaltung eines effektiven IT-Risikomanagements entsprechend Stand der Technik, derzeit nach ISO 27001.[83]
- Ein anderer denkbarer Vorteil wäre, das Unternehmen im Rahmen von Unternehmenstransaktionen bei einer **Due-Diligence-Prüfung** besser abschneiden, wenn Compliance-Vorgaben umgesetzt sind. Bzw. würde beim Unternehmenskauf ein Abschlag berechnet werden um die Compliance erst aufzubauen, wenn sie nicht gegeben wäre.[84]

---

[80] vgl Klotz, M. (2009), S. 19, vgl Böhm, M. (2008): IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT, In: HMD – Praxis der Wirtschaftsinformatik, 2008, Jg. 45, Heft 263, S. 26
[81] vgl Klotz, M. (2009), S. 21f, vgl Böhm, M. (2008), S. 26f
[82] vgl Klotz, M. (2009), S. 18
[83] vgl Bücking, J. (2014): Datenschutz, Datensicherheit und Compliance am Beispiel Islands, https://files.vogel.de/vogelonline/vogelonline/files/8058.pdf, Abfragedatum 05.07.2017
[84] vgl Klotz, M. (2009), S. 18, vgl Böhm, M. (2008), S.27

2.6 Die Kosten von Compliance

Um Compliance generell und im folgenden Beispiel IT-Compliance im Speziellen herzustellen fallen Aufwände an, da Anpassungen an IT-Anwendungen, IT-Systemen (wie Netzwerk, Datenbanken, Betriebssystemen etc.) und IT-Prozessen erforderlich sind. Es sind Einmalkosten zu berücksichtigen, wie die Erstellung oder Überarbeitung von Berechtigungskonzepten oder Einführung von Zutrittssystemen. Und in weiterer Folge sind laufende Kosten durch regelmäßig durchzuführende Maßnahmen zu berücksichtigen, wie Prozesse zum Einspielen von Patches und Security-Updates oder das Abhalten jährlicher Notfallübungen.[85]

Die angeführten Veränderungen und Investitionen dienen in erster Linie dem Schutz und der Kontrolle. Eine direkte Leistungssteigerung ist dabei in der Regel nicht vorgesehen. Weiters sind ab der Inbetriebnahme der Anpassungen laufend personelle Ressourcen aufzuwenden um die **Kontrollen** durchzuführen. Diese sind zu dokumentieren um sie bei Bedarf Prüfern, Behörden und etwaigen anderen Anforderern vorlegen zu können. In der Regel werden folglich interne **Auditprozesse** implementiert. Damit stellt man sicher, dass eine externe Überprüfungsstelle bei der Sichtung der Umsetzung geforderter Maßnahmen keine schweren Abweichungen auffindet. All diese Maßnahmen binden Ressourcen und reduzieren die Flexibilität.[86]

In der nachfolgenden Abbildung wird dargestellt wie die IT-Performance ab dem Zeitpunkt der Herstellung der IT-Compliance sinkt:

[85] vgl Böhm, M. (2008), S.19
[86] vgl Böhm, M. (2008), S.19

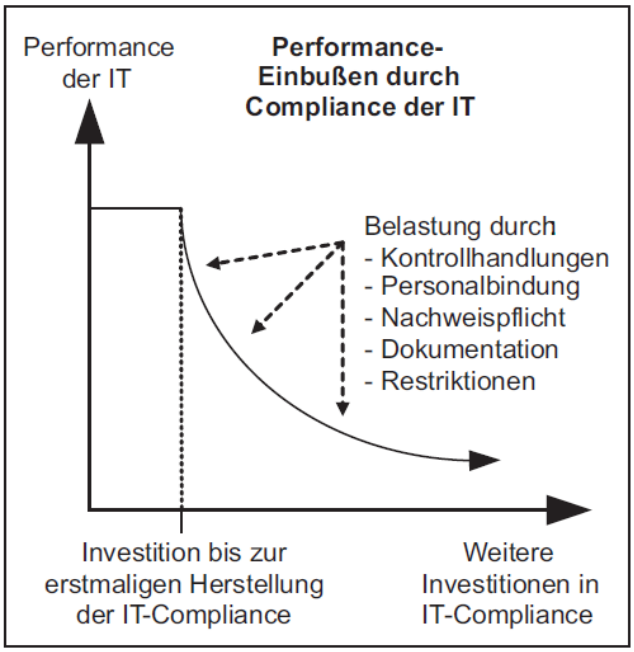

Abbildung 3: IT-Compliance wirkt auf Leistungsfähigkeit[87]

Hinsichtlich des Wertbeitrags der IT für das Unternehmen ist die Auswirkung der IT-Compliance zweistufig, wie man in der folgenden Darstellung sehen kann:

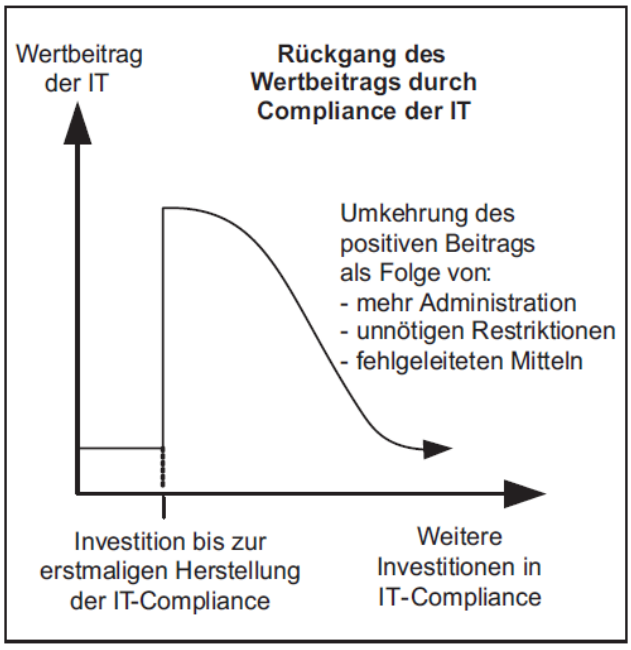

Abbildung 4: Einfluss der IT-Compliance auf Wertbeitrag der IT[88]

Mit diesem Effekt werden Unternehmen deshalb konfrontiert, da in der ersten Stufe, bis zur Herstellung der IT-Compliance ein immenser Wertbeitrag zu verzeichnen ist, da andernfalls eine Gefährdung für die Compliance des gesamten Unternehmens besteht. In

[87] Abbildung entnommen aus: Böhm, M. (2008), S.19
[88] Abbildung entnommen aus: Böhm, M. (2008), S.19

der zweiten Phase, nach Herstellung der IT-Compliance, wirkt sich aber auch in dieser Relation jede weitere Investition in IT-Compliance nachteilig für das Unternehmen aus.[89]

Auch wenn die EU-DSGVO-Compliance unseren Überlegungen nach keine reine IT-Compliance, sondern eine eher IT-gestützte Compliance ist, so treffen die gerade diskutierten Erkenntnisse auch in diesem Bereich zu, denn auch zur Herstellung der EU-DSGVO-Compliance empfiehlt es sich ein Datenschutz-Management-System einzuführen und darin sind in der Regel Aktivitäten wie Kontrollen und Audits vorgesehen. Daher lässt sich folgern, dass diese Argumentation zum Einfluss der Compliance hinsichtlich des Wertbeitrags, auch für Vorhaben zur Herstellung der EU-DSGVO-Compliance übernommen werden kann.

2.7 Erfolgreiche Umsetzung von Compliance-Vorhaben

Um dennoch eine erfolgreiche Umsetzung eines Compliance-Vorhabens sicherzustellen, sollten die im folgenden genannten Aspekte beachtet werden.

Es ist wichtig von Beginn eines IT-Compliance-Einführungsvorhabens an eine überlegte Strategie vorweisen zu können, um etwaige negative Effekte bei Investitionen in IT-Compliance zunächst kompensieren und danach auch als Vorteile nutzen zu können. Denn nach der Herstellung der IT-Compliance sollten die Investitionen nicht beendet werden. Daher sind die folgenden vier Faktoren von vornherein zu beachten um die eben im Kapitel 2.6 Die Kosten von Compliance dargestellten Effekte zu kompensieren[90]:

- **Verantwortung**: Die Unternehmensführung muss ein klares Commitment zur IT-Compliance geben, denn es ist ihre Verantwortung, dass diese hergestellt und eingehalten wird. Dazu gehört auch, dass ausreichend Mittel zur Verfügung gestellt werden müssen.
- **Planung**: Es sind von Beginn des Projekts an Maßnahmen vorzusehen, die eine aufwandsreduzierte Implementierung der Anforderungen unterstützen. Dies wäre beispielsweise Prozessstandardisierungen oder IT-Systembereinigungen. Auch diese Maßnahmen können aber Aufwand bedeuten, schaffen aber zusätzlichen Nutzen.
- **Budget**: Es sind bereits zu Projektbeginn Maßnahmen vorzusehen und zu budgetieren die über die Herstellung der Compliance hinausreichen. Beispielsweise die Ein-

[89] vgl Böhm, M. (2008), S.19
[90] vgl Böhm, M. (2008), S.20

führung eines Kontrollsystems. Dies erhöht zwar initial den Aufwand, senkt aber den Aufwand zusätzliche Anforderungen in der Zukunft umzusetzen.

- **Qualitätssteigerung**: Die Folgen der Compliance müssen konsequent zur Qualitätsverbesserung, Fehlerreduktion und für mehr Stabilität im IT-Betrieb genutzt werden. Ein sicheres und solides Fundament der IT-Betriebsführung bringt die IT hin zur Prävention statt Fehlerkorrektur. Dadurch werden komplexere und höherwertige IT-Leistungen erst möglich.

2.8 Erläuterung des Wirtschaftlichkeitsprinzips

Da nun alle Begrifflichkeiten eingeführt wurden kann nun auf die Thematik der Wirtschaftlichkeit im Sinne der EU-DSGVO-Compliance hingeführt werden.
Im Kontext der Wirtschaftlichkeit macht es Sinn hinsichtlich des angestrebten Ergebnisses zwei Begriffe zu unterscheiden: Output und Outcome. Unter Output ist das Ergebnis nach Umsetzung einer Maßnahme, d.h. nach Mitteleisatz (Input) zu verstehen. Auf der Ebene der umgesetzten Maßnahmen ist der **Output** ein **Maß für die Messung der Effektivität** einer Maßnahme zu betrachten. Ein Beispiel für Output wäre die Erstellung und Kommunikation einer Arbeitsanweisung zur Beantwortung von Auskunftsanfragen durch Betroffene. Der **Outcome** hingegen ist als **Maß der Wirksamkeit** zu interpretieren. Effektive Maßnahmen müssen nicht zwangsläufig immer wirksam sein. Output ergänzt um den Faktor Effektivität führt zum Outcome. Wenn der Mitteleinsatz einer effektiven Maßnahme auch wirksam ist, dann spricht man auf von Outcome-Effektivität. Ein Beispiel für Outcome wäre, dass bei keiner Auskunftsanfrage im vergangenen Monat durch Betroffene eine Überschreitung der gesetzlich vorgesehenen Beantwortungsfrist von einem Monat verzeichnet werden musst. Der Begriff Nutzen kann in unserem Kontext mit Outcome gelichgesetzt werden, bringt allerdings die subjektive Wahrnehmung mit ein. Synonym für **Nutzen** kann auch der Begriff Impact (zu Deutsch Wirkung) verwendet werden. Der Nutzen und somit **Outcome** von Projekten wird üblicherweise in den Projektzielen festgehalten.[91]

Wirtschaftlich orientierte Unternehmen versuchen zu erreichen, dass die Kosten den Nutzen nicht übersteigen bzw. der Nutzen die Kosten deckt. Der Begriff der Wirtschaftlichkeit kann über das ökonomische Prinzip (**Wirtschaftlichkeitsprinzip**) erklärt werden, welches davon ausgeht, dass das Wirtschaftssubjekt aufgrund der Knappheit an Gütern bei einer

[91] vgl Mühlenkamp, H. (2011): Wirtschaftlichkeit und Wirtschaftlichkeitsuntersuchungen im öffentlichen Sektor, Speyer Arbeitsheft Nr. 2014 der Deutschen Hochschule für Verwaltungswissenschaften Speyer 2011, Berlin, Speyer, S.9 u. 11f

wirtschaftlichen Handlung die eizusetzenden Mittel mit dem Ergebnis in Verhältnis setzt. Dies tut es, um nach seinen Präferenzen eine Nutzen- bzw. Gewinnmaximierung herbeizuführen.[92] Die Wirtschaftlichkeit beschreibt dadurch wie effizient ein Unternehmen arbeitet, denn die Effizienz stellt Ergebnis und Aufwand gegenüber. Effizienz bedeutet, dass man aus knappen Ressourcen das maximale herausholt.[93]

Um einer hohen Effizienz gerecht zu werden sind mehrere Lösungswege denkbar. Entweder wird ein bestimmtes Ergebnis angestrebt und dazu wird versucht, den Aufwand so gering als möglich zu halten (**Minimalprinzip**). Oder der mögliche Aufwand ist vorgegeben und man versucht unter diesen Bedingungen das Ergebnis zu maximieren (**Maximumprinzip**). Und es kann auch das **Optimalprinzip** (Rationalprinzip) angewandt werden, bei dem sowohl Aufwand als auch Ergebnis variabel sind und man versucht die geeignetste Kombination aus beidem zu finden indem das Verhältnis zwischen Aufwand und Ergebnis optimiert wird.[94]

Im Zusammenhang mit dem Thema Compliance, sowie den damit verbundenen Risiken und Chancen, erweckt die Betrachtung im Zusammenhang mit dem **Optimalprinzip** in dieser Arbeit unser interessant. Denn zum erfolgreichen Management von Risiken und Chancen kann der **risikobasierte Ansatz** herangezogen werden, der das risikobasierte Denkens als Basis in Unternehmens-Steuerungssystemen und den Entscheidungsprozessen der Organisationen fordert. Dabei lassen sich die, von einem Unternehmen angestrebtem bzw. geplantem Ergebnisse, hinsichtlich ihres erfolgreichen Eintretens, mit folgenden Fragen im Sinn des risikobasierten Ansatzes überprüfen[95]:

- Was wirkt sich positiv auf die positive Erzielung des Ergebnisses aus?
- Was wirkt sich negativ auf die positive Erzielung des Ergebnisses aus?
- Wodurch können die positiven Auswirkungen auf die positive Erzielung des Ergebnisses verstärkt werden?
- Wodurch können die negativen Auswirkungen auf die positive Erzielung des Ergebnisses reduziert werden?
- Wie können kontinuierlich Verbesserungen erzielt werden?

---

[92] vgl Piekenbrock, D., Henning, A. (2013): Einführung in die Volkswirtschaftslehre und Mikroökonomie, 2. Aufl, Berlin Heidelberg, Springer-Verlag, S. 4
[93] vgl Mankiw, N. G., Taylor M. P. (2012): Grundzüge der Volkswirtschaftslehre, 5. Aufl, Stuttgart, Schäffer-Poeschler Verlag, S.5
[94] vgl Piekenbrock, D., Henning, A. (2013), S. 4
[95] vgl Quality Austria (2015): ISO 9001 Revision einfach erklärt – Konzept des "risikobasierten Denkens", http://www.qualityaustria.com/index.php?id=5085, Abfragedatum 07.08.2017

Weiters ist in diesem Zusammenhang interessant, dass der risikoorientierte Ansatz den Grundsatz der **Proportionalität** berücksichtigt. Das bedeutet, dass geeignete Maßnahmen immer in ein Verhältnis zu dem tatsächlich vorhandenen Risiko gesetzt werden.[96] Dies beschreibt auch das Optimalprinzip, bei dem, wie bereits erläutert, sowohl Aufwand als auch Ergebnis variabel sind und man versucht die geeignetste Kombination aus beidem zu finden, indem das Verhältnis zwischen Aufwand und Ergebnis optimiert wird. Und auch der Aspekt der Wirksamkeit fließt hier nun wieder mit ein.

Im Rahmen einer Wirtschaftlichkeitsbetrachtung / -untersuchung wird daher der Input dem Outcome gegenübergestellt (**Kosten-Nutzen-Analyse**). Dabei sollte klassischerweise zu Beginn eines Projektes der Nutzen in Form von Projektziel(en) bzw. Outcome definiert werden. Daraus sind im nächsten Schritt alle wirksamen, effektiven Maßnahmen zur Erreichung der Projektziele abzuleiten. Die möglichen wirksamen Maßnahmen werden dann einer Wirtschaftlichkeitsbetrachtung unterzogen. Auf Basis dieser Analyse sollten die effizientesten Maßnahmen den verantwortlichen Entscheidern zur Auswahl vorgelegt werden. Sofern nicht die effizientesten Maßnahmen gewählt werden sollten sinnvollerweise Begründungen dokumentiert werden. [97]

2.9 Zusammenfassung

Nach einer grundlegenden Erklärung von Begrifflichkeiten wurde im vorangegangenen Kapitel erklärt, dass die EU-DSGVO das Ziel verfolgt die natürliche Person im Rahmen von Verarbeitungstätigkeiten hinsichtlich der Geheimhaltung ihrer personenbezogenen Daten und ihrer Privatsphäre zu schützen. Dazu definiert sie Grundsätze und Vorgaben, denen zur Erfüllung der EU-DSGVO-Compliance bis zum 25. Mai 2018, durch alle Datenanwendungen und betroffenen Unternehmen entsprochen werden muss. Andernfalls ist mit exorbitant hohen Strafen zu rechnen. Um diese Compliance herzustellen, sind initial organisatorische und technische Maßnahmen umzusetzen, nachhaltige Prozesse einzuführen sowie das Bewusstsein bei allen Mitarbeitern für die Relevanz des Themas Datenschutz zu schärfen. Dabei handelt es sich überwiegend um IT-gestützte Compliance, aber auch um IT-Compliance.

---

[96] vgl FMA (2011): Rundschreiben zum risikoorientierten Ansatz zur Prävention von Geldwäscherei und Terrorismusfinanzierung, https://www.fma.gv.at/download.php?d=82, Abfragedatum 07.08.2017
[97] vgl Mühlenkamp, H. (2011), S.14f

Im Gesundheitswesen wird man besonders stark von der EU-DSGVO-Compliance betroffen sein, da in diesem Bereich eine große Menge an sensiblen personenbezogenen Daten verarbeitet wird und man hier ohnehin unter stetigem Kostendruck steht. Daher liegt die Überlegung nahe, zu evaluieren, neben der Vermeidung von Nachteilen auch weitere Chancen und damit verbundenen Nutzen aus dem Compliance-Vorhaben zu ziehen. Damit wäre eine Wirtschaftlichkeitsbetrachtung hinsichtlich der Kostendeckung des Compliance Vorhabens durch die zusätzliche Generierung von weiterem Nutzen möglich. Nutzen aus IT-Compliance ergibt sich in der Regel durch Faktoren wie der Steigerung von Sicherheit, Qualität und Produktivität. Weiterer Nutzen über mögliche neu erkennbare Chancen aus der EU-DSGVO werden in folgenden Kapiteln noch genauer beleuchtet.

Es wurde auch erklärt, dass jedes Compliance Vorhaben Kosten mit sich bringt. Nach einer ersten Herstellung eines rechtskonformen Zustandes und damit verbundenem positiven Wertbeitrag für das Unternehmen, bewirken Compliance-Maßnahmen oft einen negativen Wertbeitrag für Unternehmen. Dies ist zurück zu führen auf durchzuführende Kontrollen und Audits in nachhaltigen Compliance-Systemen, welche Aufwand generieren und dem Unternehmen keinen entsprechend gleichwertigen Nutzen bringen. Unter der Beachtung dieses Aspekts ist es wichtig für ein nachhaltig erfolgreiches Vorhaben zur Umsetzung der EU-DSGVO Compliance darauf zu achten, dass die Faktoren Verantwortung, Planung, Budget und Qualitätssteigerung stets gegeben sind.

Weiters wurden Grundvoraussetzungen für wirtschaftliche Vorhaben betrachte. Es konnten drei Herangehensweisen zur Konzeption eines EU-DSGVO-Compliance Projekts hinsichtlich adäquatem Outcomes und benötigtem Mitteleinsatz, identifiziert werden:

- Minimalprinzip: Es wird/werden ein oder mehrere Ziele hinsichtlich des Vorhabens zur Erreichung der EU-DSGVO-Compliance gesetzt. Nachfolgend wird das benötigte Budget ermittelt und so klein als möglich gehalten und das Projekt anforderungskonform umgesetzt.
- Maximumprinzip: Die Sparsamkeit ist die oberste Maxime. D.h. es wird ein Budget vorgegeben und die Projektziele zur Erreichung der EU-DSGVO-Compliance orientieren sich am vorgegebenen Budget.
- Optimalprinzip: Im Zusammenhang mit Compliance kann hier der risikobasierte Ansatz eigegliedert werden. Es wird ein Maß an vertretbarem Risiko definiert und daraus werden die variablen Faktoren abgeleitet: Es werden wirksame Maßnahmen für die ein optimiertes Budget vereinbart.

Letztendlich ist darauf zu achten im Rahmen einer Wirtschaftlichkeitsuntersuchung der Input dem Outcome im Sinne einer Kosten-Nutzen-Analyse gegenüber zu stellen.

3. Herausforderungen und Chancen, Kosten und Nutzen

Im diesem Kapitel wird auf Herausforderungen und Kosten bzw. Chancen und Nutzen, im Zuge der Umsetzung der EU-DSGVO-Compliance eingegangen.

3.1 Herausforderungen

Die EU-DSGVO bringt Neuerungen mit sich, die von Unternehmen bis Ende Mai 2018 umzusetzen sind. Die Datenschutzanforderungen an die Unternehmen sind dadurch deutlich gestiegen und werden aller Voraussicht nach weiter steigen. Große und vor allem komplexe, international agierende Unternehmen mit mehreren Standorten und dazugehörigen Datenströmen innerhalb der EU werden gut beraten sein, wenn sie ihre Datenschutzorganisation zukünftig über Datenschutz-Management-System (**DSMS**) sicherstellen. Über einen Managementansatz können systematische Prozesse unternehmensweit standardisiert abgebildet und gesteuert werden und eine **nachweisliche Dokumentation** dafür liegt dann ebenfalls vor. Auf diese Art kann ein **Organisationsverschulden** nachweislich ausgeschlossen werden, vor allem wenn das DSMS einem anerkannten Standard, wie der IDW PS 980 folgt.[98]

Um die Frage beantworten zu können, wie groß die Herausforderungen und der damit verbundene Aufwand für die Unternehmen tatsächlich sein werden, gilt es vorher eine andere Frage zu stellen. Denn, der zu erwartende Aufwand wird stark davon abhängen, wie gut die Datenschutzthematik in den Unternehmen bisher bereits gelebt wurde. Eine Studie von Ernest & Young, die 2016 veröffentlicht wurde, hatte zum Ziel den Reifegrad bestehender DSMS in großen deutschen sowie international agierenden Unternehmen zu erheben. Im Rahmen der Studie wurde also bewertet, wie gut der Reifegrad der Methoden und Prozesse des DSMS bei den jeweiligen Untersuchungsteilnehmern bereits ausgeprägt war.[99] Dabei wurde 2015 in Interviews mit Verantwortlichen (i.d.R. den Datenschutzbeauftragten) eine standardisierte Checkliste mit 127 Fragen aus 30 Bereichen durchgearbeitet. An der Studie nahmen 30 Teilnehmer teil, die sich über 14 Branchen verteilen. 12 daraus

[98] vgl EY (2016): Bereit für die EU-Datenschutzgrundverordnung? Studie zum Reifegrad von Datenschutzmanagementsystemen in Unternehmen, http://www.ey.com/Publication/vwLUAssets/ey-bereit-fuer-die-eu-datenschutzgrundverordnung/$FILE/ey-bereit-fuer-die-eu-datenschutzgrundverordnung.pdf, Abfragedatum 30.07.2017, S. 4, 10 und 11

[99] Bei der Untersuchung wurde dabei aber nicht beurteilt, wie gut oder schlecht die tatsächliche Erfüllung der Datenschutzvorgaben im jeweiligen Unternehmen damals bereits war. Der Fokus lag rein auf der Erhebung des Reifegrads des jeweiligen DSMS.

zählen zu den DAX 30. 47% der befragten Unternehmen verarbeiteten Gesundheitsdaten von Kunden. Alle teilnehmenden Unternehmen hatten ihren Hauptsitz in Deutschland.[100]

Die Studie zeigte erfreulicher Weise, dass die DSMS bei vielen der Studienteilnehmer bereits gut entwickelt waren. Einige der teilnehmenden Unternehmen konnten sogar ausgereifte DSMS vorweisen. Bei einem Blick auf die Details konnten aber in der Regel Optimierungspotentiale erkannt werden, vor allem in vereinzelten unterausgeprägten Bereichen, wie zum Beispiel beim Aufbau von Datenschutzauditprozessen.[101] Wesentliche Herausforderungen die im Rahmen dieser Studie im Zusammenhang mit der Datenschutzthematik identifiziert werden konnten waren folgende:[102]

- zu wenig Personen in der Datenschutzorganisation,
- Datenschutzorganisationen in internationalen Unternehmensgruppen kämpfen mit unterschiedlichen Gesetzgebungen in den jeweiligen Ländern,
- drastisch steigende Bußgelder,
- Herausforderungen bezüglich der Herstellung der Accountability („Accountability“ ist der englische Ausdruck für Rechenschaftspflicht und stellt erhöhte Anforderungen an das aktive Management des Datenschutzes, da defacto sämtliche Entscheidungen und Aktivtäten in diesem Zusammenhang zu dokumentieren sind.[103]),
- Anforderungen durch Digitalisierung und neuer Geschäftsmodelle,
- arbeitsteilige und ausgelagerte Geschäftsprozesse.

Rechenschaftspflichtig ist in erster Linie das Management. Eine unerlässliche Notwendigkeit ist es daher auch, im Rahmen der geplanten Vorhaben rund um die Herstellung der EU-DSGVO-Compliance, das **Management Commitment** einzuholen. Der sogenannte „Tone from the Top“ ist dazu erforderlich. Das oberste Management und die gesamte Führungsmannschaft müssen hinter dem Vorhaben mit seinen definierten Zielen stehen, sich dazu selbst verpflichten und diese Verpflichtung vorleben. Dies dient auch als klares Zeichen der Wichtigkeit des Themas gegenüber der Belegschaft und steigert somit die Awareness bei den Mitarbeitern. Weiters signalisiert dies Managementrückhalt gegenüber der Datenschutzorganisation sowie dem Datenschutzbeauftragten.[104] Wie bereits in **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht**

[100] vgl EY (2016), S. 31f
[101] vgl EY (2016), S. 4
[102] vgl EY (2016), S. 7-10
[103] vgl EY (2016), S. 4
[104] vgl EY (2016), S. 18

gefunden werden. beschrieben, ist dies ein wesentlicher Faktor der zum Erfolg bzw. Misserfolg von Compliance Projekten beitragen kann und steht auch mit einer ausreichenden zur Verfügung Stellung von Ressourcen in Beziehung.

Aspekte die die EU-DSGVO mit sich bringt und auf welche auch Unternehmen mit bestehenden DSMS nochmals ein Auge zur Sicherstellung der Normerfüllung werfen sollten, sind aus den Erkenntnissen auf Basis der Recherchen zu dieser Arbeit die folgenden:

3.1.1 Datenschutzbeauftragter

Anforderungen des Gesetzgebers

Der Datenschutzbeauftragte ist in der EU-DSGVO vorgesehen, er ist aber nicht für alle Unternehmen verpflichtend einzuführen. Die Stelle, sowie die damit verbundenen Aufgaben sind in der EU-DSGVO dazu aber definiert. Bisher war in Österreich kein Datenschutzbeauftragter gefordert, wenngleich es teilweise üblich war bestimmte Rollen im Unternehmen mit Datenschutzaufgaben zu betrauen. Jedenfalls gab es bisher dazu in Österreich kein einheitliches Rollenverständnis.[105]

Bestellen müssen den Datenschutzbeauftragten gemäß Art. 37 EU-DSGVO nun jedenfalls Verantwortliche bzw. Auftragsverarbeiter in folgenden Bereichen: [106]

- Behörden oder öffentliche Stellen (außer Gerichten), sowie
- Unternehmen, deren Kerntätigkeit aus der Durchführung von Verarbeitungsvorgängen besteht, die wegen Art, Umfang und/oder Zweck eine umfangreiche regelmäßige und systematische Beobachtung von Betroffenen erforderlich macht, als auch
- Unternehmen, deren Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 der EU-DSGVO oder von personenbezogenen Daten über Verurteilungen oder Straftaten gemäß Art. 10 EU-DSGVO liegt.

Der Datenschutzbeauftragte ist von der ihm zugedachten Funktion her sozusagen „der verlängerte Arm der Behörde“. Denn er gilt, wie Georg König es formuliert, als ein:

„dem behördlichen Verfahren vorgelagertes Kontrollinstrument“[107]*.*

Seine Aufgaben liegen gem. Art. 39 EU-DSGVO darin, den Verantwortlichen bzw. Auftragsverarbeiter sowie dessen Mitarbeiter hinsichtlich der Einhaltung von Gesetzen und

[105] vgl König, G. (2016): Der Datenschutzbeauftragte: Die interne Beratungs- und Kontrollfunktion, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 231
[106] vgl VO (EU) 2016/679 ABl L 2016/119, S.55
[107] König, G. (2016), S. 233

Vorschriften im Rahmen der personenbezogenen Verarbeitungstätigkeiten zu beraten bzw. zu unterrichten. Er überwacht daher die Einhaltung der Vorgaben und auch die Zuweisung von Zuständigkeiten, der Maßnahmen zur Schulung und Sensibilisierung von Mitarbeitern und der Durchführung von Datenschutz-Folgeabschätzungen.[108]

Art. 38 EU-DSGVO regelt die Stellung und Art. 39 EU-DSGVO die Aufgaben des Datenschutzbeauftragten: Betroffene können den Datenschutzbeauftragten bzgl. Anfragen zum Schutz ihrer Privatsphäre jederzeit anrufen. Er ist zur Geheimhaltung und zur Zusammenarbeit mit der Aufsichtsbehörde verpflichtet und dient ihr als Anlaufstelle. Er ist frühzeitig in alle Fragen vom Verantwortlichen bzw. Auftragsverarbeiter einzubeziehen, die mit dem Schutz personenbezogener Daten zusammenhängen. Ihm sind dabei die erforderlichen Ressourcen zur Verfügung zu stellen. Er muss Zugang zu den personenbezogenen Daten sowie Informationen über Verarbeitungstätigkeiten erhalten und er muss sich weiterbilden dürfen. Er berichtet direkt an das Top-Management und ist in der Erfüllung seiner Aufgaben als Datenschutzbeauftragter weisungsfrei sowie unkündbar. Bei seiner Bestellung ist darauf zu achten, dass etwaige andere Aufgaben der Person nicht im Interessenskonflikt zu den Aufgaben des Datenschutzbeauftragten stehen.[109] Beispielsweise wäre der herrschenden Auffassung nach ein Interessenskonflikt gegeben, wenn der IT-Leiter zugleich die Agenden des Datenschutzbeauftragten wahrnimmt.

Weiters kann gem. Art. 37 EU-DSGVO eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten bestellen. Diese muss aber von jeder Niederlassung aus leicht erreichbar sein. Dabei wird es in der Praxis um zwei Faktoren gehen: [110]

- Zum einen wie gut der Datenschutzbeauftragte tatsächlich erreichbar ist, was aber nicht zwangsläufig bedeutet, dass er physisch erreichbar sein muss. In diesem Fall sind alle andern möglichen Kommunikationsmittel, wie E-Mail, (Video-)Telefonie, Chat etc. auch in Betracht zu ziehen.
- Zum anderen muss die Verständigungsmöglichkeit hinsichtlich gemeinsamer Sprache mitberücksichtigt werden. Der Datenschutzbeauftragte muss sich sowohl mit Mitarbeitern, aber auch mit der Aufsichtsbehörde gut verständigen können. Hier wird es in der Praxis aber voraussichtlich auch reichen, wenn ein Dolmetscher ausreichend schnell greifbar ist, da sonst bei Unternehmensgruppen mit Standorten in

[108] vgl VO (EU) 2016/679 ABl L 2016/119, S.56
[109] vgl Feiler, L., Forgó, N. (2017), S. 26, vgl VO (EU) 2016/679 ABl L 2016/119, S.55f
[110] vgl König, G. (2016), S. 236

unterschiedlichen Staaten, ein Gruppen-Datenschutzbeauftragter defacto nicht möglich wäre.

Der Datenschutzbeauftragte muss jedenfalls kein unternehmensinterner Mitarbeiter sein, er kann auch extern besetzt werden. Seine Kontaktdaten sind durch den Verantwortlichen bzw. Auftragsverarbeiter zu veröffentlichen sowie der Aufsichtsbehörde mitzuteilen.[111]

Bedeutung für das Gesundheitswesen

Ob im Gesundheitswesen ein Datenschutzbeauftragter gesetzlich verpflichtend zu bestellen ist, scheint am ersten Blick diskutabel. Im Gesundheitswesen könnte man argumentieren, dass die Verarbeitung von Gesundheitsdaten nicht zur Kerntätigkeit des stationären Krankenversorgers zählt, sondern eine Nebentätigkeit darstellt, denn es wurde nicht klar in der EU-DSGVO geregelt was als Neben- oder Haupttätigkeit zu verstehen ist. Die Frage ist, ob die Tätigkeit als unumgängliche Voraussetzung für die Kerntätigkeit des Unternehmens notwendig ist.[112] So betrachtet ist in der heutigen Zeit klar ableitbar, dass die medizinische Versorgung von Patienten in der stationären Krankenversorgung ohne entsprechende Datenverarbeitung nur eingeschränkt bis gar nicht möglich wäre. Das Gesundheitswesen fällt der herrschenden Meinung nach daher unter diese Regelung, dass ein Datenschutzbeauftragter gesetzlich verpflichtend zu bestellen ist.

So oder so steht aber außer Streit, dass alleine aufgrund der angedrohten Strafausmaße es jedenfalls empfehlenswert ist einen Datenschutzbeauftragten oder eine andere verantwortliche Person mit der Überprüfung der Einhaltung der Vorgaben der EU-DSGVO zu beauftragen.[113] Strafen für Verstöße gegen die Regelungen zum Datenschutzbeauftragten (Art. 37-39 EU-DSGVO) werden mit Geldbußen von bis zu € 10 Mio. bzw., falls dies höher ist, mit 2% des gesamten weltweiten Jahresumsatzes der Unternehmensgruppe bemessen am vergangenen Geschäftsjahr sanktioniert.[114]

3.1.2 Register der Verarbeitungstätigkeiten

Anforderungen des Gesetzgebers

In dieser neu geschaffenen Regelung wurden durch die EU-DSGVO die Aufgaben der Behörde zu den Unternehmen verlegt. Denn bisher führte die Datenschutzbehörde das Da-

[111] vgl VO (EU) 2016/679 ABl L 2016/119, S.55
[112] Siehe dazu auch Erwägungsgrund Nr. 97 zur EU-DSGVO in: Pollirer, H.-J., Weiss, E., Knyrim, R., Haidinger, V. (Hrsg) (2017), S. 100f
[113] vgl Pollirer, H-J. (2015): Die Datenschutz-Grundverordnung: Der Datenschutzbeauftragte (Teil II), Dako 2015/37 Heft 3/2015, S.65
[114] vgl König, G. (2016), S. 240

tenverarbeitungsregister. Dorthin mussten Unternehmen früher Datenanwendungen[115] mit Personendatenbezug melden. Zukünftig ist die Verantwortung zur Erstellung des Verarbeitungsregisters beim Unternehmer. Das Verarbeitungsregister im Sinne der EU-DSGVO muss sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter geführt werden. Darin sind jene Verarbeitungstätigkeiten aufzuführen, die der jeweiligen Zuständigkeit unterliegen.[116]

Es gibt auch Ausnahmen von der Regelung zur verpflichtenden Führung eines Verarbeitungsregisters. Wenn ein Unternehmen weniger als 250 Mitarbeiter beschäftigt, unabhängig davon ob es sich dabei um Vollzeit- oder Teilzeitarbeitskräfte handelt, ist es von der Verpflichtung befreit, sofern nicht eine der folgenden Restriktionen greift: [117]

- Wenn eine Verarbeitungstätigkeit ein Risiko für die Rechte und Freiheiten des Betroffenen darstellt, dann ist das Unternehmen nicht von der Pflicht entbunden.
  Beispiel: Eine Videoüberwachung kommt in einem Unternehmen mit weniger als 250 Mitarbeitern zum Einsatz. Diese Verarbeitungstätigkeit ist in einem Verarbeitungsregister zu führen.
- Weiters ist ein Verarbeitungsregister zu führen, wenn eine Verarbeitungstätigkeit nicht nur gelegentlich erfolgt (z.B. nur einmal im Monat).
  Beispiel: neue Mitarbeiter werden in einem Unternehmen mit weniger als 250 Mitarbeitern für die Erstellung eines Mitarbeiterausweises fotografiert. Diese Verarbeitungstätigkeit ist in einem Verarbeitungsregister zu führen.
- Es ist ebenfalls dann eine Verpflichtung da, ein Verarbeitungsregister zu führen, wenn besondere Datenkategorien verarbeitet werden. Dies betrifft gem. Art. 9 Abs. 1 EU-DSGVO als sensibel definierte Daten, sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 EU-DSGVO.
  Beispiel: Auch in einem kleinen Gesundheitsbetrieb, in welchem weniger als 250 Mitarbeiter beschäftigt sind, ist ein Verarbeitungsregister zuführen, da dort Gesundheitsdaten verarbeitet werden.

[115] Auch hier war mit dem Begriff Datenanwendung nicht zwangsläufig ein Software-Programm gemeint, sondern die Anwendung im Sinne der Verarbeitungstätigkeit; vgl DSB (2017): Meldung beim Datenverarbeitungsregister, https://www.dsb.gv.at/meldung-beim-dvr, Abfragedatum 20.08.2017
[116] vgl Selk, R. (2016): Verzeichnis von Verarbeitungstätigkeiten (Art 30 DSGVO): Wer muss es haben, wie hat es auszusehen?, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 181
[117] vgl Feiler, L., Forgó, N. (2017), S. 22, vgl Selk, R. (2016), S. 184ff

Im Verzeichnis der Verarbeitungstätigkeiten ist schriftlich zu führen und kann daher auch elektronisch geführt werden. Folgende Informationen sind gem. Art. 30 EU-DSGVO im Verarbeitungsregister zu erfassen[118]:

- Name und Kontaktdaten des Verantwortlichen und ggf. weiterer Verantwortlicher,
- Name und Kontaktdaten des Auftragsverarbeiters (wenn dieser das Register führt) inkl. der Kategorien von Verarbeitungen die dieser für den Verantwortlichen vornimmt,
- Name und Kontaktdaten des Datenschutzbeauftragten (nur vom Verantwortlichen zu führen),
- Zweck der Verarbeitung (nur vom Verantwortlichen zu führen),
- Beschreibung der Kategorien von Betroffenen (nur vom Verantwortlichen zu führen),
- Beschreibung der Kategorien von betroffenen personenbezogenen Datenarten und ihrer Löschungsfristen (wenn möglich),
- Kategorien von Empfängern mit der Information über etwaigen Sitz im Drittland bzw. ihrem Status als internationale Organisation,
- sofern personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden, ist das Drittland bzw. die Organisation zu nennen und es sind die geeigneten Garantien anzuführen sofern Art. 49 Abs. 1 Unterabsatz 2[119] EU-DSGVO eintritt,
- eine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 EU-DSGVO, der die "Sicherheit der Verarbeitung" regelt (siehe dazu auch 3.1.6 Informationssicherheit nach dem Stand der Technik).

Die Idee hinter dem, das Verarbeitungsregister regelnden Art. 30 der EU-DSGVO, liegt im Nachweis der Einhaltung der Verordnung, da die Datenschutzbehörde jederzeit berichtigt ist die Vorlage des Registers anzufordern. Die Erstellung des Registers zählt im Übrigen nicht zu den per Gesetzt definierten Pflichten des Datenschutzbeauftragten. [120]

[118] vgl VO (EU) 2016/679 ABl L 2016/119, S.50f
[119] Anmerkung: hier scheint ein Fehler in der Referenzierung der Absätze innerhalb dieses Artikels im Gesetz vorzuliegen. An mehreren Stellen wird auf Absatz 1 und einen jeweiligen Unterabsatz verwiesen. Die Absätze scheinen aber den Unterabsätzen zu entsprechen. Auch logisch scheint es sich tatsächlich um Art. 49 Abs. 2 EU-DSGVO zu handeln.
[120] vgl Selk, R. (2016), S. 182

Bedeutung für das Gesundheitswesen

Das Besondere im Gesundheitswesen wird sein, dass hier sehr viele Verarbeitungstätigkeiten sensible personenbezogene Daten betreffen. Dies bedeutet in weiterer Folge, dass sehr viele Datenschutz-Folgeabschätzungen durchgeführt werden müssen. Jedes kleine Pflegeheim, auch mit unter 250 Mitarbeitern, wird ein Verarbeitungsverzeichnis führen müssen. Werden die Vorgaben in diesem Zusammenhang nicht erfüllt, so wird mit dem Strafausmaß von € 10 Mio. bzw. 2% Konzernumsatz sanktioniert.[121]

3.1.3 Datenschutz-Folgeabschätzung / Privacy-Impact-Assessment

Anforderungen des Gesetzgebers

Die Datenschutz-Folgenabschätzung, auch Privacy Impact Assessment (kurz PIA) genannt, ist vor allem dann vorgesehen, wenn neue Technologien verwendet werden, die ein hohes Risiko für den Betroffenen hinsichtlich des Schutzes seiner Privatsphäre bergen.[122] Dies hat sich aufgrund der Art, des Umfangs, der Umstände oder des Zwecks der Verarbeitung zu ergeben.[123]

Der Verantwortliche gem. Art. 35 EU-DSGVO hat in diesem Fall eine Abschätzung der Folgen der vorgesehenen Verarbeitungstätigkeiten für den Schutz personenbezogener Daten durchzuführen. Zu der Entscheidung ob eine PIA tatsächlich durchzuführen ist muss der Verantwortliche selbst kommen. Dabei kann er auch feststellen, dass es ausreichend ist, für mehrere ähnliche Verarbeitungstätigkeiten mit ähnlichem Risiko eine einzige PIA durchzuführen.[124] Eine PIA ist jedenfalls dann durchzuführen, wenn die gem. Art. 35 Abs. 3 EU-DSGVO genannten Bedingungen erfüllt sind[125]:

- wenn eine Bewertung persönlicher Aspekte von natürlichen Personen erfolgt (z.B. im Zuge von automatisierten Profiling-Abläufen) und diese Bewertung als Grundlage für Entscheidungen herangezogen wird, die in weiterer Folge Rechtswirkung gegenüber der Person entfalten oder die Person in ähnlich erheblicher Weise beeinträchtigen,
- wenn eine umfangreiche Verarbeitung von sensiblen Daten oder von personenbezogenen Daten über strafrechtlich Verurteilungen und Straftaten erfolgt oder
- wenn eine Überwachung öffentlich zugänglicher Bereiche erfolgt.

---

[121] vgl Selk, R. (2016), S. 182
[122] vgl Pollirer, H-J. (2015a): Die Datenschutz-Grundverordnung: Die Datenschutz-Folgenabschätzung (Teil III), Dako 2015/47 Heft 4/2015, S.89
[123] vgl Trieb, G. (2016): Datenschutz-Folgeabschätzung und vorherige Konsultation der Aufsichtsbehörde: Von der Registrierungspflicht zur weitgehenden Selbstregulierung, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 219f
[124] vgl Trieb, G. (2016), S. 218 und 220
[125] vgl VO (EU) 2016/679 ABl L 2016/119, S.53

Bei der Durchführung einer PIA ist jedenfalls gem. Art. 35 Abs. 2 EU-DSGVO der Rat des Datenschutzbeauftragten, sofern vorhanden, einzuholen. Weiters sind folgende Prüfschritte im Rahmen einer PIA gemäß Art. 35 Abs. 7 EU-DSGVO zu absolvieren:[126]

1. Beschreibung der Merkmale der Verarbeitungstätigkeit sowie des Zwecks der Verarbeitung inkl. etwaiger berechtigter Interessen,
2. Bewertung der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitungsvorgänge im Hinblick auf den Zweck der Verarbeitung,
3. Ermittlung der Risiken aus Betroffenensicht hinsichtlich des Schutzes seiner Rechte und Freiheiten,
4. Mittel zur Bewältigung der Risiken (geplante Maßnahmen zur Abhilfe, Garantien, Sicherheitsvorkehrungen) und Verfahren die den Schutz der Daten sicherstellen und den Nachweis dafür erbringen.

Wenn der Verantwortliche nach Absolvierung der PIA-Prüfschritte zu der Erkenntnis gelangen sollten, dass trotz der getroffenen organisatorischen und technischen Maßnahmen die im vertretbaren Rahmen hinsichtlich verfügbarer Technologien und Implementierungskosten anzusiedeln sind, immer noch ein erhöhtes Risiko für den Betroffenen verbleibt, dann hat er die Aufsichtsbehörde zu konsultieren. Dies wird auch als „**vorherige Konsultation**“ bezeichnet (Art. 36 EU-DSGVO). Die Verordnung verfolgt dabei zwei Ziele: Zum einen kann im Falle einer geplanten Verarbeitungstätigkeit mit nicht vertretbarem Risiko für den Betroffenen, durch die Aufsichtsbehörde zu adäquaten Maßnahmen und Mitteln beraten werden. Andererseits kann die Behörde, wenn keine Maßnahmen und Mitteln mehr helfen, eine Verarbeitungstätigkeit dieser Art noch rechtzeitig verhindern, weil verbieten.[127]

<u>Bedeutung für das Gesundheitswesen</u>

Nicht für alle personenbezogenen Daten ist die Durchführung einer PIA relevant. Bei der Verarbeitung von Gesundheitsdaten wird die verpflichtende Durchführung einer PIA aber jedenfalls gefordert sein. Denn unter Art. 35 Abs. 3 lit. b EU-DSGVO fällt die umfangreiche Verarbeitung von Gesundheitsdaten. Dies trifft auf sämtliche Verarbeitungstätigkeiten in der stationären Krankenversorgung zu.[128]

[126] vgl Trieb, G. (2016), S. 222, vgl Pollirer, H-J. (2015a), S.90ff
[127] vgl Trieb, G. (2016), S. 218f und 227
[128] vgl Trieb (2016), S. 221

3.1.4 Erfüllung der Betroffenenrechte

Im Zuge der Erarbeitung der EU-DSGVO wurden die Betroffenenrechte neu geregelt. Dabei wurden das Auskunfts-, Richtigstellungs- und Löschungsrecht überarbeitet. Neu hinzugekommen, sind das Recht auf Vergessenwerden und das Recht auf Datenübertragbarkeit.[129]

Regelung der Modalitäten und Transparenz

Im Art. 12 EU-DSGVO werden allgemeine Regelungen hinsichtlich der Kommunikation vorgegeben. Diese Regelungen gelten für die nachfolgend beschriebenen Rechte, die in den Art. 13 bis 22 EU-DSGVO geregelt sind sowie für Art. 34 EU-DSGVO (Meldungen an Betroffene im Rahmen eines Datenschutzvorfalls).

Der Verantwortliche hat es dem Betroffenen gegenüber möglichst einfach zu machen eine Anfrage einzubringen. Die Anfrage, sofern keine exzessiven oder unbegründeten Anfragen durch den Antragsteller eingehen oder aufwändige mehrfache Datenkopien angefordert werden, ist kostenlos zu beantworten. Für die Anfrage ist keine Schriftlichkeit gefordert und auch kein aktiver Nachweis der Identität durch den Betroffenen. Auf Wunsch des Betroffenen kann die Auskunft auch mündlich erfolgen. Nur im berechtigten Zweifelsfall durch den Verantwortlichen, z.B. bei der Verwendung von Fantasie E-Mail-Adressen oder einem rein telefonischen Ansuchen, darf gem. Art. 12 Abs. 6 EU-DSGVO der Verantwortliche zusätzliche Informationen zur Bestätigung der Identität einfordern, wie eine Ausweiskopie. Die Anfrage ist dann unverzüglich zu beantworten, spätestens aber nach einer Frist von einem Monat. Der Verantwortliche hat dem Betroffene alle Informationen zur Verarbeitung in präziser, transparenter, verständlicher und leicht zugänglicher Form zur Verfügung zu stellen. Wenn es besonders gute Gründe bei der Bearbeitung komplexer Anfragen gibt, dann sind diese gem. Art. 12 Abs. 3 EU-DSGVO dem Antragsteller binnen eines Monats zu nennen und dadurch kann die Frist auf zwei Monate verlängert werden. Es gibt wenig Gründe (z.B. unbegründete oder zu exzessive Anfragen durch den Antragsteller) unter denen der Verantwortliche berechtigt ist die Auskunft zu verweigern. Sofern er dies aber tut hat er dem Betroffenen innerhalb einer Frist von einem Monat zu informieren, ihm die Gründe zu nennen sowie ihn über die Möglichkeit der Beschwerde bei der Aufsichtsbehörde bzw. den Rechtsweg zu informieren.[130]

---

[129] vgl Wagner, B. (2015): Die Datenschutz-Grundverordnung: die Betroffenenrechte (Teil IV), Dako 2015/59 Heft 5/2015, S.112

[130] vgl Haidinger, V. (2016): Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertrag-barkeit und Widerspruch (Art 15-21 DSGVO), in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S.125-128, vgl VO (EU) 2016/679 ABl L 2016/119, S.39f

Im Kontext dieser allgemeinen Vorgaben sind die weiteren folgenden Rechte zu erfüllen:

Recht auf Information

Wenn Informationen zu einer natürlichen Person erhoben werden, dann ist diese Person darüber zu informieren. Wenn die Daten direkt bei dieser Person erhoben werden, dann hat der Verantwortliche gem. Art. 13 EU-DSGVO dem Betroffenen folgende Informationen mitzuteilen:[131]

- Name und Kontaktdaten des Verantwortlichen bzw. Vertreters,
- Kontaktdaten des Datenschutzbeauftragten sofern vorhanden,
- Zweck und Rechtsgrundlage der Verarbeitung der erhobenen Daten,
- Die Angabe des berechtigten Interesses des Verantwortlichen oder Dritten, falls die Verarbeitung sich auf Art. 6 Abs. 1 lit. f EU-DSGVO stützt und die Interessen oder Grundrechte bzw. -freiheiten des Betroffenen nicht überwiegen,
- ggf. die Empfänger oder Kategorien daraus,
- Bekanntgabe der Absicht des Verantwortlichen die Daten an ein Drittland oder eine internationale Organisation zu übermitteln mit den fallweise benötigten Formalien wie Garantien.

Zusätzlich hat der Verantwortliche, zum Zeitpunkt der Erhebung noch weiterführende Informationen bekanntzugeben, um eine faire und transparente Verarbeitung zu gewährleisten. Er hat den Betroffenen beispielsweise über die Dauer der Speicherung, sämtliche Rechtsansprüche (wie z.B. Auskunftsrecht, Recht auf Vergessenwerden, Beschwerderecht bei der Aufsichtsbehörde) über die Logik von Profiling-Anwendungen zur automatisierten Entscheidungsfindung zu informieren. Er hat auch alle weiteren Zwecke der Verarbeitung der personenbezogenen Daten zu nennen, sofern solche vorliegen.[132]

Wenn die Informationen nicht bei der natürlichen Person selbst erhoben werden, dann sind gem. Art. 14 EU-DSGVO nahezu dieselben Informationen mitzuteilen wie sie oberhalb bereits zum Art. 13 EU-DSGVO punktuell aufgezählt wurden. Zusätzlich sind die Kategorien der verarbeiteten personenbezogenen Daten sowie die Quelle, aus der diese stammen nennen.[133]

---

[131] vgl VO (EU) 2016/679 ABl L 2016/119, S.40f
[132] vgl VO (EU) 2016/679 ABl L 2016/119, S.41
[133] vgl Feiler, L., Forgó, N. (2017), S. 16

Recht auf Auskunft

Art. 15 EU-DSGVO regelt, dass dem Betroffenen eine Bestätigung darüber auszuhändigen ist, ob die Personen betreffende personenbezogene Daten verarbeitet werden. Wenn keine Daten über die Person bearbeitet werden, ist dem Betroffenen eine Negativauskunft zu erteilen. Wenn Daten vorliegen und auch keine Ausnahmen hinsichtlich des Auskunftsrechts gelten, dann sind folgende Informationen durch den Verantwortlichen zu beschaffen bzw. auszuhändigen:[134]

- Verarbeitungszwecke,
- Kategorien der verarbeiteten Daten,
- Die Empfänger bzw. die Kategorien von Empfängern, an welche die Daten weitergegeben wurden, vor allem jene im Drittland bzw. internationale Organisationen,
- Wenn möglich, die geplante Dauer der Speicherung der Daten, jedenfalls aber die Kriterien für die Festlegung dieser Dauer,
- Die Information ob ein Recht auf Löschung, Berichtigung, Einschränkung der Verarbeitung bzw. eine Widerspruchsrecht gegen die Verarbeitung oder Beschwerderecht an die Aufsichtsbehörde besteht,
- Informationen über die Herkunft der erhobenen Daten, falls diese nicht beim Betroffenen selbst erhoben wurden,
- Auskünfte über die verwendete Logik und die Tragweite bei Verarbeitungstätigkeiten mit automatisierter Entscheidungsfindung wie dem Profiling,
- Bei internationalen Datentransfers: die Grundlage geeigneter Garantien,
- Kopien der Daten.

Recht auf Berichtigung

Gem. Art. 16 EU-DSGVO hat der Betroffene ein Recht auf Korrektur bzw. Ergänzung falscher personenbezogener Daten. Beispielsweise, wenn der Betroffene erkennt, dass ein falsches Geburtsdatum zu seiner Person gespeichert wurde oder Informationen zur Wohnadresse unvollständig sind. Der Verantwortliche hat die unzutreffenden Daten zu berichtigen.[135]

Art. 19 EU-DSGVO regelt dazu, dass Unternehmen denen Daten des Betroffenen weitergegeben wurden zu informieren sind, wenn dieses Recht oder die nachfolgende erklärten Rechte auf Löschung und Einschränkung der Verarbeitung, geltend gemacht wurden.[136]

---

[134] vgl Haidinger, V. (2016), S.127, vgl VO (EU) 2016/679 ABl L 2016/119, S.43
[135] vgl Haidinger, V. (2016), S.129
[136] vgl Haidinger, V. (2016), S.134

Recht auf Löschung („Recht auf Vergessenwerden“)

Art. 17 EU-DSGVO regelt das Recht auf Löschung, auch als Recht auf Vergessenwerden benannt. Dadurch hat der Betroffene das Recht auf unverzügliche Löschung seiner personenbezogenen Daten, wenn die Verarbeitung in einer Form erfolgt, dass die EU-DSGVO dadurch verletzt wird. Zum Beispiel dann, wenn der Betroffene seine Einwilligung zur Verarbeitung widerrufen hat.[137] Interessanterweise sind die Unterschiede zu den bisherigen Regelungen des DSG 2000 nicht als zu groß.[138] Den wesentlichen Unterschied macht wohl das neue Strafausmaß aus, denn dieses Recht war ein viel Diskutiertes im Rahmen der Verabschiedung der EU-DSGVO, vor allem im Bereich der Social Media und Online Service Anbieter.

Recht auf Einschränkung der Verarbeitung

Gem. Art. 18 EU-DSGVO hat der Betroffene auch einen Anspruch auf Einschränkung der Datenverarbeitung für eine gewisse Dauer. Dabei darf der Verantwortliche die Daten nur noch Speichern, sie aber nicht mehr verarbeiten, wenn die Zustimmung der betroffenen Person dazu fehlt oder ein sonstiger Rechtsanspruch. Beispielsweise kann der Betroffene das Recht auf Einschränkung geltend machen, wenn er die Richtigkeit seiner Daten bestreitet. Für den Zeitraum der Überprüfung der Richtigkeit der Daten kann der Betroffene verlangen, dass die Verarbeitung der Daten einzuschränken ist. [139]

Recht auf Datenübertragbarkeit

Im Art. 20 EU-DSGVO wir das Recht auf Datenüberübertragbarkeit, auch Recht auf Portabilität genannt, geregelt. Dies besagt, dass dem Betroffenen Daten, die der Betroffene dem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten hat. Dies soll dem Zweck dienen, dass er diese Daten ohne Behinderung an einen anderen Verarbeiter weitergeben kann. Und der Betroffene hat auch das Recht zu verlangen, dass der Verantwortliche die Daten direkt an den neuen Verarbeiter übergibt, sofern dies technisch machbar ist.[140] Erwähnenswert ist auch, dass der Betroffene diesen Anspruch gegenüber dem Verantwortlichen, aber nicht gegenüber dem Auftragsverarbeiter hat.[141]

[137] vgl Feiler, L., Forgó, N. (2017), S. 18
[138] vgl Haidinger, V. (2016), S.131f
[139] vgl Haidinger, V. (2016), S.133
[140] vgl Haidinger, V. (2016), S.134
[141] vgl Feiler, L., Forgó, N. (2017), S. 17

Widerspruchsrecht

Im Art. 21 EU-DSGVO ist geregelt, dass der Betroffene das Recht hat Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten einzulegen, wenn diese für eine Aufgabe im öffentlichen Interesse oder im berechtigten Interesse des Verantwortlichen oder Dritten erfolgt. Er muss den Widerspruch aber so argumentieren können, dass er Gründe hat die sich aus seiner besonderen Situation ergeben und die gegen die Verarbeitung der Daten sprechen. Im Rahmen von Direktmarketing besteht ein absolutes Widerspruchsrecht.[142]

Automatisierte Entscheidung im Einzelfall einschließlich Profiling

Auch zum Thema Profiling gibt es hier eine Regelung. In Art. 22 Abs. 1 EU-DSGVO wir definiert, dass der Betroffene nicht ausschließlich einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung (worunter auch Profiling fällt) unterworfen werden darf, sofern diese ihm gegenüber in weiterer Folge eine rechtliche Wirkung entfalten würde oder sie in ähnlicher Weise erheblich beeinträchtigt.[143] Ein Beispiel dafür wäre, dass die Krankenversicherung einen Selbstbehalt geltend macht, wenn die Smartphone-App keinen signifikanten Fortschritt bei der Tele-Therapie verzeichnet.

Bedeutung der Betroffenenrechte für das Gesundheitswesen

Rein organisatorisch gesehen werden an stationäre Krankenversorger durch die erweiterten Betroffenenrechte Anforderungen gestellt. Im Folgenden werden exemplarisch ein paar erkennbare Themen aufgezählt:

Allen voran muss erhoben werden, wie weit die Regelungen das jeweilige Gesundheitsunternehmen betreffen. Denn auch vor sortierten Papierakten, die es im Keller so manch einer Gesundheitseinrichtung noch gibt, macht die neue Verordnung nicht halt. Die Umsetzung der Betroffenenrechte, auch für diese Dokumente mit zu berücksichtigen, kann durchaus aufwendig werden.

Weiters ist es notwendig, für jede Anfrage hinsichtlich Gesundheitsdaten zu prüfen ob die vorliegende Bestätigung der Identität ausreichend ist. Das Gesetz gibt vor hier keine zu großen Hürden für den Betroffenen zu schaffen. Zu unbedarfte Handhabungen solcher Anfragen würden Social Engineering Angriffen aber Tür und Tor öffnen. Vor allem im Umgang mit sensiblen Daten, wie Gesundheitsdaten, wird es bestimmt notwendig sein sich hier einen Prozess für eine sichere und effiziente Handhabung von Anfragen zu überlegen. Weiters muss geprüft werden, ob alle Informationen entsprechend Rechts auf Aus-

[142] vgl Haidinger, V. (2016), S.135, vgl VO (EU) 2016/679 ABl L 2016/119, S.45
[143] vgl VO (EU) 2016/679 ABl L 2016/119, S.46

kunft ausgegeben werden können bzw. auch das Recht auf Datenübertragbarkeit erfüllt werden kann.

Auch Patientenbehandlungsverträge werden einer Prüfung und einer Überarbeitung bedürfen, damit diese den Anforderungen der EU-DSGVO hinsichtlich der Vorgaben zu Modalitäten bzw. der Transparenz sowie dem Recht auf Information entsprechen.

Viele Applikationen im Gesundheitswesen sind derzeit auch so konzipiert und implementiert, dass sie – durch die sehr langen Aufbewahrungsfirste, z.B. 30 Jahre für Patientendaten im stationären Bereich – keine Löschung der Daten vorsehen. Im Gegenteil, diese Applikationen gelten als revisionssicher. Es ist jede Behandlung zu jedem Patienten zu dokumentieren und mit jeder durchführenden behandelnden Person zu verzeichnen. Daher werden derzeit diese Daten in der Regel im System in sich unveränderbar und nicht löschbar gespeichert. Es wird notwendig sein gemeinsam mit dem Hersteller Wege zu finden um diese Daten dennoch nach Ablauf der jeweiligen Speicherfristen zu löschen.

Weiters muss die Rechenschaftspflicht zu all diesen Themen eingehalten werden. Das bedeutet zusätzlichen Dokumentationsaufwand, der nicht unerheblich sein wird. Ein Beispiel ist, die nachvollziehbare Dokumentation des Entzugs sowie der Vergabe von Berechtigungen auf Patientenakten im Krankenhausinformationssystem (KIS) für unterschiedliche behandelnder Ärzte in einem Krankenhaus. Und dabei ist zu bedenken, dass es in Krankenhäusern ohnehin eine Menge Dokumentations- und Nachweispflichten gibt, wie im Bereich der Patientenaufklärung oder im medizinischen Qualitätsmanagement.[144]

3.1.5 Melden von Datenschutzvorfällen

Bei einem Datenschutzvorfall, bzw. sogenannten **Data Breach**, handelt es sich um eine Datenpanne, bei der eine natürliche Person einen physischen, materiellen oder immateriellen Schaden erleidet. Darunter fallen Situationen[145] in denen die natürliche Person die Kontrolle über die personenbezogenen Daten verliert oder es zu einer Einschränkung ihrer Rechte kommt. Oder wenn es weiters zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, finanziellen Verlusten, unbefugter Aufhebung der Pseudonymisierung, Rufschädigung, dem Verlust der Vertraulichkeit von Daten die dem Berufsgeheimnis unterliegenden oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen für

[144] vgl Meyer, S. (2017), S.28 u. 31

[145] vgl Erwägungsgrund Nr. 85 zur EU-DSGVO in: Pollirer, H.-J., Weiss, E., Knyrim, R., Haidinger, V. (Hrsg) (2017), S. 88f

den Betroffenen kommt.[146] Ein Data Breach ist gem. Art. 33 und 34 EU-DSGVO unverzügliche den Betroffenen und innerhalb von 72h an die Aufsichtsbehörde zu melden.[147]

Folgende Informationen muss eine **Meldung an die Aufsichtsbehörde** gem. Art. 33 Abs. 1 EU-DSGVO jedenfalls beinhalten [148]:

- Beschreibung der Verletzungsart inkl. Angabe der Kategorien der Betroffenen und Datensätze sowie ungefähren Betroffenen- bzw. Datensatzanzahl (sofern möglich),
- Name und Kontaktdaten des Datenschutzbeauftragten für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen aus der Verletzung,
- Beschreibung der ergriffenen bzw. vorgeschlagenen Maßnahmen zur Behebung und ggf. Maßnahmen zur Abmilderung der nachteiligen Auswirkungen

Die Informationen können auch sukzessiv and die Aufsichtsbehörde übermittelt werden, wenn nicht alle Informationen zum Zeitpunkt der Meldung zur Verfügung stehen. Die Meldung muss jedenfalls innerhalb der vorgesehenen Frist erfolgen.[149] Damit die Aufsichtsbehörde im Nachhinein auch überprüfen kann, ob alle Bestimmungen eingehalten wurden, hat der Verantwortliche die Verletzung sowie alle im Zusammenhang stehenden Fakten, Auswirkungen und ergriffenen Abhilfemaßnahmen zu dokumentieren.[150]

Die **Meldung an den Betroffenen** muss gem. Art. 34 EU-DSGVO klar und einfach formuliert werden. Dabei müssen ebenfalls die Informationen angeführt werden die im obigen Absatz gem. Art. 33 EU-DSGVO der Aufsichtsbehörde zu melden sind.[151]

<u>Bedeutung für das Gesundheitswesen</u>

Hier wurden im Kontext des Gesundheitswesens keine Besonderheiten im Vergleich zu Unternehmen in anderen Branchen erkannt. Aber natürlich ist zu bedenken, dass hier mit besonders sensiblen Daten agiert wird und dass ein Data Breach, wenn er der Öffentlichkeit zu melden ist, einen großen Imageverlust für die betroffene Gesundheitseinrichtung darstellen kann. Man muss diesbezüglich daher auch bedenken die Unternehmenssprecher / -kommunikation in das Aufsetzen eines solchen Prozesses miteinzubeziehen.

---

[146] vgl Oman, M. (2016): Daten weg – was nun? Data Breaches und ihre DSGVO-Folgen gem Art 33,34 DSGVO, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 210
[147] vgl Oman, M. (2016), S. 209
[148] vgl VO (EU) 2016/679 ABl L 2016/119, S.52
[149] vgl Feiler, L., Forgó, N. (2017), S. 29
[150] vgl Oman, M. (2016), S. 215
[151] vgl VO (EU) 2016/679 ABl L 2016/119, S.53

3.1.6 Informationssicherheit nach dem Stand der Technik

Datenschutz bedarf Datensicherheit. Datensicherheit beschäftigt sich mit der Sicherstellung der **Vertraulichkeit, Verfügbarkeit und Integrität** von Daten. Wofür diese Begriffe stehen erklärt Pollirer wie folgt:[152]

„Integrität: Informationen dürfen nur von den vorgesehenen Personen und Prozessen verändert werden;

Vertraulichkeit: Informationen dürfen nur für die vorgesehenen Personen und Prozesse offengelegt werden;

Verfügbarkeit: Informationen müssen für die vorgesehenen Personen und Prozesse bereitgestellt werden, wenn diese sie benötigen;“

Der Datensicherheit wird in der EU-DSGVO mehr Beachtung geschenkt, als zuvor im Rahmen des DSG 2000. Bereits in den Grundsätzen der Verarbeitung (Art. 5 EU-DSGVO) wurde die Pflicht festgehalten, geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Datensicherheit zu ergreifen. [153]

Art. 32 EU-DSGVO regelt die Sicherheit der Verarbeitung personenbezogener Daten. Gemäß der Vorgabe sind folgende Faktoren vom Verantwortlichen bzw. Auftragsverarbeiter zu berücksichtigen bzw. sind technische und organisatorische Maßnahmen zu ergreifen, um dem Risiko des Betroffenen angemessenes Schutzniveau zu gewährleisten: [154]

- Stand der Technik („state of the art“),
- Implementierungskosten,
- Umstände und Zweck der Verarbeitung, sowie
- Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Viele der eben verwendeten Begrifflichkeit lassen viel Interpretationsspielraum zu. Der Leser der Verordnung fragt sich, ab wann das Schutzniveau dem Risiko angemessen ist und auch die Erklärung, dies an Eintrittswahrscheinlichkeit und Schwere des Risikos für den Betroffenen sowie dem Stand der Technik etc. festzumachen scheint nicht sehr hilfreich. Daher ist in den Erwägungsgründen zur Verordnung festgehalten, dass der Ausschuss Leitlinien für Verarbeitungstätigkeiten herausgeben kann, um darin festzuhalten

[152] Pollirer, H.-J. (2016): Sicherheit der Verarbeitung (Art 32 DSGVO), in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 201
[153] vgl Pollirer, H.-J. (2016), S. 199
[154] vgl VO (EU) 2016/679 ABl L 2016/119, S.51

wann aus seiner Sicht ein hohes Risiko für die Rechte und Freiheiten des Betroffenen vorliegen. Dies kann auch in der umgekehrten Form erfolgen, so dass der Ausschuss vorgibt wann aus seiner Sicht davon auszugehen ist, dass kein hohes Risiko besteht.[155]

Weiters führt die EU-DSGVO im Art. 32 Abs. 1 **Maßnahmen** an, die zur Erreichung der Datensicherheit zu setzen sind: [156]

„[…] 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. […]“

In diesem Kontext werden wir mit zwei weiteren neuen Begriffen konfrontiert „Belastbarkeit“ und „Pseudonymisierung“:

Die **Belastbarkeit** ist ein weiteres Kriterium, das die EU-DSGVO neben Verfügbarkeit, Vertraulichkeit und Integrität einfordert. Es steht aber eng mit dem Kriterium Verfügbarkeit in Zusammenhang. Damit ist gemeint, dass IT-Systeme eine angemessene und stabile Performance (Antwortzeitverhalten) aufweisen müssen, damit sinnvoll damit gearbeitet werden kann.[157]

Die **Pseudonymisierung** bezeichnet ein Verfahren, bei dem personenbezogene Daten pseudonymisiert werden. Dies wiederum bedeutet, dass der Personenbezug zum Betroffenen unkenntlich gemacht wird. Es kann ohne rechtlich zulässige Mittel bei pseudonymisierten Daten nicht eruiert werden kann, wem diese Daten zuzuordnen sind.[158]

Weiters werden im Art. 32 Abs. 2 EU-DSGVO die **Risiken** aufgezählt, die bei der Beurteilung des angemessenen Schutzniveaus zu berücksichtigen sind. Dies sind vor allem Risiken die mit der Verarbeitung (wie Übermittlung, Speicherung etc.) der personenbezogenen Daten in Zusammenhang stehen, unabhängig davon ob dies unbeabsichtigt oder un-

[155] vgl Pollirer, H.-J. (2016), S.199, vgl Erwägungsgrund Nr. 77 zur EU-DSGVO in: Pollirer, H.-J., Weiss, E., Knyrim, R., Haidinger, V. (Hrsg) (2017), S. 85f
[156] vgl VO (EU) 2016/679 ABl L 2016/119, S.51f
[157] vgl Pollirer, H.-J. (2016), S. 201
[158] vgl Pollirer, H.-J. (2016), S. 200

rechtmäßig erfolgen kann: Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugter Zugang.[159]

Gem. Art. 32 Abs. 4 EU-DSGVO haben der Verantwortliche bzw. der Auftragsverarbeiter ihre Mitarbeiter, die Zugang zu personenbezogenen Daten haben, entsprechend zu schulen und zu verpflichten, so dass diese in der Regel die betroffenen Daten nur auf Anweisung des Verantwortlichen verarbeiten[160].

Viele der bisher beschriebenen Schritte sind Aktivitäten die üblicherweise im Rahmen des Risikomanagements durchgeführt werden bzw. im Rahmen eines Informationssicherheits-Management-Systems (**ISMS**) vorgesehen sind. Die Abläufe dazu werden von der ISO/IEC 27001 (mit dem Titel „Information technology – Security techniques – Information security management system – Requirements“) hinsichtlich der Anforderungen an das Managementsystem bzw. ISO/IEC 27002 (mit dem Titel „Information technology – Security techniques – Code of practice for information security controls“) hinsichtlich der Vorschläge und Vorgaben zur Umsetzung beschrieben.[161] Denn Art. 32 Abs. 3 EU-DSGVO definiert, dass die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 EU-DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 EU-DSGVO als Faktor herangezogenen werden kann, um die Erfüllung der genannten Anforderungen nachzuweisen.[162]

<u>Bedeutung für das Gesundheitswesen</u>

Wie bereits in 2.4 Bedeutung von Compliance im Gesundheitswesen erwähnt, liegt einer KPMG Studie aus dem Jahr 2015 zufolge, das Gesundheitswesen im Vergleich zu anderen Industriesektoren, hinsichtlich technischer Kompetenz im Schutz von IT-Infrastruktur und elektronischer Gesundheitsdaten deutlich zurück. Dies zeigt sich durch den Einsatz von veralteten klinischen Technologien, unsicheren netzwerkfähigen medizinischen Devices und einem generellen Mangel an Prozessen im Bereich Informationssicherheits-Management sowie entsprechenden Zertifizierungen zu Informationssicherheits-Management-Systemen (ISMS).[163]

[159] vgl Pollirer, H.-J. (2016), S. 200, vgl VO (EU) 2016/679 ABl L 2016/119, S.52
[160] vgl VO (EU) 2016/679 ABl L 2016/119, S.52
[161] vgl Feiler, L., Forgó, N. (2017), S. 28, vgl Pollirer, H.-J. (2016), S. 201
[162] vgl VO (EU) 2016/679 ABl L 2016/119, S.52
[163] vgl KPMG (2015), S.1

Nach Aussage der KPMG die sich diesbezüglich auf Ihren Erfahrungsschatz beruft, sind Gesundheitsorganisationen mit erhöhten Sicherheitsbedrohungen in folgenden Bereichen konfrontiert: [164]

- mit der zugelassenen Nutzung von digitalen Patientenakten und die Automatisierung von klinischen Systemen,
- mit dem Einsatz von veralteten Systemen zur Verwaltung elektronischen Patientenakte sowie klinischer Applikationen die zum Zeitpunkt Ihrer Konzeption nicht dafür spezifiziert wurden sicher in heutigen Netzwerken betrieben zu werden, mit Softwareanbietern die eben diese Problematik von sich weg und hin zum Leistungsanbieter schieben,
- mit den einfachen Möglichkeiten elektronisch geschützte Gesundheitsdaten, sowohl unternehmensintern (Laptops, Mobile Devices, USB-Sticks etc.) als auch unternehmensextern (an Drittanbieter, über Cloud Services etc.) zu verteilen,
- mit der heterogenen Natur von Netzwerksystemen and Applikationen (z.B. werden netzwerkfähige Beatmungsgeräte im selben Netzwerk mit Erfassungssystemen betrieben, die das Internet durchsuchen dürfen),
- angesichts des zunehmenden Wertes von kompromittierten Daten am Schwarzmarktmit, entwickelt sich eine Bedrohungslandschaft, in der Cyber-Attacken immer ausgeklügelter und kapitalkräftiger ausgestattet stattfinden können.

Andererseits ist natürlich auch festzuhalten, dass die Vernetzung im Gesundheitswesen große Vorteile hinsichtlich der Steigerung von Qualität und Effizienz in den medizinischen Abläufen mit sich bringen kann.[165]

In der KPMG Studie, die von Forbes Insights durchgeführt wurde, wurden 223 Verantwortliche im Gesundheitswesen in den U.S. befragt. 56% der Unternehmen kamen aus for-profit Organisationen und 44% aus dem not-for-profit Bereich. Alle Gesundheitsunternehmen hatten einen Umsatz von zumindest 500 Millionen US-Dollar. 70% hatten sogar einen Umsatz von mehr als einer Milliarde US-Dollar.[166]

[164] vgl KPMG (2015), S.1
[165] vgl KPMG (2015), S.1
[166] vgl KPMG (2015), S.6

Den Studienergebnissen nach, nehmen die Befragten die größten Angriffspotentiale von außerhalb des Unternehmens wahr. Externe Angreifer und Drittanbieter sind die erkannten Top-Schwachstellen: [167]

Abbildung 5: Die größten Schwachstellen in der Datensicherheit[168]

Als größte Bedenken wurden Bedrohungen durch Malware und potentielle Verletzungen des Health Insurance Portability and Accountability Act (HIPPA) genannt:[169]

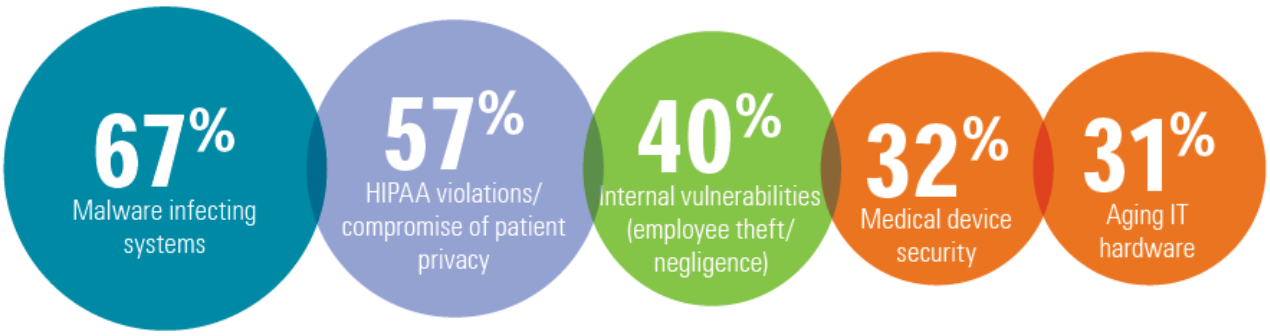

Abbildung 6: Die Top-Bedenken im Beriech Informationssicherheit[170]

Das Gesundheitswesen hat also die Notwendigkeit erkannt im Bereich Informationssicherheits-Management bzw. hinsichtlich des dazugehörigen Managementsystems, Maßnahmen zu ergreifen. Aber bezüglich der dafür notwendigen Investitionen wurde dieser Erkenntnis in der Vergangenheit nicht immer Folge geleistet. Michael Ebert, KPMG Partner und CyberSecurity Berater im Gesundheitswesen meint dazu, dass hinsichtlich der Investitionen im Gesundheitsbereich immer die Abwägung getroffen wird, ob vorrangig in die Patientensicherheit oder in die Sicherheit der Daten der Patienten investiert werden sollen.[171] Dem Ergebnis der Studie zu folge liegt der Schluss nahe, dass in der Regel zugunsten der ersten Alternative entschieden wurde.

---

[167] vgl KPMG (2015), S.2
[168] Abbildung entnommen aus: KPMG (2015), S. 2; Originaltitel „greatest vulnerabilities in data security“
[169] vgl KPMG (2015), S.2
[170] Abbildung entnommen aus: KPMG (2015), S. 2; Originaltitel „top information security concerns“
[171] vgl KPMG (2015), S.2

In den kommenden Monaten sollte diese Thematik daher dringend vorangetrieben werden, denn gem. Art. 83 Abs. 4 EU-DSGVO werden Geldbußen von bis zu € 10 Mio. bzw. 2% des internationalen Konzernumsatzes des Vorjahres fällig, wenn die gesetzlichen Anforderungen nicht erfüllt sind.[172]

3.1.7 Datenschutz durch Technikgestaltung und datenschutzfreundliche Vorsteinstellungen

Der Art. 25 EU-DSGVO regelt "Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Vorsteinstellungen", also Privacy-by-Design (auch „data protection by design“) genannt im Abs. 1 und Privacy-by-Default im Abs. 2.[173]

Privacy-by-Design

Art. 25 Abs. 1 EU-DSGVO definiert dabei klar, dass der Verantwortliche derjenige ist, der Privacy-by-Design in seinem Unternehmen einzuführen hat, da er für die Ordnungsmäßigkeit seiner Datenverarbeitung verantwortlich ist. Privacy-by-Design bedeutet, dass ein System so zu gestalten ist, dass es möglichst wenig in die Privatsphäre des Betroffenen eingreift und es möglichst gar nicht zulässt, dass Eingriffe vorgenommen werden, die nicht dem Zweck des Systems entsprechen. Dabei hat der Datenschutz im gesamten Technologie-Lebenszyklus berücksichtigt zu werden. D.h. vom Entwurfsstadion des Systems an bis zur Außerbetriebnahme.[174]

Wie bereits festgehalten, hat dabei der Verantwortlich laut EU-DSGVO die Verantwortung seine Abläufe zu analysieren und entsprechende technische und organisatorische Maßnahmen zu ergreifen um Privacy-by-Design schon bereits vor der Verarbeitung und während dieser sicherzustellen und dass unter Risikoabwägung und Berücksichtigung von Kosten und Nutzen. Dies wird auch als **Verhältnismäßigkeitsabwägung** bezeichnet und im Art. 25 Abs. 1 genau ausdefiniert. Die Maßnahmen die hier genannt werden sind uns allerdings schon aus dem Art. 32 bekannt, denn es sind dieselben Maßnahmen die im Zusammenhang mit der Verhältnismäßigkeitsabwägung für Datensicherheit (siehe dazu 3.1.6 Informationssicherheit nach dem Stand der Technik) definiert wurden.[175]

---

[172] vgl Pollirer, H.-J. (2016), S. 201
[173] vgl VO (EU) 2016/679 ABl L 2016/119, S.48
[174] vgl Hötzendorfer, W. (2016): Privacy by Design and by Default: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 137 und 139
[175] vgl Hötzendorfer, W. (2016), S. 144

Diese Vorgaben richten sich an den Verantwortlichen und nicht an den System-Hersteller sowie auch die Strafe bei Nicht-Einhaltung. Dennoch entsteht ein indirekter Druck dem Hersteller gegenüber, da dieser vom Verantwortlichen auf ihn ausgeübt wird[176] (siehe dazu mehr in 3.3.1 Vermeidung von Strafen). Der Hersteller soll auf diese Weise motiviert werden Technologien, die zum Schutz der Privatsphäre konzipiert wurden und die man auch als PETs (Kurzform für Privacy-Enhancing-Technologies) bezeichnet, in seinen Systemen gerecht zu berücksichtigen.[177]

Legt man die EU-DSGVO eng aus, lässt sich daraus ableiten, dass man als Verantwortlicher auch seine bestehenden Systeme gegen die Privacy-by-Design Anforderungen prüfen muss. Dies stellt natürlich eine besondere Herausforderung dar, wenn man nur ein indirektes Druckmittel dem Hersteller des Produkts gegenüber hat. Die Wirtschaftlichkeit einer Lösung sollte jedoch immerhin gewahrt bleiben.[178]

Privacy-by-Default

Art. 25 Abs. 2 EU-DSGVO regelt diese, als Privacy-by-Default, bezeichnete Vorgabe. Es besagt, dass auch hier durch technische und organisatorische Maßnahmen sichergestellt werden muss, dass durch Voreinstellungen nur personenbezogene Daten verarbeitet werden, die für den Verarbeitungszweck bestimmt sind. Dies gilt für die Kriterien Datenmenge, -umfang, Speicherfrist und Zugänglichkeit. Diese Einstellungen dürfen nur vom Betroffenen selbst geändert werden vor allem hinsichtlich der Zugangsberechtigungen anderer natürliche Personen zu diesen Daten. Im letzteren Satz sind Social Media wie Facebook adressiert. Ein klassisches Beispiel hierfür wäre die Notwendigkeit der Freigabe eines, vom Betroffenen hochgeladenen Fotos, an einen erwünschten Freundeskreis.[179] Dies trifft auch das Ziel dieser Regelung, nämlich dass der Anwender sich durch diese Voreinstellungen weniger Gedanken um die Einhaltung des Datenschutzes machen muss.

Was auffällt, ist dass es hier keine Vorgabe einer Verhältnismäßigkeitsprüfung gibt. D.h. die Maßnahmen die für Privacy-by-Default zu ergreifen sind, sind jedenfalls umzusetzen, unabhängig von etwaigen Kosten, Risiken etc.[180] Und auch hier gilt wieder, dass ein Ver-

[176] vgl Erwägungsgrund Nr. 78 zur EU-DSGVO in: Pollirer, H.-J., Weiss, E., Knyrim, R., Haidinger, V. (Hrsg) (2017), S. 86
[177] vgl Hötzendorfer, W. (2016), S. 141
[178] vgl Spyra, G. (2016): Die EU-DSGVO: Alter Wein in neuen Schläuchen?, Vortrag auf der 16. Conhit, https://gmds.de/fileadmin/user_upload/Aktivitaeten_Themen/Medizinische_Informatik/dgi/workshops/20160418/02-04_spyra_20160418.pdf, Abfragedatum 20.08.2017
[179] vgl Hötzendorfer, W. (2016), S. 146f, vgl VO (EU) 2016/679 ABl L 2016/119, S.48
[180] vgl Hötzendorfer, W. (2016), S. 147

antwortlicher seine bestehenden Systeme danach zu überprüfen hat, ob damit den Privacy-by-Default Anforderungen entsprochen wird. Andernfalls sind auch für bestehende Systeme entsprechende Maßnahmen umsetzen.[181]

Bedeutung von Datenschutz durch Technikausgestaltung für das Gesundheitswesen

Da sich streng gesehen, die Anforderungen der EU-DSGVO auch an bestehende Systeme richten, sollte man vor allem Systeme in denen sensible Daten, wie Gesundheitsdaten (z.B. Krankenhausinformationssysteme (KIS) oder Medizinprodukte) verarbeitet werden, einer Prüfung unterziehen. Bei Abweichungen von den Anforderungen sollten gemeinsam mit dem Hersteller mögliche Lösungswege diskutiert und gefunden werden.[182] Bei Verstößen ist mit Geldbußen von bis zu € 10 Mio. bzw. 2% des internationalen Konzernumsatzes des Vorjahres zu rechnen[183].

3.2 Kosten und Budgets

Die TRUSTe Inc. führte bereits Ende September / Anfang Oktober 2015, also sogar noch vor dem finalen Beschluss und der Verabschiedung der EU-DSGVO auf EU-Ebene, eine Umfrage zum Thema „Preparing for the EU General Data Protection Regulation“ durch. Die Umfrage wurde online durchgeführt und berücksichtigte 202 Experten mit Knowhow im Bereich Datenschutz aus Unternehmen mit mehr als 250 Mitarbeitern. Dabei wurden 103 Teilnehmer aus US und 99 aus Europa (35 aus UK, 34 aus Deutschland und 30 aus Frankreich) befragt.[184] Durch die Studie wurde die Erkenntnis gewonnen, dass sich aus dem Kreis der Befragten im Herbst 2015 zwei Gruppen (zu jeweils 50% der Befragten) bilden ließen. Nämlich jener Gruppe, die noch keine Awareness hinsichtlich der damals bevorstehenden Regulierungen hatte und einer zweiten Gruppe, die bereits gut informiert zum Thema EU-DSGVO waren und teilweise auch schon mit Vorbereitungen gestartet hatten. Interessant dabei ist auch die Erkenntnis, dass es hier keinen wesentlichen Unterschied gab, ob es sich um US-amerikanische Unternehmen oder Unternehmen mit Sitz in der EU handelte. Auch interessant ist die Erkenntnis, dass aus der Gruppe mit Awareness

[181] vgl Spyra, G. (2016)
[182] vgl Spyra, G. (2016)
[183] vgl Hötzendorfer, W. (2016), S. 148
[184] vgl TRUSTe Inc (2015): Research Report: Preparing fort h EU General Data Protection Regulation: Assessing Awareness, Readiness & Impact of the Proposed Changes in US, UK, France & Germany, https://info.trustarc.com/Web-Resource-GDPR-Research-Report_LP.html, Abfragedatum 14.08.2017, S.2

damals bereits 65% mit Vorbereitungen auf die EU-DSGVO gestartet hatten, obwohl das Recht noch gar nicht verabschiedet wurde.[185]

Wesentlich im Rahmen dieser Arbeit sind vor allem die Aussagen die zu den budgetären Vorkehrungen der Unternehmen, die eine Aussage hinsichtlich der erwarteten Kosten der Unternehmen zu den jeweiligen Vorhaben im Rahmen der Herstellung der EU-DSGVO-Compliance machen. 83% der befragten Unternehmen aus der Gruppe mit Awareness hatten im Herbst 2015 bereits ein Budget für die EU-DSGVO Thematik vorgesehen. Daraus gaben bereits damals 31% an zwischen 100.000, -- und 500.000, -- US Dollar für die EU-DSGVO Thematik budgetiert zu haben. Dem damaligen Umrechnungskurs nach waren dies zwischen ca. 90.000, -- und 445.000, -- EUR. Weitere 21% dieser Befragten gaben sogar an mehr als 500.000, -- US Dollar budgetiert zu haben. Auf der anderen Seite gab es auch 18% die bekannt gaben, noch kein bzw. kein explizit für EU-DSGVO Thema ausgezeichnetes Budget oder max. 10.000, -- US Dollar Budget vorgesehen zu haben.[186]

In der folgenden Abbildung der TRUSTe Inc. werden die Studienergebnisse dazu veranschaulicht:

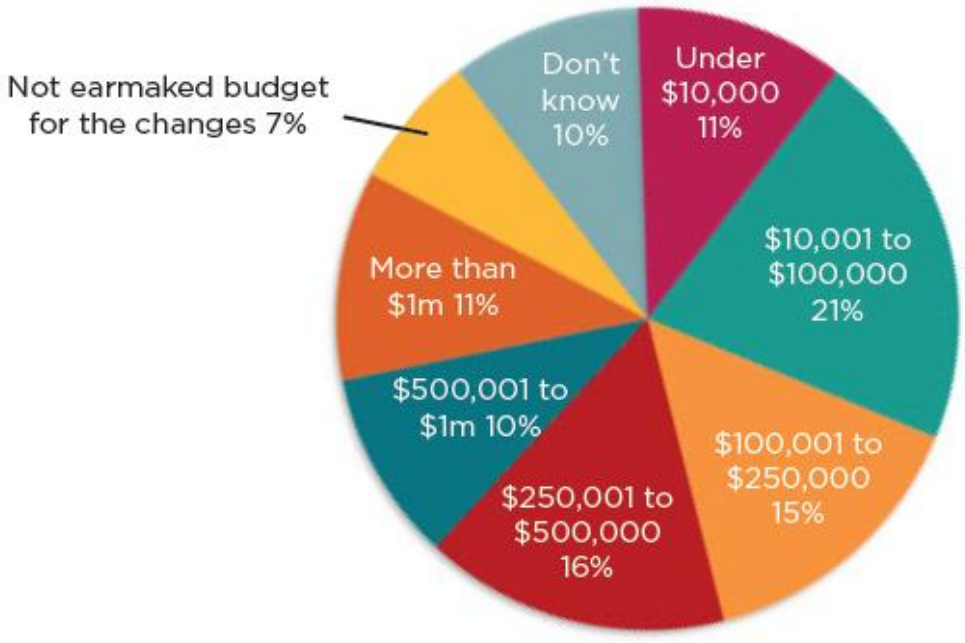

Abbildung 7: Das jährliche Budget um die Änderungen der regulatorischen Anforderungen zu adressieren187

[185] vgl TRUSTe Inc (2015), S.4
[186] vgl TRUSTe Inc (2015), S.7
[187] Abbildung entnommen aus: TRUSTe Inc (2015), S.7; Originaltitel "Annual budget allocated to address these changes in regulatory requirements?"

40% der Befragten gaben im Rahmen der Studie an, dass das Budget nur dann zugeteilt wird, sobald die EU-DSGVO verabschiedet werden würde. Dies würde zwei Jahre Vorbereitungszeit bis zum Zeitpunkt des Inkrafttretens des Gesetzes bedingen. Weitere 20% der Befragten gaben an, dass das Budget nur dann zugeteilt wird, sobald die EU-DSGVO wirksam wird. D.h. mit Ende Mai 2018. Dadurch wird das Risiko eingegangen, dass man zu diesem Zeitpunkt den Gesetzen noch nicht voll und ganz entspricht, was zu Strafen führen könnte.

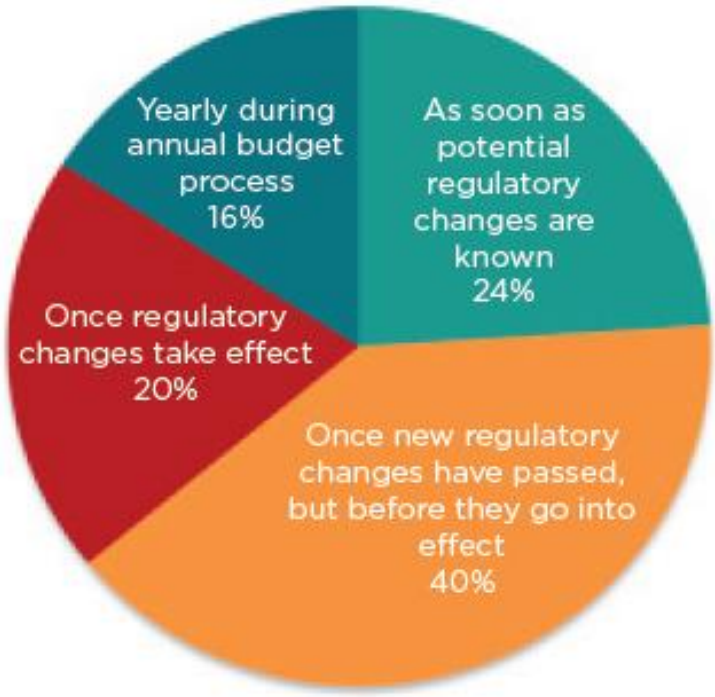

Abbildung 8: Zeitpunkt der Budgetentscheidungen bzgl. der regulatorischen Änderungen188

3.3 Chancen und Nutzen

Bei der Erarbeitung der EU-DSGVO verfolgte der Gesetzgeber seine Vorstellungen, welchen Nutzen das Gesetz den Betroffenen, aber auch der Wirtschaft bringen wird. Zum einen wollte man das Vertrauen der EU-Bürger in den sicheren Umgang von Unternehmen im Online-Bereich hinsichtlich Datenschutz sowie damit verbunden die Stärkung der digitalen Wirtschaft innerhalb der EU fördern. Weiters geht der Gesetzgeber davon aus, dass er Einsparungen von bis zu 2,3 Billionen Euro pro Jahr für die Wirtschaft durch eine Harmonisierung des Datenschutzrechts auf EU-Ebene über alle 28 Mitgliedstaaten hinweg erwirken kann. Damit verbunden ist eine einheitliche Rechtsdurchsetzung, die wiederum dem Vertrauen der EU-Bürger zu Nutzen kommt. So wie auch das neue Prinzip „Datenschutz

[188] Abbildung entnommen aus: TRUSTe Inc (2015), S.7; Originaltitel „When are the budget decisions made regarding this kind of regulatory change?“

durch Technik“ positive Auswirkungen auf die IT-Wirtschaft haben kann (siehe dazu auch 3.1.7 Datenschutz durch Technikgestaltung und datenschutzfreundliche Vorsteinstellungen).[189]

Wie bereits in 2.5 Der Nutzen von Compliance thematisiert, gibt es aus der wirtschaftlichen Betrachtung heraus zwei Kategorien von Nutzen. Zum einen kann es ein Nutzen für das betroffene Unternehmen sein, negative Auswirkungen aus möglichen Nachteilen zu vermeiden, indem das Risiko des Eintritts des unerwünschten Ereignisses reduziert wird. Andererseits ist es auch möglich, dass ein Unternehmen durch ein Compliance Projekt, einen echten „Business Enabler“ generiert und einen wettbewerbsfördernden Nutzen mit der Herstellung der EU-DSGVO-Compliance erzeugt. Beide Aspekte werden im Folgenden detaillierter beleuchtet.

3.3.1 Vermeidung von Strafen

Dass die Vermeidung von Strafen ein sehr wichtiger Beweggrund für die Unternehmen im Rahmen der Herbeiführung der EU-DSGVO-Compliance ist wurde bereits thematisiert. Sowie die Empfehlung zur Implementierung eines DSMS um die organisatorischen und technischen Maßnahmen (TOMs), die derzeit erarbeitet und umgesetzt werden, auch nachhaltig weiterzuführen und sich damit auch in der Zukunft compliant und straffrei zu halten bzw. einen Reputationsverlust zu vermeiden.

Aber nicht nur die Verantwortlichen selbst sind bei einem weiteren Blick auf die Thematik betroffen. Um Strafen zu vermeiden, werden die Verantwortlichen für Verarbeitungstätigkeiten personenbezogener Daten zukünftig nicht nur die Kosten und Eigenschaften eines IT-Produktes abwägen. Zusätzlich werden auch Überlegungen angestellt werden, hinsichtlich des notwendigen Aufwandes den Einsatz des Produkts EU-DSGVO-konform zu gestalten. Auch wenn die Verantwortlichen und Auftragsverarbeiter Normadressaten der EU-DSGVO sind, wird der Druck auf die Produkthersteller ebenfalls erzeugt, da nicht EU-DSGVO konforme Produkte früher oder später bei Kaufentscheidungen nicht mehr berücksichtigt werden. Davon abgesehen droht dem Hersteller ein Imageschaden, wenn er nicht in der Lage ist eine EU-DSGVO-konforme Anwendung anbieten zu können. Weiters kann der Verantwortliche natürlich auch, im Falle einer Strafe die aufgrund des Einsatzes einer nicht geeigneten Anwendung zustande kommt, in weiterer Folge prüfen, ob aus gel-

[189] vgl EY (2016), S. 4, vgl Krisch, A. (2016): DSGVO: Chancen und Risiken für die IT-Wirtschaft, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 370, vgl TRUSTe Inc (2015), S.4

tenden Rechtsvorschriften, wie z.B. den Bestimmungen zur Produkthaftung heraus, der Produktherstellern nicht auch haftbar ist. Die Gefahr eines Regresses droht dem Hersteller daher, wenn er nicht nachweisen kann, dass sein Produkt dem Stand der Technik entsprechend funktioniert. [190]

Bedeutung für das Gesundheitswesen

Es wird wohl zur gängigen Praxis werden müssen, dass im Rahmen von Neuanschaffungen in den Ausschreibungsunterlagen bereits Privacy-by-Design vom Hersteller zu fordern ist. Prallelen kann man hier auch einen Blick auf die Thematik des Einkaufsprozesses von netzwerkfähigen Medizinprodukten riskieren. Die DIN EN 80001 (mit dem Titel „Risikomanagement für medizinische IT-Netzwerke“) gibt eine detaillierte Abklärung von Anforderungen im Rahmen des Einkaufsprozesses vor. Hier wird es Sinn machen in der Zukunft harmonisierte Einkaufsprozesse mit standardisierten Vorgaben einzuführen.

3.3.2 Hebung weiterer Chancen aus der Erfüllung der EU-DSGVO

Chancen sind erkennbar im Zusammenhang mit aktuellen technologischen Strömungen, die häufig im Zusammenhang mit dem Begriff Digitalisierung fallen. Digitalisierung beschreibt die Veränderung von Abläufen und Ereignissen, wie beispielsweise der Kommunikation durch die zunehmende Nutzung von digitalen Geräten. Sowie die Veränderung von Instrumenten und Objekten, wie beispielswiese Fahrzeugen durch die digitale Modifikation.[191]

Big Data

Der Begriff Big Data steht für große Mengen an Daten, die aus unterschiedlichsten Bereichen wie dem Internet, der Finanzindustrie, dem Gesundheitswesen, den sozialen Medien, von Überwachungskameras sowie Flug- und Fahrzeugen etc. stammen. Diese großen Datenmengen werden gesammelt und mit speziellen Methoden gespeichert, verarbeitet und ausgewertet.[192]

---

[190] vgl Krisch, A. (2016), S.373f
[191] vgl Gabler Wirtschaftslexikon (2017a), Stichwort: Digitalisierung, http://wirtschaftslexikon.gabler.de/Archiv/-2046143105/digitalisierung-v3.html, Springer Gabler Verlag (Hrsg), Abfragedatum 16.08.2017
[192] vgl Gabler Wirtschaftslexikon (2017b), Stichwort: Big Data, http://wirtschaftslexikon.gabler.de/Archiv/-2046774198/big-data-v4.html, Springer Gabler Verlag (Hrsg), Abfragedatum 16.08.2017

Der Bereich Big Data wird durch die folgenden drei technologischen Entwicklungen vorangetrieben[193]:

1. Betriebliche Digitalisierung: Betriebliche Abläufe werden immer mehr rein elektronisch durchgeführt,
2. Private Digitalisierung: Mobile Devices und der Einsatz beliebiger Apps, führt zur Generierung vieler personenbezogener Daten im Alltag. Der Begriff Quantified Self ist in diesem Zusammenhang gängig und beschreibt die Vermessung des eigenen Verhaltens wie z.B. durch Schrittzähler-Apps.
3. Social Media: Privatpersonen teilen diese Daten auch mit anderen.

Bei Big Data Analysen werden viele, unterschiedlich gut strukturierte Daten anhand von Algorithmen verknüpft. Das Ziel ist es über die sogenannte Korrelation dieser Informationen Fragestellung mit einem gewissen Grad an Wahrscheinlichkeit beantworten zu können. Es geht dabei nicht darum, dass z.B. ein Betreiber einer Big-Data-Webanwendung ein Profil einer echten Person tatsächlich zuordnen kann. Vielmehr geht es darum **typische Verhaltensweisen von Personen abschätzen zu können**. Ob vor der Webanwendung dann tatsächlich eine alleinstehende Mutter sitzt oder ob es ein Familienvater ist, der aber das Kaufverhalten einer alleinstehenden Mutter erfüllt ist nicht relevant. Wichtig ist nur, dass das Kaufverhalten richtig bewertet und durch die Applikation befriedigt werden kann. Der Begriff Big Data sagt daher auch nichts darüber aus, ob personenbezogene Daten dazu verwendet werden. Das kann der Fall sein, muss es aber nicht. Ob Daten für die Big-Data-Analysen verwendet werden dürfen ist somit im Einzelfall zu prüfen und unabhängig vom angestrebten Ergebnis der Big-Data-Analyse. Je größer aber die Datenmengen sind, die verarbeitet werden und je genauer die Datenqualität ist, umso größer wird die Komplexität im Zusammenhang mit der rechtlichen Prüfung, denn die, zur Kategorisierung des Verhaltens verwendeten Daten sind häufig indirekte als auch direkte personenbezogene Daten.[194]

<u>Bedeutung im Gesundheitswesen:</u>

Das Gesundheitswesen ist eine der Branchen die ein sehr großes Potential hinsichtlich Big Data bietet. Für Medizin und Gesundheitswesen ist diese Technik sowohl in der For-

[193] vgl Rüpin, S. (2015): Big Data in Medizin und Gesundheitswesen, Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz, Volume 58, Issue 8, S. 794

[194] vgl Steinmaurer, K. M. (2016): Big Data und Profiling: Chancen und Risiken in der Datenschutz-Grundverordnung, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz, S. 82f

schung, als auch der medizinischen Praxis interessant, da sich hier neue Datenquellen und Datenanalysemöglichkeiten auftun. In der Forschung kann Big Data z.B. im Bereich der Omics-Forschung[195] besonders wertvoll sein. In der medizinischen Praxis bietet der elektronische Patientenakt, Open Data und Quantified Self neue Möglichkeiten zur Datenanalyse.[196] Ein weites Beispiel für einen solchen Anwendungsbereich wäre die Rehabilitation im Zusammenhang mit Quantified Self. Therapeuten können die sich daraus ergebenden Möglichkeiten für Telerehabilitationsfälle am einzelnen Patienten optimal nutzen. Weiters ermöglicht die Auswertung einer Menge von Therapieergebnissen Analysen hinsichtlich bestimmter Leistungsmerkmale.

Profiling

Im Unterschied zu Big Data wird beim Profiling jedenfalls mit personenbezogenen Daten gearbeitet und weiters gibt es dazu, im Unterschied zu Big Data, auch eine Definition in der EU-DSGVO im Art. 4 Z4[197]:

„"Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;“

Profiling verfolgt das Ziel, mit großer Wahrscheinlichkeit das **Verhalten einer Person vorherzusagen**, wie z.B. aus der Verknüpfung einer bestimmten Adresse mit der Eigenschaft „alleinstehend“ eine Wahrscheinlichkeit für Zahlungsunfähigkeit abgeleitet werden kann. Die EU-DSGVO setzt dem Schranken. In Art. 22 Abs. 1 EU-DSGVO wir definiert, dass der Betroffene nicht ausschließlich einer automatisierten Verarbeitung beruhenden Entscheidung (worunter auch Profiling fällt) unterworfen werden darf (siehe dazu auch 3.1.4 Erfüllung der Betroffenenrechte).[198]

Hinsichtlich des Zusammenhangs mit Big Data ist davon auszugehen, dass Profiling-Anwendung in der Zukunft verstärkt cloudbasierten Big-Data-Tools nutzen werden. [199]

---

[195] OMICs Forschung: steht für die Forschungsgebiete mit der Endung "-omics": Genomics (Genforschung), Proteomics (ermittelt das Auftreten von einem bestimmten Protein oder Enzym in einer Zelle), Metabolomics (beschäftigt sich mit Stoffwechselprodukten); vgl Standard: Wundersame Welt der "-omics" vom 12. September 2004, http://derstandard.at/1783795/Wundersame-Welt-der--omics, Abfragedatum 16.08.2017
[196] vgl Rüpin, S. (2015), S.794f
[197] VO (EU) 2016/679 ABl L 2016/119, S.33
[198] vgl Steinmaurer, K. M. (2016), S. 85
[199] vgl Steinmaurer, K. M. (2016), S. 85

Die EU-DSGVO setzt zukünftig für Big-Data bzw. Profiling Vorhaben ausdrücklich geregelt die Durchführung einer Datenschutz-Folgeabschätzung voraus. Der Verantwortliche hat diese Abschätzung durchzuführen und muss beurteilen, ob die Anwendung datenschutzkonform ist, was dem Vorhandensein des notwendigen rechtlichen Know-how bedarf.[200]

Bedeutung für das Gesundheitswesen

Es liegt auf der Hand, dass Big Data und Profiling Chancen für das Gesundheitswesen mit sich bringen. Es ist aber leider festzustellen, dass gegenüber der aktuellen Rechtslage keine neuen Verbesserungen oder Möglichkeiten, Daten in diesem Hinblick wirtschaftlich besser nutzen zu können, geschaffen wurden. Folglich bedeutet dies, dass wenn jemand Big-Data bzw. Profiling-Anwendungen betreiben will bzw. entsprechende Geschäftsmodelle verfolgt, er von vornherein darauf zu achten hat, dass die Anwendungen dem Grundsatz Privacy-by-Design nach zu gestalten sind. Weiters hat er auch das Wissen im Unternehmen aufzubauen (oder extern hinzuziehen kann) um Beurteilungen zur Rechtskonformität durchführen zu können.[201]

Open Data

Mit dem Begriff Open Data werden Daten bezeichnet, die ohne Einschränkungen jedem zu seiner Nutzung zur Verfügung stehen. Sie dürfen verbreitet und weiterverwendet werden. Jeder darf auf sie zugreifen, sie nutzen und teilen.[202]

Dies führt uns zu einem weiteren Begriff in diesem Zusammenhang, dem Open Government Data (OGD). Dieser wird nach Kaltenböck, M. & Thurner, T. wie folgt erklärt: [203]

„Offene Verwaltungsdaten (engl. Open Government Data, OGD) sind Datenbestände, die von der öffentlichen Verwaltung im Bereich der Hoheitsverwaltung und privatwirtschaftlichen Verwaltung im Interesse der Allgemeinheit erhoben werden und in einem anerkannten offenen, maschinenlesbaren Format zur beliebigen, digitalen Weiterverarbeitung zur Verfügung gestellt werden“.

Diese Daten stehen also der Öffentlichkeit zur Verarbeitung zur Verfügung, soweit dass sie nicht die Rechte und Freiheiten des einzelnen Betroffenen gefährden.

---

[200] vgl Steinmaurer, K. M. (2016), S. 96
[201] vgl Steinmaurer, K. M. (2016), S. 96f
[202] vgl Palmethofer, W., Semsrot, A., Alberts, A. (2017): Der Wert persönlicher Daten: Ist Datenhandel der bessere Datenschutz? Sachverständigenrat für Verbraucherfragen, http://www.svr-verbraucherfragen.de/wp-content/uploads/Open_Knowledge_Foundation_Studie.pdf, Abfragedatum 14.08.2017, S.11
[203] Kaltenböck, M., & Thurner, T. (2011). Open Government Data Weissbuch. Wien: Edition Donau-Universität Krems, S. 18

Bedeutung für das Gesundheitswesen

Open Data findet bereits Verwendung im Bereich des öffentlichen Gesundheitswesens. Es hilft bei der Entwicklung von entsprechenden Programmen und der Überprüfung ihrer Wirksamkeit. Daten, wie Statistiken zu Mortalität und Morbidität oder Informationen über Gesundheitszustand und Gesundheitsverhalten einer Bevölkerung werden überwiegend von öffentlichen Dienstleistern und Institutionen der öffentlichen Verwaltung erhoben (Gebietskörperschaften, Krankenanstalten, Sozialversicherungsträger, Kammern etc.).[204] Der Nutzen von Big Data im Gesundheitswesen wurde bereits angesprochen. Wenn auf einer übergreifenden z.B. nationalen Ebene, diese Daten in einer Form in der sie nicht gegen Rechte und Freiheiten einzelner Betroffener verstoßen (in Form von Open Data) genutzt werden können, dann führt dies indirekt durch die Vorteile die sich daraus für das Gesundheitswesen allgemein ableiten lassen, wieder zu Vorteilen einzelner Einrichtungen im Gesundheitswesen. Die Einhaltung der Vorgaben der EU-DSGVO zum Schutz der Rechte des Einzelnen sind dabei natürlich zu beachten.

3.4 Zusammenfassung

Im vorangegangenen Kapitel wurden zuerst die Anforderungen, die die EU-DSGVO mit sich bringt, erklärt. Vor allem die Ausgestaltung und Umsetzung des Datenschutz-Management-Systems (DSMS) ist dabei von Interesse. Denn der Aufbau eines DSMS hilft dabei Abläufe zu standardisieren, eine Dokumentation im Sinne der Rechenschaftspflicht aufzubauen und somit auch Organisationsverschulden nachweislich auszuschließen. Ein weiter betrachteter Faktor ist das Management-Commitment ohne welches ein Vorhaben dieser Art schwer durchzuführen ist.

Anschließend wurde auf organisatorische Themen, wie der Einführung und Ausgestaltung der Rolle des Datenschutzbeauftragten, dem Aufbau von zentralen Verarbeitungsregistern, der Durchführung von Datenschutz-Folgeabschätzungen, der Erfüllung der Betroffenenrechte sowie der Meldung von Datenschutzvorfällen eingegangen. Ebenso sind die technischen Herausforderungen von Bedeutung, wie das IT-technische Sicherheitsniveau im Gesundheitswesen und die Herausforderungen die Neuerungen wie Privacy-by-Design

[204] vgl Stockinger, G. (2013): Potentiale von Open Government Data im österreichischen Gesundheitswesen am Beispiel der Kinder- und Jugendgesundheit, Krems, FH Krems, Master‘s Thesis, S.3f

und Privacy-by-Default mit sich bringen. All diese Themen wurden detailliert betrachtet und im Kontext des Gesundheitswesens analysiert.

Auf Basis einer Studie wurde ermittelt, welche voraussichtlichen Kosten in Form von vorgesehenen Budgets Unternehmen für derartige Projekte in der Praxis zur Verfügung gestellt werden.

Weiters wurde ein Blick auf die Chancen und möglichen erkennbaren Nutzen aus der EU-DSGVO geworfen. Zum einen wurde auf den Nutzen einer Risikoreduktion hinsichtlich des Eintretens einer Datenschutzverletzung und des damit zusammenhängenden Strafausmaßes bzw. Reputationsschadens eingegangen. Zum anderen wurde analysiert, welche denkbaren Chancen durch Digitalisierungsvorhaben im Kontext der EU-DSGVO gegeben sind. Denn durch die Konsolidierung von Daten, sowie die technischen Errungenschaften im Bereich von Big Data Analysen und Profiling ergeben sich neue Möglichkeiten die auch in der EU-DSGVO geregelt werden. Diese beiden Themen wurden daher beleuchtet. Auch das Schlagwort „Open Data“ im Zusammenhang mit dem zur Verfügung stellen von Behandlungsergebnissen im gemeinnützigen Sinne, ist eine weitere Chance für Entwicklung im Gesundheitswesen und wurde daher erklärt.

4. Empirischer Forschungsteil

Der vorangehende Teil der Arbeit hat sich mit der Theorie rund um EU-DSGVO, Compliance und Wirtschaftlichkeit beschäftigt. Im Folgenden wird erläutert wie der empirische Teil dieser Arbeit durchgeführt wurde. Denn mittels der empirischen, qualitativen Sozialforschung wurde versucht die Forschungsfrage über Experteninterviews praxisbezogen zu beantworten. Daher werden im Folgenden, nach einleitenden Worten zur empirischen Sozialforschung bzw. dem Forschungsprozess, die verwendeten Erhebungs- und Auswertungsmethoden aus dem Methodensatz der qualitativen Sozialforschung erläutert sowie das Untersuchungsdesign und die ausgewählten Untersuchungsteilnehmer beschrieben.

4.1 Der empirische Forschungsprozess

Atteslander definiert die empirische Sozialforschung als[205]:

„[…] die systematische Erfassung und Deutung sozialer Tatbestände“

Der Begriff „empirisch“ steht für „erfahrungsgemäß“ - d.h. durch Sinnesorgane wahrgenommene Umwelt. Unter der Soziologie versteht man die Erfahrungswissenschaft. Und „Systematisch“ meint, dass etwas nach Regeln zu erfolgen hat. Dem zufolge ist der empirische Forschungsprozess nach Vorgaben geplant und nachvollziehbar für jede Phase anzulegen.[206]

Im Vorfeld jeder empirischen Untersuchung hat man sich drei Fragen zu stellen:

1. **Was** soll erfasst werden? (Entdeckungszusammenhang)
2. **Warum** soll es erfasst werden? (Verwertungszusammenhang)
3. **Wie** soll es erfasst werden? (Begründungszusammenhang)

Der **Entdeckungszusammenhang** ist der Anlass einer Untersuchung bzw. eines Forschungsvorhabens und umfasst die Motive und Interessen warum eine Untersuchung durchgeführt wird. Darin werden die Kontextfaktoren der Forschung beschrieben und die zu untersuchende Problemen in eine wissenschaftliche Fragestellung überführt.[207]

[205] Atteslander, P. (2006): Methoden der empirischen Sozialforschung, 11. Aufl, Berlin, Erich Schmidt Verlag, S.3
[206] vgl Atteslander, P. (2006), S.3
[207] vgl Atteslander, P. (2006), S.195

In dieser Arbeit ist der Entdeckungszusammenhang durch die Untersuchung der Auswirkungen der Herbeiführung der EU-DSGVO-Compliance auf das Gesundheitswesen, eingeschränkt auf den stationären Bereich, gegeben. Daraus wurden die Forschungsfrage sowie Ihre Subfragen abgeleitet.

Der **Verwertungszusammenhang** bezeichnet die Auswirkungen einer Untersuchung und ihrer Präsentation hinsichtlich der Öffentlichkeit und ihren Beitrag zur Lösung theoretischer oder praktischer Probleme.[208]

In dieser Arbeit ist der Verwertungszusammenhang die Beantwortung der Forschungsfrage, um Erkenntnisse über die tatsächliche Situation in der Praxis zu gewinnen, nämlich welchen Herausforderungen und Chancen österreichische Verantwortliche und Auftragsverarbeiter im Sinne des Art. 4 EU-DSGVO in der stationären Krankenversorgung bei der Herbeiführung der EU-DSGVO-Compliance bis zum 25. Mai 2018 begegnen und ob bzw. wie dabei die damit verbundenen Kosten und Nutzen im Sinne des Wirtschaftlichkeitsprinzips gegenübergestellt werden.

Der **Begründungszusammenhang** erklärt das methodologische Vorgehen zur Untersuchung des Problems. Das bedeutet es klärt, welches methodische Verfahren angewandt wurde und mit welchen Textunterlagen das Problem bearbeitet wird.[209]

In dieser Arbeit wurde zur methodischen Bearbeitung das Experteninterview in Form eines Leitfadeninterviews gewählt. Im Anschluss wurden die transkribieren Interviews einer qualitativen Inhaltsanalyse unterzogen. Die gewählte Erhebungs- sowie die gewählte Auswertungsmethode werden nachfolgend genauer beleuchtet.

4.2 Das Experteninterview

Die Definition qualitativer Experteninterviews nach Kaiser lautet:

„Qualitative Experteninterviews können definiert werden als ein systematisches und theoriegeleitetes Verfahren der Datenerhebung in Form der Befragung von Personen, die über

[208] vgl Atteslander, P. (2006), S.195
[209] vgl Atteslander, P. (2006), S.195

exklusives Wissen über politische Verhandlungs- und Entscheidungsprozesse oder über Strategien, Instrumente und die Wirkungsweise von Politik verfügen."[210]

Diese Definition ist sehr politikwissenschaftlich orientiert, aber kann auch auf andere Anwendungsbereiche umgelegt werden. Defacto geht es darum eine theoriegeleitete, systematische Datenerhebung in Form einer Befragung eines Experten durchzuführen. Darin enthalten sind die Gütekriterien für ein qualitatives Experteninterview:

Zum einen ist die Art des Wissens des Experten, von dessen Wissen man im Rahmen der Auswertung profitieren möchte, relevant. Der **Forscher hat dabei dieser Person gegenüber neutral und offen zu sein**, da sich neue Erkenntnisse, neue Relevanzsysteme und Deutungsmuster ergeben können.[211]

Ein weiterer wesentlicher Faktor in der Definition ist die **theoriegeleitete** Vorgehensweise bedeutet in diesem Zusammenhang, dass ein theoretisches Wissen über den Untersuchungsgegenstand bereits vorliegt.[212] Dies ist im Rahmen der Arbeit dadurch gegeben, dass die Theorie in Bezug auf die Forschungs- und Subforschungsfragen aufgearbeitet wurden und in der Erarbeitung des Interviewleitfadens daher Berücksichtigung fand. Im Anschluss kann die Theorie dann auch im Rahmen der Analyse wieder angewandt werden.

Auch der Begriff „Systematisch" ist in diesem Kontext wichtig, um der Anforderung der **intersubjektiven Nachvollziehbarkeit** der Verfahren der Datenerhebung und –analyse nachzukommen. Das kann eine qualitative Untersuchung, im Gegensatz zu einer quantitativen Untersuchung nur schwer erfüllen, da der Standardisierungsgrad des Erhebungsinstruments, in diesem Fall das Leitfadeninterview, nicht ausreichend hoch ist.[213] Um für einen Dritten dennoch klar erkennbar bzw. nachvollziehbar darzustellen, wie die Erhebung stattgefunden hat und wie man daraus zu den Analyseergebnissen gelangt ist, werden im Folgenden Untersuchungsdesign und Untersuchungsteilnehmer vorgestellt:

[210] Kaiser, R. (2014): Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung, Wiesbaden, Springer Verlag, S.6
[211] vgl Kaiser, R. (2014), S.7
[212] vgl Kaiser, R. (2014), S.6f
[213] vgl Kaiser, R. (2014), S.6

4.2.1 Interviewleitfaden

Aus der Forschungsfrage wurden Subfragen abgeleitet und es wurde ein Leitfaden für ein Experteninterview entwickelt mit dem Praxisantworten auf die sich ergebenden Fragestellungen eingeholt wurden.

Forschungsfrage:

Welchen Herausforderungen und Chancen begegnen österreichische Verantwortliche und Auftragsverarbeiter im Sinne des Art. 4 EU-DSGVO in der stationären Krankenversorgung bei der Herbeiführung der EU-DSGVO-Compliance bis zum 25. Mai 2018 und wie werden die damit verbundenen Kosten und Nutzen im Sinne des Wirtschaftlichkeitsprinzips gegenübergestellt?

In diesem Zusammenhang ergeben sich folgenden Unterfragen zur Forschungsfrage, auf die mit den jeweiligen Fragen des Interviewleitfadens eingegangen werden[214]:

Subforschungsfrage 1:

Wie stellen Unternehmen mit Verantwortung für Gesundheitsdaten aus der österreichischen stationären Krankenversorgung die erfolgreiche Umsetzung eines Vorhabens zur Erfüllung der EU-DSGVO-Compliance bis Mai 2018 sicher?

Verknüpfung zum Interviewleitfaden:

- Frage 1: Gibt es im Sie betreffenden Unternehmen bzgl. der Einführung der EU-DSGVO-Compliance ein volles Commitment seitens Vorstand bzw. Geschäftsführung und auf welche Art und Weise wird dies deutlich?
- Frage 2: Wurde ein Ziel oder wurden mehrere Ziele für das EU-DSGVO-Compliance Projekt vereinbart, an dem die Erreichung gemessen werden kann? Wie lautet das Ziel bzw. wie lauten die wesentlichsten Ziele?
- Frage 4: Werden im Projekt auch Maßnahmen vorgesehen, die über die Herstellung der Compliance hinausgehen (z.B. Maßnahmen zur Implementierung eines Datenschutzmanagementsystems oder eines Datenschutzauditprozesses)?

[214] Anmerkung: Alle Vorhaben und Tätigkeiten zur Herstellung der EU-DSGVO-Compliance werden im Rahmen der Interviewfragen für den einfacheren Sprachgebrauch als Projekt bezeichnet. Dafür war es aber nicht erforderlich, dass ein formales Projekt im Sinne von Projektmanagement Standards im Unternehmen existieren musste.

- Frage 5: Werden im Projekt auch Maßnahmen vorgesehen, die eine aufwandsreduzierte Implementierung der Anforderungen unterstützen (z.B. die Herbeiführung von Prozessstandardisierungen oder IT-Systembereinigungen)?

Subforschungsfrage 2:

Welchen technischen und organisatorischen Herausforderungen begegnen diese Unternehmen dabei?

Verknüpfung zum Interviewleitfaden:

- Frage 3: Welchen organisatorisch und technisch umzusetzenden Maßnahmen begegnet das Sie betreffende Unternehmen im Rahmen des Projekts?
  a. Bitte nennen Sie die wesentlichsten Herausforderungen mit denen sich das Sie betreffende Unternehmen im Projekt konfrontiert sieht.
  b. Bitte nominieren Sie daraus die drei größten Herausforderungen, reihen sie diese der Größe der Herausforderung nach und begründen sie ihre Einschätzung.

Subforschungsfrage 3:

Welchen Aufwand kalkulieren die untersuchten Unternehmen um den Herausforderungen gerecht zu werden?

Verknüpfung zum Interviewleitfaden:

- Frage 4: Einer Umfrage der TRUSTe Inc. vom Oktober 2015 nach, gaben zum Thema der Vorbereitung und Budgetierung der Umsetzung der EU-DSGVO bereits damals mehr als 30% der befragten Unternehmen, welche über das Thema EU-DSGVO bereits informiert waren an, zwischen 100.000,- und 500.000,- US Dollar (damals umgerechnet zwischen ca. 90.000,- und 445.000,- EUR) dafür budgetiert zu haben.
  Wie liegt das Budget zur Herstellung der EU-DSGVO-Compliance im Sie betreffenden Unternehmen im Vergleich zur Studie? Bitte wählen Sie eine der Antwortmöglichkeiten als die zutreffende Antwort:
  c. Im angegebenen Rahmen der Studie
  d. Über dem angegebenen Rahmen der Studie
  e. Deutlich über dem angegebenen Rahmen der Studie
  f. Unter dem angegebenen Rahmen der Studie
  g. Deutlich unter dem angegebenen Rahmen der Studie
  h. Es wurde kein Budget vorgesehen

- Frage 5: Sofern ein Budget für das Projekt zur Herstellung der EU-DSGVO-Compliance vorhanden ist, wie wurde es ermittelt? Bitte wählen Sie eine der Antwortmöglichkeiten als die zutreffende Antwort:
  a. Minimalprinzip (Auf Basis der vereinbarten Projektziele wurden die Mittel – Budget und Personalressourcen - abgeleitet und freigegeben)
  b. Maximumprinzip (Die möglichen verfügbaren Mittel – Budget und Personalressourcen – wurden vorgegeben und die Projektziele danach ausgerichtet)
  c. Optimalprinzip (Es wird ein Maß an vertretbarem Risiko definiert und daraus werden wirksame Maßnahmen abgeleitet, für die ein optimiertes Budget vereinbart wird)
  d. Sonstige Antwort – bitte um Erläuterung!

Subforschungsfrage 4:

Liegt der Nutzen in der Herbeiführung der EU-DSGVO-Compliance nur in der Vermeidung von Nachteilen aus Datenschutzverletzungen oder erkennen die untersuchten Unternehmen weitere Chancen?

Verknüpfung zum Interviewleitfaden:

- Frage 8: Im Folgenden geht es darum zu beurteilen, welchen Nutzen das Sie betreffende Unternehmen aus dem Projekt zur Herstellung der EU-DSGVO-Compliance generieren kann. Wurde eine oder wurden beide der folgenden Arten von Nutzen erkannt und falls ja, nennen Sie bitte konkrete erkannte Nutzen aus den zutreffenden Kategorien:
  a. Vermeidung von Nachteilen (z.B. Reduktion des Strafrisikos, Vermeidung von Imageschäden)
  b. Generierung von Vorteilen (z.B. Steigerung der Wettbewerbsfähigkeit wie durch die Erfüllung von Vorgaben bei Ausschreibungen, Steigerung des Unternehmenswertes, Steigerung der Qualität und Effizienz)
- Frage 9: Sind im Sie betreffenden Unternehmen Projekte zu Themen wie Digitalisierung, Big Data und / oder Open Data ein Thema? Falls ja, konnten in diesem Zusammenhang Chancen durch das Projekt zur Herstellung der EU-DSGVO-Compliance erkannt werden?

Subforschungsfrage 5:

Wie planen die untersuchten Unternehmen den erkannten Nutzen zu realisieren und kann der erkannte Nutzen die entstehenden Aufwände decken?

Verknüpfung zum Interviewleitfaden:

- Es wird auch der erste Teil der Frage 8 wird zur Beantwortung der Subforschungsfrage 5 herangezogen
- Frage 10: Wurde der erkannte Nutzen auch monetär bewertet und gibt es geplante (Folge-) Projekte um ihn zu generieren?

Subforschungsfrage 6:

Versuchen die untersuchten Unternehmen einen wirtschaftlichen Mehrwert dabei zu generieren, sollen rein die Kosten gedeckt werden oder wird dies nicht betrachtet?

Verknüpfung zum Interviewleitfaden:

- Es wird auch hier Frage 10 wird zur Beantwortung der Subforschungsfrage 6 herangezogen
- Frage 11: Wurden die erwarteten Kosten dem genannten Nutzen gegenübergestellt?
  a. Wenn ja, konnte das Sie betreffende Unternehmen einen positiven Wertbeitrag aus dem Vorhaben ableiten?
  b. Wenn nein, warum nicht?

4.2.2 Datenquelle

Eine Auswahl an möglichen österreichischen Unternehmen für den empirischen Teil dieser Arbeit erfolgte danach, ob die möglichen Interviewpartner in eine der folgenden Kategorien fielen:

(1) Unternehmen die als Verantwortliche im stationären Bereich des Gesundheitswesens tätig sind, z.B. Betreiber von Krankenhäusern oder Rehabilitationseinrichtungen, aber auch Unternehmen im Bereich Lehre und Forschung oder der Sozialversicherung, die Patientendaten im stationären Bereich verantworten,
(2) Unternehmen die Auftragsverarbeiter für Verantwortliche im stationären Bereich des Gesundheitswesens tätig sind und Patientendaten verarbeiten, sowie
(3) Berater für solche Verantwortliche und/oder Auftragsverarbeiter.

Dabei ging es in erster Linie darum die Interviewpartner so einzugrenzen, dass diese jedenfalls Expertise im Umgang mit Gesundheitsdaten im Sinne der Verarbeitung und Verantwortung mitbrachten. Weiters galt es auszuschließen, dass Interviews mit Personen aus dem nicht stationären Bereich, wie z.B. niedergelassen Ärzten geführt wurden, da diese aufgrund ihrer Größe (Einzelpersonen oder kleine gemeinschaftlich geführte Arztpraxen) mit anders gelagerten organisatorischen Problemen konfrontiert sind. Und es sind Aufbewahrungsfristen für personenbezogene Daten im stationären Bereich von denen im ambulanten Bereich zu unterscheiden, was auch zu anderen Herausforderungen in der Behandlung dieser Daten führt.

Es wurden im nächsten Schritt Anfragen an Verantwortliche und Unternehmen in diesen Sektoren in Oberösterreich, Wien und Salzburg gestellt. Für Kategorie (1) erfolgten 6 Anfragen woraus sich 5 Zusagen und Interviews ergaben. Für Kategorie (2) erfolgte eine Anfrage zu der sich eine Zusage ergaben. Zu Kategorie (3) erfolgten drei Anfragen zu der sich eine Zusage ergab. Bei manchen Interviewpartnern der Kategorie (1) stellte sich im Zuge des Interviews heraus, dass Sie zusätzlich auch in Kategorie (2) fielen, was für die Untersuchung aber keinesfalls von Nachteil ist.

Es wurde bei der Auswahl der Experten darauf geachtet, dass sie über die relevanten Informationen entsprechend des Interviewleitfadens verfügten, dass sie in der Lage waren präzise Informationen zum betroffenen Unternehmen zu machen und natürlich wurde ihre Bereitschaft und Verfügbarkeit im Vorfeld abgeklärt. Dies war mitunter ein Grund, dass die Interviews alle anonym geführt wurden, da auch vertrauliche Informationen über die Unternehmen genannt wurden, wie z.B. der Budgetrahmen für das Vorhaben zur Einführung der EU-DSGVO-Compliance. Wären die Interviews nicht anonym geführt worden, dann hätten sich viele der Experten nicht zum Interview bereit erklärt. Berater wurden in der Vorbereitung zum Interview darauf hingewiesen, dass sie bei der Beantwortung der Fragen sich an einem beratenen Unternehmen im Gesundheitswesen orientieren sollen.

Soziodemographische Daten zu den Experten spielen bei der qualitativen Expertenbefragung keine Rolle und wurden daher nicht erfasst.[215] Da sich die Arbeit mit einer international gültigen Grundverordnung beschäftigt war es nicht relevant eine regionale Eingrenzung vorzunehmen. Dennoch wurden Interviews mit Experten aus Unternehmen mit Sitz in Wien (4), Oberösterreich (2) und Salzburg (1) geführt. Bei der Nennung der

[215] vgl Kaiser, R. (2014), S.72 und S.8

Eckdaten wird das Bundesland bewusst nicht angegeben, da man mit dieser Information in Kombination mit den anderen Eckdaten sonst schnell darauf schließen könnte aus welchem Unternehmen der Interviewpartner stammt.

Folgende Interviewpartner und Interviews konnten sodann durchgeführt werden:

Interviewdetails		Informationen zum Interviewpartner			
Code [216]	**Interview-termin**	**Position des Inter-viewpartners im Unterneh-men**	**Position des Interviewpart-ners im EU-DSGVO Projekt**	**Im eigenen Unternehmen oder im Kun-denauftrag mit der EU-DSGVO beschäftigt**	**Berater oder Ver-antwortlicher o-der Auftragsverarbei-ter im Sinne der EU-DSGVO**
E1	08.08.2017 um 08:30h, im Büro des Inter-viewpartners	Verantwortlicher für IT auf Grup-penebene	Mitglied im Projekt-lenkungsaus-schuss	im eigenen Unternehmen	Verantwortlicher
E2	22.08.2017 um 16:30h, in einem Café	ehem. Mitarbei-ter der Rechts-abteilung	ehem. Daten-schutzbeauftragter und Projektinitiator	im eigenen Unternehmen	sowohl Verantwortli-cher im Rahmen der akademischen For-schung, als auch Auftragsverarbeiter für Drittmittelfor-schungen
E3	24.08.2017 um 08:15h, in einem Bespre-chungszim-mer bei der Inter-viewpartnerin	Rechtsanwältin	Externe Beraterin des Kunden	im Kundenauftrag	Beraterin
E4	25.08.2017 um 11:30h, in einem Gastgarten	Bereichsleiter für Informati-onssicherheit und Daten-schutz	Verantwortlicher für das Management-system	beides (im eigenen Un-ternehmen und im Kundenauftrag)	sowohl Verantwortli-cher im eigenen Unternehmens, als auch Auftragsverar-beiter für Kunden
E5	31.08.2017 um 11h, im Büro des Inter-viewpartners	CISO	Projektleitung, ge-meinsam mit einer Kollegin	im eigenen Unternehmen	Verantwortlicher
E6	04.09.2017 um 14h, im Büro des Inter-viewpartners	CISO & Daten-schutzbeauf-tragter	Datenschutzbeauf-tragter	im eigenen Unternehmen	in erster Linie Ver-antwortlicher, aber auch Auftragsverar-beiter
E7	11.09.2017 um 09:15h, im Büro der Inter-viewpartnerin	CISO	Projektleitung	im eigenen Unternehmen	in erster Linie Ver-antwortliche, aber auch Auftragsverar-beiter z.B. für Töch-ter

Tabelle 1: Angaben zum Interviewpartner[217]

[216] Die Interviewpartner wurden mit einem Code versehen, damit auch in den weiteren Ausführungen auf die einzelnen Experten verwiesen werden kann. Das E im Code steht für Experte und die Nummer sagt aus um das wievielte Interview von den sieben durchgeführten es sich im zeitlichen Verlauf handelt.

[217] Quelle: eigene Darstellung

Es wurden in Summe sieben Interviews geführt. Dabei wurden fünf Interviews mit Verantwortlichen im Gesundheitswesen geführt. Alle fünf Unternehmen sind Betreiber von stationären Gesundheitseinrichtungen, teilweise aber nicht nur ausschließlich. Schwerpunktmäßig sind zwei im Bereich Rehabilitation und drei im Bereich Krankenversorgung bzgl. der zu verantwortenden Gesundheitseinrichtungen engagiert. Eines der fünf Unternehmen ist auch im Bereich Forschung und Lehre und ein anderes Unternehmen in der Sozialversicherung tätig. Weiters ist ein Experte interviewt worden, der für einen Auftragsverarbeiter aus dem Bereich IT-Dienstleister tätig ist. Ein weiteres Interview konnte mit einer Interviewpartnerin aus der Rechtsberatung geführt werden.

Folgende Eckdaten beschreiben den Kontext der betreffenden Unternehmen zu welchen die Interviewpartner Aussagen getätigt haben:

Informationen zum betreffenden Unternehmen				
Code	**Branche und Unternehmenszweck**	**Unternehmensgröße**	**Internationaler Vorjahresumsatz der Unternehmensgruppe**	**errechnetes Schadensausmaß**
E1	Gesundheitswesen, Errichtungs- und Betriebsprojekte	8.200 Mitarbeiter	Teil eines international agierenden Mutterkonzerns; Jahresumsatz des Mutternkonzerns 2016: rd. € 29 Mrd. Jahresumsatz des betroffenen Unternehmens 2016: rd. € 1,16 Mrd.	Mutternkonzern -> Strafe bis zu rd. € 1,16 Mrd.; betroffenes Unternehmen -> Strafe bis zu rd. € 46 Mio.
E2	Forschung und Lehre im Gesundheitswesen	4.400 Mitarbeiter, davon 1.600 Ärzte und ca. 3.000 wissenschaftliche Mitarbeiter	rd. € 512 Mio., 390 Mio. daraus kommen vom Staat Österreich	als öffentliche Stelle unterliegt das Unternehmen keinen Geldbußen nach Art. 83 DSGVO
E3	Gesundheitswesen	mehr als 1.000 Mitarbeiter	im Mrd. Bereich	Strafen im Mio. bzw. Mrd. Bereich
E4	IT-Dienstleister im Gesundheits- und Sozialwesen	190 Mitarbeiter	rd. € 21 Mio.	bis zu 4% des Vorjahresumsatzes, d.h. das wären € 840.000, -- Strafausmaß als Verantwortlicher und bis zu 2% des Vorjahresumsatzes, d.h. das wären € 420.000, -- Strafausmaß als Auftragsverarbeiter.
E5	Gesundheitswesen, Sozialversicherung	1.200 Mitarbeiter	laut dem letzten veröffentlichten Jahresbericht 2015: rd. € 3,6 Mrd. Pensionsversicherung; rd. € 1 Mrd. Krankenversicherung; rd. € 140 Mio. Bundespflegegelder; in Summe rd. € 7,74 Mrd. Umsatz; die Zahlen für 2016 sind noch nicht veröffentlicht, aber ähnlich	mögliche Strafen zwischen € 95 Mio. (2%) und € 190 Mio. (4%); da es sich um eine öffentliche Stelle handelt entfallen die hohen Geldbußen an sich; wobei aber für Beteiligungen an Gesundheitseinrichtungen nicht ausschließbar ist, dass das Strafausmaß herangezogen werden könnte; dies wird derzeit noch juristisch geprüft und bis-

				lang wird daher vom worst-case ausgegangen
E6	Betreiber von Gesund-heitseinrich-tungen	7.158 Mitarbeiter (davon 1.037 Ärzte und sonsti-ge akademische Mitarbeiter, 3.583 Pflegefach- und Pflegehilfsmitar-beiter, 737 medi-zinisch-technische Mitar-beiter und Heb-ammen, 1.732 im Bereich Verwal-tung und Betrieb sowie 69 Mitarbei-ter in anderen Bereichen)	Jahresbericht 2016: rd. € 535 Mio. Euro	€ 10,7 Mio. (bei Strafausmaß von 2%) bzw. € 21,4 Mio. (bei Strafausmaß von 4%)
E7	Gesund-heitsdienst-leister	rd. 6.000 Mitarbei-ter konzernweit	rd. € 500 Mio.	bei einem Strafausmaß von 2% bzw. 4% wären die € 10 Mio. bzw. € 20 Mio. erreicht

Tabelle 2: Angaben zum betreffenden Unternehmen der Interviewpartner[218]

Folgende Eckdaten beschreiben den Kontext der betreffenden EU-DSGVO-Compliance Vorhaben in diesen Unternehmen:

Informationen zum EU-DSGVO Projekt					
Code	**Leitende Abteilung für das EU-DSGVO Projekt**	**Involvierte Ab-teilungen in das EU-DSGVO Projekt**	**Projektstart**	**geplante Projektdauer**	**warum über den 25.05.2018 hinaus?**
E1	Rechtsabtei-lung	IT, Personal, Konzernkommu-nikation	August 2017	11 Monate; bis Ende Juni 2018	Wegen etwaiger Nachar-beiten und der Etablie-rung des Auditprozesses
E2	Rechtsabtei-lung	IT, Personal	voraussichtlich im Q3 2017, aktuell findet ein Vorprojekt statt	formal noch nicht definiert	Voraussichtlich wird die Projektdauer darüber hinausgehen, denn es sind sehr viele Arbeiten zu erledigen
E3	Rechtsabtei-lung	IT, Personal	schon in 2017 gestartet	überwiegende Projektteile bis zum 25.05.2018, aber weitere Arbeiten dar-über hinaus	Wegen etwaiger Nachar-beiten

[218] Quelle: eigene Darstellung

E4	Informations-sicherheit und Daten-schutz	Fachbereiche werden je nach Bedarf hinzuge-zogen	ein bestehendes System wird seit dem Q4 2016 ausgebaut	nicht definiert	kontinuierliche Verbesse-rung des bestehenden Systems; daher kein geplantes Ende
E5	die für Risi-komanage-ment zuständige Abteilung	Abteilungen aus allen Unternehmensbereichen	Juni 17	an sich bis zum 25.05.2018; wird aber erst festge-legt, da das Gesamtvorha-ben in 2 Projek-te geteilt ist und der Projektplan für das zweite Projekt erst im Q4 2017 verab-schiedet wird	möglicherweise wegen etwaiger Nacharbeiten
E6	Es gibt Fol-geprojekte aus einem Analysepro-jekt; das betroffene Folgeprojekt dem Bereich Informations-sicherheit & Datenschutz zugeteilt	IT, Recht und andere Abteilun-gen werden nach Bedarf hinzuge-zogen	es wurde schon im Frühjahr 2017, nach den Analyseergeb-nissen des Vor-projekts, gestartet	geplant mit 25.05.2018, aber weitere Arbeiten dar-über hinaus sind denkbar	Wegen etwaiger Nachar-beiten
E7	Geschäfts-führung	IT, Recht, Patien-tenadministration, Ärzteschaft, Pfle-ge, Facility Ma-nagement	formaler Start im Juli 2017; prak-tischer Start mit 1. September 2017	gesetzlich rele-vante Projektteil-e bis zum 25.05.2018, mit anschließender Evaluie-rungsphase bis 30.09.2018	Im Mai erfolgt die Über-gabe in die Linie und somit wurde auch ge-plant, dass es im An-schluss noch eine Evaluierungsphase gibt (bis 30.09.2018)

Tabelle 3: Angaben zu den betreffenden EU-DSGVO Projekten der jeweiligen Unternehmen[219]

Die Interviews wurden persönlich geführt und via Diktiergerät aufgezeichnet. Die Interviewpartner gaben zu diesen Aufzeichnungen ihre Zustimmung und erhielten auch die Transkripte im Anschluss zu Ihrer Information übermittelt. Zum Schutz der teilnehmenden Personen bzw. betroffenen Unternehmen wurden die Interviews anonymisiert.

In Summe liegen 132 Minuten Tonmaterial, 52,5 Seiten Transkript und 184 codierte Paraphrasen vor. Ein Interview dauerte im Durchschnitt ca. 19 Minuten.

4.3 Die qualitative Inhaltsanalyse

Die Transkripte wurden einer qualitativen Inhaltsanalyse nach dem Ablaufmodell der zusammenfassenden Inhaltsanalyse nach Mayring unterzogen. Das Ablaufmodell stellt sich wie folgt dar:

[219] Quelle: eigene Darstellung

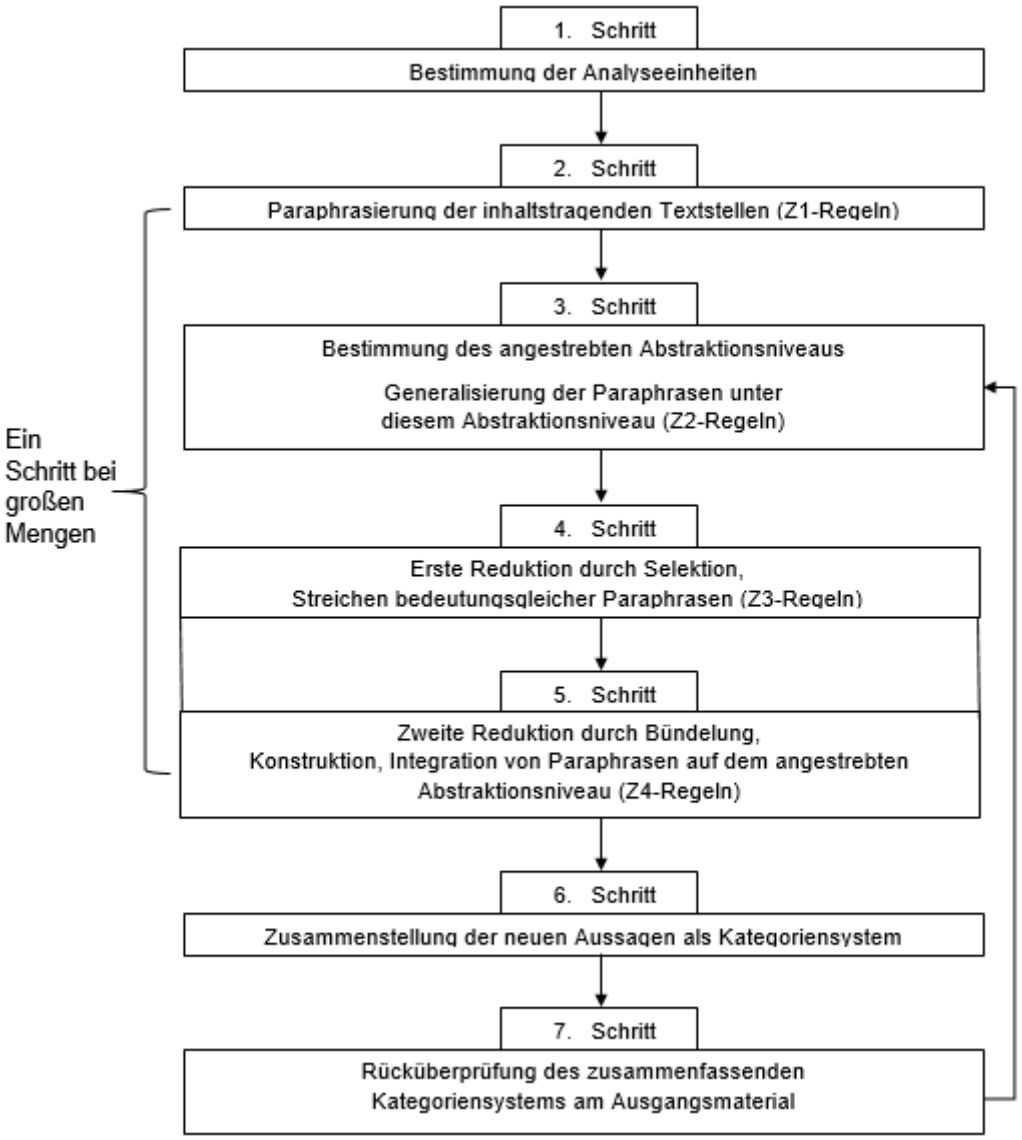

Abbildung 9: Ablaufmodell zusammenfassender Inhaltsanalyse[220]

Im ersten Schritt wird eine Analyse der Erkenntnisse der Interviews durchgeführt. Dabei wird das transkribierte Tonmaterial in Aussagen, als kleinste Analyseeinheit gegliedert und paraphrasiert. Jede Analyseeinheit wurde im nächsten Schritt auf Merkmale bzw. Kategorie hin geprüft. Wenn eine Aussage zuteilbar war, dann wurde diese codiert. Die codierten Paraphrasen werden dann vereinheitlicht um doppelte oder nicht relevante Paraphrasen streichen zu können, dies spiegelt die Schritte der Generalisierung und Reduktion wieder. Im letzten Schritt wird die notwendige Information aggregiert und je Fragestellung kategorisiert bzw. Variablen innerhalb der Kategorien zugeteilt. Das ganze Kategoriensystem wird nochmals gegen das Ursprungsmaterial überprüft. Durch dieses Vorgehen wird nun eine Auswertung der Ergebnisse möglich.

[220] Abbildung entnommen aus: Mayring, P. (2015), S. 70

Bei der Interpretation werden dabei drei Grundformen des Interpretierens unterschieden: die Zusammenfassung, die Explikation und die Strukturierung. Bei der Zusammenfassung reduziert man die Inhalte der Transkripte auf das Wesentliche. Dabei wird durch Abstraktion reduziert, aber in einer Form, dass immer noch das Abbild des Grundmaterials gegeben ist. Bei der Explikation werden zu einzelnen Textteilen, die fraglich sind, zusätzliche Materialien herangetragen, die dann zur Erläuterung dienen. Im Falle dieser Arbeit war es z.B. öfter nötig den Kontext einer Aussage für eine Analyseeinheit zu ergänzen. Bei der Strukturierung werden spezielle Aspekte aus den Transkripten gefiltert um sie nach bestimmten Kriterien einzuschätzen.[221]

Laut Atteslander ist der Kernpunkt einer jeder Inhaltsanalyse die Bildung von Kategorien. Diese werden aus theoretischen Annahmen abgeleitet. Die Summe aller Kategorien wird als Kategoriensystem bezeichnet. [222] Im Falle dieser Arbeit sind die Kategorien anhand der Forschungsfrage bzw. der Subforschungsfrage erarbeitet worden. Der Zusammenhang zwischen Frage und Kategorie besteht wie folgt:

Kategorien	Subforschungsfragen
Rahmenbedingungen	Subforschungsfrage 1
Herausforderungen	Subforschungsfrage 2
Budget	Subforschungsfrage 3
Chancen	Subforschungsfrage 4
Nutzen	Subforschungsfrage 5
Wirtschaftlichkeit	Subforschungsfrage 6

Tabelle 4: Konnex zwischen dem Kategoriensystem und den Subforschungsfragen[223]

Weiters wurden die Kategorien in Variablen (auch Merkmale genannt) gefasst. Jedes Merkmal kann dann eine oder mehrere Ausprägungen haben.[224] Die Variablen zu den einzelnen Kategorien werden im Rahmen der Präsentation der Ergebnisse je Kategorie vorgestellt.

[221] vgl Mayring, P. (2015): Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12. Aufl, Weinheim und Base, Beltz, S. 67
[222] vgl Atteslander, P. (2006), S.189
[223] Quelle: eigene Darstellung
[224] vgl Atteslander, P. (2006), S.189

5. Ergebnisse

Nachfolgend werden die Ergebnisse der empirischen Untersuchung präsentiert und interpretiert.

5.1 Darstellung und Interpretation der Ergebnisse

Im Folgenden werden die Antworten und Beobachtungen aus den Experteninterviews aufbereitet und interpretiert. Die Darstellung richtet sich nach den gebildeten Kategorien der Inhaltsanalyse, die, wie in 4.3 Die qualitative Inhaltsanalyse bereits dargestellt, mit den Sub-Forschungsfragen in Beziehung gesetzt wurden.

5.1.1 Kategorie „Rahmenbedingungen“

Bei diesem ersten Thema geht es um das Vorhaben „Herstellung der EU-DSGVO-Compliance“ an sich. In Verbindung mit dieser Kategorie steht die folgende Subforschungsfrage:

Subforschungsfrage 1:
Wie stellen Unternehmen mit Verantwortung für Gesundheitsdaten aus der österreichischen stationären Krankenversorgung die erfolgreiche Umsetzung eines Vorhabens zur Erfüllung der EU-DSGVO-Compliance bis Mai 2018 sicher?

Zu dieser Kategorie konnten im Rahmen der Untersuchung, entweder theoriegestützt oder im Rahmen der qualitativen Inhaltsanalyse folgende Variablen erkannt werden:

Variablen	Entwicklung
Awareness	während Analyse entdeckt
Commitment	theoriegeleitet entwickelt
Zielvorgaben	theoriegeleitet entwickelt
Bewertung der Zielerreichung	theoriegeleitet entwickelt
Managementsysteme	theoriegeleitet entwickelt
langfristig wirkende DSMS-Maßnahmen	theoriegeleitet entwickelt

Tabelle 5: Variablen der Kategorie "Rahmenbedingungen"[225]

Awareness und Commitment

Awareness (das Bewusstsein) und Commitment (das "Sich bekennen" bzw. "Sich verpflichten") stehen eng in Beziehung, beeinflussen einander gegenseitig und können auf

[225] Quelle: eigene Darstellung

unterschiedlichen Unternehmensebenen stattfinden. Man benötigt, wie bereits im Kapitel 3.1 Herausforderungen beschrieben, in der Regel das Commitment des Managements um die Awareness der Mitarbeiter inkl. der nachfolgenden Führungsebenen ("Tone from the Top") zu gewinnen. Um das Commitment des Managements zu erhalten, muss aber zuerst auch eine gewisse Management-Awareness, auch im Sinne eines Bewusstseins für die Herausforderungen, einhergehende Komplexität, bzw. den Nutzen des Themas, vorhanden sein. Diese wird oft, wie auch im Rahmen der Interviews deutlich wurde, von thematisch verantwortlichen Mitarbeitern forciert.

Bei allen Interviewpartnern (E1, E3, E4, E5, E6 und E7[226]), bei denen eine volle **Management-Awareness** vorlag, dort gab es auch ein klares Management-Commitment. Einige (E1 und E4) betonten auch explizit, dass das Thema bzw. Vorhaben einen hohen Stellenwert beim Management genießt. E2 hingegen sprach von mangelnder Management-Awareness. Es wurde zwar die Wichtigkeit des Themas Datenschutz an sich erkannt, aber es fehlt vor allem das Verständnis für die Komplexität des Vorhabens und dem damit verbundenen Ressourcenbedarf. Und in diesem Fall sprach der Interviewpartner E2 auch nur von einem eingeschränkten Management-Commitment:

„[…] das Wichtigste und das Schwierigste ist ein volles Commitment zu bekommen und damit meine ich jetzt auch die erforderlichen Ressourcen zu erhalten."

Ein klares **Management-Commitment** lag beim Interviewpartner E4 vor, der Auftragsverarbeiter ist, sowie bei den Experten die Gesundheitseinrichtungen betreiben (E1, E5, E6, E7). Auch E3, die als Rechtsberaterin für ein verantwortliches Unternehmen sprach, erkannte dort ein vorliegendes Management-Commitment. Experte E2, der sowohl als Verantwortlicher als auch als Auftragsverarbeiter agiert, konnte nur ein schwach ausgeprägtes Commitment anführen. Er führt dies darauf zurück, dass dieses Unternehmen als öffentliche Stelle nicht mit den hohen Strafen von bis zum € 20 Mio. bzw. 4% des internationalen Konzernumsatzes des Vorjahres rechnen muss. Aber auch E5 ist Verantwortlicher in einer öffentlichen Stelle. Hier gibt es allerdings einen Unterschied, da diese Organisation neben ihrer Haupttätigkeit auch Gesundheitseinrichtungen betreibt, für die im Rahmen der juristischen Prüfung noch nicht geklärt werden konnte, ob hier ggf. auch das hohe Strafausmaß zu tragen kommen kann. Man geht daher vom worst-case aus und setzt daher die Projektvorgaben entsprechend.

[226] Bei E7 wurde es im Interview nicht direkt ausgesprochen, im Kontext sowie den Gesprächen vor und nach dem Interview und dem angesprochenen Folgeprojekt lässt sich aber darauf schließen, dass es gegeben ist.

Weiters hatten alle Unternehmen (E1, E3, E4, E5, E6 und E7), in denen Management-Awareness vorlag, bereits in irgendeiner Form mit dem Vorhaben zur Umsetzung der EU-DSGVO-Compliance operativ gestartet. Auch wenn der **Projektfortschritt** sehr unterschiedlich war. Viele befanden sich erst in frühen Projektphasen wie E1 und E7. E5 hatte beispielsweise schon einen großen Teil des ersten Projektteils, des Analyseprojekts abgewickelt. E6 hat schon ein Analyseprojekt abgeschlossen, welches noch vor dem Beschluss der EU-DSGVO gestartet wurde. Das Folgeprojekt zur Umsetzung der Maßnahmenempfehlungen wurde bei E6 ebenfalls bereits im Frühjahr 2017 gestartet. Und E4 sprach davon, dass das Vorhaben aufgrund bereits sehr reifer, bestehender Prozesse in diesem Bereich, kein echtes eigenes Projekt benötige, sondern die zu ergreifenden Maßnahmen eher im Zuge eines kontinuierlichen Verbesserungsprozesses des bestehenden Managementsystems voranschritten. Bei E2 hingegen gab es zum Zeitpunkt des Interviews noch keinen Projektstart.

Zielvorgaben und Bewertung der Zielerreichung

Bei den Projektzielen bzw. Zielen der Umsetzungsvorhaben wurde überwiegende geantwortet, dass das ernannte **Hauptziel die Erreichung der EU-DSGVO-Compliance** sei (E1, E2, E4, E6 und E7).

E2 ergänzte dazu, dass es für das ihn betreffende Unternehmen vor allem wichtig wäre, dass Unternehmensexterne die Erfüllung der Compliance wahrnehmen können. E3 und E7 gaben an, dass dazu sogar mehrere Ziele vereinbart wurden. Auch E6 zählte die Sub-Ziele Erfüllung der Betroffenenrechte, das Führen des Verfahrensverzeichnisses, die fristgerechte Meldung etwaiger Data-Breaches und das Durchführen der Datenschutzfolgeabschätzungen bis zum gesetzlichen Stichtag auf. E3, E4 und E6 führten an, dass man sich dessen bewusst sei, dass es keine 100%ige Erreichung der EU-DSGVO-Compliance zum Stichtag des 25.05.2018 geben könnte und dass man daher einen **risikobasierten Ansatz** verfolge. E3 erklärte diese Tatsache wie folgt:

[…] in den großen, sehr großen Unternehmen kann man sicherlich nicht 100%ige Compliance sofort schaffen, aber eben ein Minimum, sodass man vorweisen kann das man schon etwas getan hat, gestartet hat und in dem Zusammenhang dann aber definitiv eine Risikoorientierung. […]

E4 erwähnte, dass im Falle des ihn betreffenden Unternehmens die kritischste Kundengruppe im Rahmen der Compliance-Umsetzung verstärkt fokussiert werden würde. Was auch einer Risikofokussierung entspricht.

Bei keinem Interviewpartner konnte festgestellt werden, dass das betreffende Unternehmen **formalisierte, präzise messbare Projektziele** bzw. Ziele für das Umsetzungsvorhaben definiert hat. E3 erklärte, dass das sie betreffende Unternehmen mehrere Ziele definiert hätte und auch E7 hatte eine Liste an Projektzielen vorliegen, die sie als prinzipiell überprüfbar erklärte. Aber es hat kein Interviewpartner angegeben, dass er ein Vorgehen anwende mit dem er den Grad der zu erreichenden Compliance zum 25.05.2017 ausdefiniert vorgeben und auch messen könnte. E4 war der Einzige der überhaupt eine Methode anwandte um zu überprüfen, ob die Compliance gewisser Maßen ausreichend umgesetzt wurde, indem er ein jährliches externes Datenschutzaudit durchführen lässt. Unter den Experten konnten aber unterschiedliche Ansichten zum Thema erfolgreich durchgeführter externer Datenschutzaudits als mögliche Zielvorgabe erkannt werden. E2 erläuterte in diesem Zusammenhang, dass man sich mit der Messbarkeit im Bereich der Compliance generell sehr schwer täte. Seiner Meinung nach wären auch externe Audits zur Überprüfung der ausreichenden Herstellung von Compliance kein adäquates Mittel, da ein beauftragter externer Auditor ggf. andere Themenschwerpunkte setzen könnte als eine prüfende Behörde, wodurch man wiederrum keine Gewissheit zum tatsächlichen Grad der Compliance erlangen könne.

<u>Managementsysteme und langfristig wirkende DSMS-Maßnahmen</u>

Sowohl Interviewpartner E1 und E4 konnten können bereits im sie betreffenden Unternehmen eine Datenschutz-Management-System vorweisen, welches nur noch anforderungsadäquat adaptiert werden muss. Andere Interviewpartner erklärten, dass solche Systeme zukünftig durch die Projekteinführung auch vorgesehen sind (E5 und E7) bzw., wie im Falle von E6, ein bereits bestehendes ISMS um das DSMS erweitert werden soll. Bei E7 ergibt sich sogar die Situation, dass nach erfolgreicher Einführung des DSMS die Einführung eines ISMS angedacht ist. Der Nutzen bzw. die **Notwendigkeit von DSMS wurde in der Regel erkannt**. E2 erklärte, dass aufgrund der eben nicht gegebenen Management-Awareness eine Diskussion zu diesem Thema nicht geführt werden konnte und daher keine Einführung eines DSMS vorgesehen ist.

Daher gaben die Interviewpartner E1, E4, E5 und E7 auch im Zusammenhang mit der Frage nach langfristig wirkenden DSMS-Maßnahmen an, dass sie ggf. **bestehende Managementsysteme und Auditprozesse** einführen bzw. in dem Sinne adaptieren, damit diese zukünftig EU-DSGVO-konform sind.

Als weitere nachhaltige Maßnahmen wurden Prozessstandardisierungen und Systembereinigungen erkannt. Zum einen werden in den Bereichen der einzuführenden Prozesse, wie im Bereich der Betroffenenrechte, namentlich genannt beim Recht auf Auskunft angedacht. E1 sprach diesbezüglich über eine konzernweite **Standardisierung** der Handhabung dieses Ablaufs. Auch E3 erwähnte Standardisierungen, erklärte aber dass diese voraussichtlich erst nach dem 25.05.2018 implementiert werden sollen. Dies gilt auch für die häufig genannten mitgedachten Möglichkeiten für (IT-)Systembereinigungen (E2, E3, E4). Allerdings wurde hier häufig erklärt, dass diese Bestrebungen in erster Linie von der IT ausgingen und kein erklärtes Projektziel, sondern eher ein Nebenprodukt wären bzw. eine Gelegenheit um sich über den aktuellen Stand einen Überblick zu verschaffen, wie E4 meinte. E7 stellte klar, dass in der knappen verbleibenden Zeit kein Fokus mehr auf Standardisierungen gelegt werden könne, aber wenn die Sinnhaftigkeit solcher erkannt werden würde, dann würde man die Verantwortlichen darüber informieren.

Interpretation

Zusammenhänge konnten zwischen den Faktoren Strafausmaß, Awareness und Commitment, Projektfortschritt und zur Verfügung gestellte Ressourcen ausgemacht werden. Es wäre interessant weiter zu hinterfragen, ob das Management-Commitment tatsächlich durch die hohen Strafandrohungen getrieben ist. Dies wurde in den Interviews von mehreren Experten auch so angesprochen, wie z.B. E7:

„[...] Das Gesetz zieht jetzt deswegen aus meiner Sicht so stark, […] wegen den Strafen. Das ist das was Vorstände usw. jetzt […] treibt dazu das auch richtig [...] an dieser hohen Stelle zu positionieren […]“

Und E6 spricht weiters an, dass man darüber nicht nur das Management-Commitment, sondern auch das Commitment anderer Verantwortlicher im Unternehmen gewinnen kann:

„Das sind doch so horrende Strafdrohungen, dass hier relativ schnell Einsicht [...]die hohen Strafen überzeugen auch die Leute die eher abgeneigt von solchen Maßnahmen waren, die was in die Richtung gezielt haben, dass man die Sicherheit erhöht.“

Auf die Empfehlung zu weiteren Untersuchungen zu möglichen Hypothesen aus den Erkenntnissen der Kategorie „Rahmenbedingungen“ wird im Kapitel 5.2 Erkannte mögliche Korrelationen eingegangen.

Das **oberste Ziel** - sei es formal festgelegt oder auch nur ausgesprochen - dass in den Interviews genannt wurde, war bei allen die **Herstellung der EU-DSGVO-Compliance bis zum 25.05.2018**. Dieses Ziel wurde aber nie formalisiert. Kein Interviewpartner beschrieb in klaren Worten, wann die ausreichende Compliance erreicht sei und wie man dies auch messen könne. Auch Überlegungen dahingehend, sich über beauftragte externe Audits EU-DSGVO-Compliance attestieren zu lassen, wurde mit stichhaltigen Argumenten anderer Experten in Zweifel gezogen.

Ganz klar zeichnet sich in diesem Zusammenhang auch das Bild, dass den Unternehmen bewusst ist - vor allem aufgrund noch **mangelnder Vorgaben bzw. fehlender Guidelines** z.B. von der Datenschutzbehörde oder weitere ausstehende Sondergesetzgebungen des nationalen Gesetzgebers - dass die Erreichung einer 100%igen Compliance bis zum gesetzlichen Stichtag unrealistisch scheint. Man wählt daher eher den **risikobasierten Ansatz** und orientiert sich in den Zielen an "einem guten Maß an Compliance", so dass man vorweisen kann „schon etwas getan zu haben“ (E3) um damit Fahrlässigkeit auszuschließen. Aber fest steht auch, dass unscharfe Zielvorgaben mit fehlender Messbarkeit der Zielerreichung, wie es hier in der Regel der Fall ist, entsprechend klassischer Projektmanagement Literatur keine gute Startvoraussetzung für ein Projektvorhaben dieser Größenordnung sie. Teilweise wurden Teilprojektziele abgeleitet, aber niemand hat klar formuliert welcher Umstand bestätigt, dass das Ziel „EU-DSGVO-Compliance“ ausreichend erreicht ist. Vielmehr wird von einem ständigen Prozess gesprochen, der **eine kontinuierliche Verbesserung** des Compliance-Zustands mit sich bringen soll, wie bei E4:

„Aber wahrscheinlich wird man da auch den Weg gehen mit Betriebsführungskunden mal zu starten, nach dem risikobasierten Ansatz […] und dann mal diese zuerst zu machen und dann zu sagen im Rahmen eines Managementsystems über die Jahre hinweg […] das zu erweitern, ja.“

Daher kann man schließen, dass für die Vorhaben zur Erreichung der EU-DSGVO-Compliance zwar der **Output** der Projekte und Vorhaben definiert ist, aber kein **Outcome** festgelegt werden kann. D.h. das Maß der Wirksamkeit der Maßnahme, also der tatsächliche Nutzen, ist schwer bewertbar.

Die Einhaltung der **Kriterien der erfolgreichen Umsetzung eines Compliance Projektes**, wie diese in **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.** erläutert wurden, wurden durch das Experteninterview für die betreffenden Unternehmen überprüft:

	Verantwortung	Planung	Qualitäts-steigerung	Budget
	Management-Commitment inkl. Mittel	**Umsetzung aufwandsredu-zierender Maß-nahmen**	**Maßnahmen für mehr Stabilität, Fehlerreduktion etc.**	**für nachhaltige Lösungen**
E1	Commitment vorhan-den	konzernweite Standardisierung für die Betroffenenrechte wie das Recht auf Auskunft		DSMS und -auditprozess initial vorhanden
E2	schwach ausgeprägtes Commitment	Systembereinigung war kein definiertes Ziel im Rahmen der Umsetzung - IT denkt das an, aber kein Fokus darauf		zum Projektfortschrittsgrad war keine DMS-Einführung vorge-sehen
E3	Vorstand verabschie-dete Projekt zur Um-setzung der Vorgaben im Unternehmen.	Systembereinigungen und Standardisie-rungen sind angedacht, werden voraus-sichtlich aber erst nach dem 25.5.2018 umgesetzt.		Geplante Maßnahmen die über die Herstellung der Compliance hinausgehen sind vermutlich geplant, da es schon vorher Compliance-Audits gab, die jetzt auf Datenschutz ausgeweitet werden.
E4	Commitment sowie die strategische Entschei-dung viel Wert auf Da-tenschutz zu legen ist vorhanden, da bei Missachtung sehr ne-gative Auswirkungen für das Unternehmen erwartet werden.	Vornahme von Optimierungen ist kein definiertes Ziel, das Vorhaben wird aber genutzt um sich vorbereitend dafür ei-nen Überblick zu verschaffen		Ein funktionierendes, interagie-rende ISMS und ein DSMS wurden bereits aufgebaut. Es existieren Auditprogramme, Prozesse etc. Für die EU-DSGVO-Compliance werden Adaptierungen vorgesehen.
E5	Volles Commitment ist vorhanden. Die Ge-schäftsführung hat gezielt beauftragt die Vorbereitungen für die EU-DSGVO mit vollem Tempo zu betreiben.	*Eine aufwandsreduzierende Implemen-tierung von Anforderungen erfolgt im zweiten erwähnten Programm; Aber mit Vereinfachungen in der Wertschöp-fungskette bzw. Bearbeitungsprozessen ist zu rechnen. Hoffnung auf Vereinfa-chungen in Bezug auf die Administration der Datenschutzthemen.*		*Das Projekt befindet sich in der Analysephase - das Umset-zungsprogramm wird erst kon-zipiert.*
E6	Ein volles Commitment seitens des Vorstands ist gegeben, was sich auch dadurch zeigt, dass er das Analy-seprojekt von sich aus beauftragt hat.	Das Audit-Management wird gerade neu aufgesetzt und es soll künftig Daten-schutz-Audits geben. Prozessstandardi-sierungen und Automatisierungen müssen soweit möglich eingeführt wer-den. Das betrifft auch die Betriebsfüh-rung, die getrieben von Ransomware Attacken und Lizenzaudits, darauf ach-tet muss, dass nur definierte Anwen-dungen in vorgegebenen Versionen zum Einsatz kommen. Für einen ver-nünftigen Betrieb benötigt es automati-sierte Verteilung und die Anwender dürfen über keine Adminrechte verfü-gen. Dazu muss auch Change-Management bzw. müssen generell alle Kernprozesse der IT verbessert werden.		Wir sind dabei ein Daten-schutzmanagementsystem zum Leben zu erwecken, im Sinne eines KVP's mit wiederholenden PDCA Zyklen, priorisierten Maßnahmen und Trendanaly-sen hinsichtlich Risikoentwick-lung. Das, was man aus dem ISMS kennt hätten wir auch beim Datenschutz vor.

E7	Es gibt ein volles Commitment seitens des Geschäftsführers. Das Commitment wird dadurch deutlich, dass der Geschäftsführer als Projektauftraggeber das Projekt beauftragt hat und budgetäre Mittel zur Verfügung stellt.	Im Projekt wir die Implementierung eines Datenschutzauditprozesses vorgesehen; Aufgrund der knappen verbleibenden sind Prozessoptimierungen nicht Teil des Datenschutzprojektes. Sollten aber Nichtkonformitäten zu bestehenden Prozessbeschreibungen im Zuge des Projekts erkannt werden, werden sie auf der Liste der Nicht-Konformitäten verzeichnet und dem zuständigen Verantwortlichen aufgezeigt.	Im Projekt wird die Implementierung eines Datenschutzmanagementsystems vorgesehen.

Tabelle 6: Bewertung der Erfolgskriterien für erfolgreiche Compliance-Einführungen an den 7 Experteninterviews[227]

Die Auswertung ergibt, dass in der Regel das Commitment sowie ein ausreichendes Budget, welches auch die Einführung von nachhaltigen DSMS Systemen vorsieht, vorliegt. Die Auswertung zeigt weiters, dass viele Interviewpartner die Themen, wie die Implementierung von Maßnahmen zur aufwandsreduzierten Implementierung der Anforderungen, wie der Umsetzung von Prozessstandardisierungen oder IT-Systembereinigungen zwar andenken, aber überwiegend nicht konsequent im Umsetzungsplan berücksichtigen. Dass die Folgen der Compliance zur Qualitätsverbesserung, Fehlerreduktion und Betriebsstabilität beitragen sollten, wird meist auch nur aus erwünschter Nutzen auf der persönlichen Agenda angeführt.

Den Kriterien der erfolgreichen Umsetzung eines Compliance Projektes nach wären die Unternehmen der jeweiligen Interviewpartner **überwiegend auf einem guten Weg**. Eine sehr erfolgreich wird nach diesen Vorgaben dem Einführungsprojekt von E1 und E6 zugesagt. Das schwache Commitment bei E2 schlägt sich auch auf die anderen Faktoren nieder und stellt damit keine guten Projektweichen. Eine Nachbetrachtung der Ergebnisse zur Evaluierung der Aussage der Gütekriterien wäre eine weitere interessante Folgeuntersuchung.

5.1.2 Kategorie „Herausforderungen“

Bei diesem zweiten Thema geht es darum zu erfahren mit welchen Herausforderungen die betroffenen Unternehmen sich konfrontiert sehen und welche ihrer Meinung nach die drei größten Herausforderungen sind. In Verbindung mit dieser Kategorie steht die folgende Subforschungsfrage:

[227] Quelle: eigene Darstellung

Subforschungsfrage 2:

Welchen technischen und organisatorischen Herausforderungen begegnen diese Unternehmen dabei?

Zu dieser Kategorie konnten im Rahmen der Untersuchung, entweder theoriegestützt oder im Rahmen der qualitativen Inhaltsanalyse folgende Variablen erkannt werden:

Variablen	Entwicklung
organisatorische Herausforderung	theoriegeleitet entwickelt
technische Herausforderung	theoriegeleitet entwickelt
größte Herausforderung	theoriegeleitet entwickelt
zweitgrößte Herausforderung	theoriegeleitet entwickelt
drittgrößte Herausforderung	theoriegeleitet entwickelt

Tabelle 7: Variablen der Kategorie "Herausforderungen"[228]

Es wurden technische und organisatorische Herausforderungen erkannt. Zu den **technischen Herausforderungen** zählt allen voran das Thema der anforderungskonformen Umsetzung des „Recht auf Vergessenwerden“. Diese Herausforderung wurde in vier Interviews angesprochen und ist die jedenfalls die kritischste der technischen Herausforderungen bzw. wohl aller Herausforderungen. Weitere technische Herausforderungen sind die folgenden genannten:

Technische Herausforderungen	Interviewpartner
Technische Umsetzung des Recht auf Vergessenwerden	E1, E4, E5, E6
Umsetzung der Verpflichtungen in der Form, dass Aspekte der Digitalisierung wie im Rahmen von privacy-by-design und -default mitberücksichtigt wurden	E3
fristgerechte anforderungskonforme Anpassung der IT-Systeme	E3
Abarbeitung von technischen Maßnahmen um am Stand der Technik zu sein, für EU-DSGVO und Gesundheitstelematikgesetz nach ISO 27001 und ISO 80001	E6
Bestehende, für das ISMS verwendete Tools überprüfen, ob sie die EU-DSGVO Anforderungen auch erfüllen können	E6

Tabelle 8: technische Herausforderungen laut der Interviewpartner[229]

Diese Maßnahmen, außer der normkonformen technischen Umsetzung des Recht auf Vergessenwerden, wurden aber von niemandem zu den drei größten Herausforderungen gerechnet.

[228] Quelle: eigene Darstellung
[229] Quelle: eigene Darstellung

Die **organisatorischen Herausforderungen** überwiegen deutlich. Es wurden mehr als dreimal so viele organisatorischen Herausforderungen wie technische Herausforderungen genannt:

Organisatorische Herausforderungen	Interviewpartner
Betroffenenrechte sind umzusetzen, wie das Recht auf Auskunft und damit einhergehend sind (IT-)Prozessanpassungen und -standardisierungen, Automatisierung und Zuständigkeiten im Unternehmen zu klären	E1, E3, E6
Selbstverantwortliche Erhebung von personenbezogenen Verarbeitungstätigkeiten und Entscheidung hinsichtlich des Führens im Verarbeitungsregister und der Durchführung der PIA	E3, E6, E7
Lösch-, Aufbewahrungs- und Informationspflichten für personenbezogene Datenarten abklären	E3, E5
Positive Awareness bei allen Mitarbeitern wecken	E2, E6
Beschaffung der benötigten Ressourcen	E2, E6
Datenschutz-Folgeabschätzungen durchführen	E3, E4
Überarbeitung von Dienstleister-, Lieferanten-, Mitarbeiter- und Kundenverträgen sowie der Einholung der Zustimmungserklärung beim Betroffenen	E3, E6
Der Aufbau einer Datenschutzorganisationsstruktur stellt die größte Herausforderung bzw. Organisationsanpassungen hinsichtlich der Einführung von Vertretern für Datenschutz und Informationssicherheit in allen Organisationseinheiten	E5, E7
Die Umsetzung des Awareness Themas inkl. eines verpflichtenden E-Learning Modul zum Thema Datenschutz und Informationssicherheit	E5, E7
Eine formalkorrekte Behandlung von Data Breaches	E3
geographische Ausbreitung und unbekannte gesetzliche Vorgaben in den einzelnen EU-Mitgliedsstaaten	E1
Commitment aller Beteiligten	E2
Die Umsetzung der Vorgaben der Auftragsverarbeiterpflichten stellt eine Herausforderung dar.	E4
Die Erarbeitung von Richtlinien und Vorgaben stellt eine Herausforderung dar. Das Vorhandene muss dabei auf die neuen gesetzlichen Bedürfnisse angepasst werden.	E7
Evaluierung und Kontrolle ist eine Herausforderung; ein Auditprozess mit Prüfbericht etc. wird eingeführt und im Projekt wird ein Auditplan aufgesetzt.	E7
Die Verabschiedung von Leitlinien des übergeordneten DACH-Verbands ist nicht auszuschließen.	E5
Die gegenseitige Abstimmung der Projekte stellt eine Herausforderung dar.	E5
Ein bestehendes nach ISO 27001 zertifiziertes ISMS wurde um ein DSMS erweitert um beide Managementsysteme zu integrieren.	E5

Tabelle 9: organisatorische Herausforderungen laut der Interviewpartner[230]

Die Interviewpartner wurden dazu befragt, welche dieser aufgezählten Herausforderungen für gereiht die drei größten waren:

[230] Quelle: eigene Darstellung

Herausforderung	Art[231]	Nennung		1.[232]	2.	3.
Technische Umsetzung des Recht auf Vergessenwerden	TEC	4	E1, E4, E5, E6		x (E1)	x (E4), x (E5)
Betroffenenrechte sind umzusetzen, wie das Recht auf Auskunft und damit einhergehend sind (IT-)Prozessanpassungen und -standardisierungen, Automatisierung und Zuständigkeiten im Unternehmen zu klären	ORG	3	E1, E3, E6			x (E1), x (E3 - Teilaussage), x (E6 - Teilaussage)
Selbstverantwortliche Erhebung von personenbezogenen Verarbeitungstätigkeiten und Entscheidung hinsichtlich des Führens im Verarbeitungsregister und der Durchführung der PIA	ORG	3	E3, E6, E7	x (E3)		x (E6 - Teilaussage)
Lösch-, Aufbewahrungs- und Informationspflichten für personenbezogene Datenarten abklären	ORG	2	E3, E5	x (E5 - für Patienten)	x (E5 - für Mitarbeiter)	E3
Positive Awareness bei allen Mitarbeitern wecken	ORG	2	E2, E6		x (E6)	x (E2)
Beschaffung der benötigten Ressourcen	ORG	2	E2, E6	x (E6)	x (E2)	
Datenschutz-Folgeabschätzungen durchführen	ORG	2	E3, E4		x (E4)	
Überarbeitung von Dienstleister-, Lieferanten-, Mitarbeiter- und Kundenverträgen sowie der Einholung der Zustimmungserklärung beim Betroffenen	ORG	2	E3, E6		x (E3)	x (E6 - Teilaussage)
Der Aufbau einer Datenschutzorganisationsstruktur bzw. Organisationsanpassungen hinsichtlich der Einführung von Vertretern für Datenschutz und Informationssicherheit in allen Organisationseinheiten	ORG	2	E5, E7	x (E7)		
Die Umsetzung des Awareness Themas inkl. eines verpflichtenden E-Learning Modul zum Thema Datenschutz und Informationssicherheit	ORG	2	E5, E7		x (E7)	
Eine formalkorrekte Behandlung von Data Breaches	ORG	1	E3			x (E3 - Teilaussage)
geographische Ausbreitung und unbekannte gesetzliche Vorgaben in den einzelnen EU-Mitgliedsstaaten	ORG	1	E1	x (E1)		
Commitment aller Beteiligten	ORG	1	E2	x (E2)		

[231] ORG steht für Organisatorisch und TEC steht für Technisch
[232] 1. steht für die größte Herausforderung, 2. steht für die zweitgrößte Herausforderung und 3. steht für die drittgrößte Herausforderung

Die Umsetzung der Vorgaben der Auftragsverarbeiterpflichten	ORG	1	E4	x (E4)		
Die Erarbeitung von Richtlinien und Vorgaben stellt eine Herausforderung dar. Das Vorhandene muss dabei auf die neuen gesetzlichen Bedürfnisse angepasst werden.	ORG	1	E7			X (E7)

Tabelle 10: die drei größten Herausforderungen[233]

Wohl eine der größten Herausforderung (weil sie am häufigsten genannt wurde, wenn auch nie explizit als Top-Herausforderung), kann die **technische Umsetzung des Rechts auf Vergessenwerden** gesehen werden. Dies mag vor allem auch daran liegen, dass hier noch große Unsicherheit herrscht, wie Daten anforderungskonform gelöscht werden müssen. E5 beschreibt die Problematik dabei wie folgt:

„[…] die technische Herausforderung, das Löschen ist eine Thematik die ganz kritisch gesehen wird. Es ist schon eine relativ große Herausforderung oft bei gewisse Systemkomplexitäten das man die Daten sauber in das System hinein bekommt mit allen Verknüpfungen, Abhängigkeiten, Berechnungen und ich denke noch schwieriger wird es dann werden die Daten auch wieder los zu werden auch dann im Hinblick auf diverse Backupsysteme, Backupbänder Stichwort was passiert wenn jetzt der Betroffene sagt er möchte seine Daten gelöscht haben ... es kommt dann irgendwo in einem System zu einem IT-Ausfall, man muss wieder zurückrollen zu einem bestimmten Stand, wie zieht man das dann wieder nach.“

Dabei spricht E4 zwei für ihn ungeklärte Themen an: komplexe Abhängigkeiten der personenbezogenen Daten über mehrere Systeme hinweg zu löschen, sicherzustellen dass die Daten von allen Medien entfernt wurden inklusiver der Medien für die Datensicherung. E6 setzt dem hinzu:

„[…] Da müssen wir schauen dass wir in den Datenbanken Felder hinterlegen, wo der Zweck warum wir es aufheben hinterlegt ist und dort wo es eine gesetzliche Grundlage gibt können wir sowieso nicht löschen. Nur dort wo es diese nicht gibt, müssen wir dann sowieso schauen nach dem Minimalprinzip dass gar nicht länger gespeichert sind als erforderlich und gegebenenfalls das man sie dann löscht. Das Löschen von Daten ist wahrscheinlich die größte technische Herausforderung.“

Diese Aussage inkludiert, dass die Hersteller der verwendeten Anwendungen im betroffenen Unternehmen noch keine ausgereifte Lösung zu dieser Problematik anbieten, was dadurch klar wird, dass der Experte davon ausgeht, dass das betroffene Unternehmen

[233] Quelle: eigene Darstellung

selbst Überlegungen anstellen muss um dabei sogar in die Datenbanken der Systeme einzugreifen.

Ebenfalls sehr häufig genannt wurde das Thema der **Erfüllung der Betroffenenrechte allgemein** und damit die Definition von (IT-)Prozessanpassungen, Standardisierungen, Automatisierung und Zuständigkeiten im Unternehmen zu klären.

Und es wurde auch von drei Experten genannt, dass die selbstverantwortliche Erhebung von personenbezogenen Verarbeitungstätigkeiten, die Entscheidung hinsichtlich des Führens im **Verarbeitungsregister und der Durchführung der PIA** vor allem sehr aufwendig werden würde. Dies ist im Gesundheitswesen klar so zu sehen, da nahezu jede Verarbeitungstätigkeit mit sensiblen Daten umgeht und daher eine PIA kaum zu vermeiden sein wird.

Weiters mehrfach genannt wurden:

- **Lösch-, Aufbewahrungs- und Informationspflichten** für personenbezogene Datenarten abklären: Hier geht es um die Erhebung der Anforderungen und somit Vorbereitung zur technischen Umsetzung des Recht auf Vergessenwerden. Es ist für jede personenbezogene Datenart zu klären in welchem System sie sich auf welcher rechtlichen Basis für wie lange befinden darf.
- **Positive Awareness bei allen Mitarbeitern** wecken: Dazu wurde erklärt, dass es wichtig ist den Kollegen zu vermitteln, dass Datenschutz in der Verantwortung aller liegt und dass es nicht ein Thema ist, dass ein Verantwortlicher für das Unternehmen umsetzen kann. Datenschutz geht jeden in seinem Einflussbereich an!
- **Beschaffung der benötigten Ressourcen**: Die benötigten Ressourcen, Budget aber auch Personal, sind nicht immer leicht zu erhalten. Ein Projekt wie dieses muss aber mit den ausreichenden Mitteln ausgestattet werden, da sonst die zentralen Grundvoraussetzungen nur schwer geschaffen werden können. Es gilt Management-Awareness in diesem Bereich zu schaffen und dem Management die Komplexität des Vorhabens klar zu machen.
- **Datenschutz-Folgeabschätzungen durchführen**: Den Experten ist klar, dass vor allem im Gesundheitswesen eine Menge an Verarbeitungstätigkeiten aufgrund der verarbeiteten sensiblen Daten einer PIA zu unterziehen sind.
- **Überarbeitung von Dienstleister-, Lieferanten-, Mitarbeiter- und Kundenverträgen** sowie der Einholung der Zustimmungserklärung beim Betroffenen: Oft ergibt sich diese Aufgabe erst nach näherer Betrachtung der zu erledigenden Themen. Beim Schaffen der Voraussetzungen für anforderungskonformes Verhalten wird klar, dass Verträge aller Art anzupassen sind.

- **Der Aufbau einer Datenschutz-Organisation** stellt eine große Herausforderung dar, sowie die Organisationsanpassungen hinsichtlich der Einführung von Vertretern für Datenschutz und Informationssicherheit in allen Organisationseinheiten. Gerade bei dezentralen Strukturen bzw. Konzernstrukturen verkomplizieren diese organisatorischen Themen die Projekte oft sehr.
- **Die Umsetzung des Awareness Themas** inkl. eines Schulungsprogramms. Teilweise wird dazu ein verpflichtendes E-Learning Modul zum Thema Datenschutz und Informationssicherheit produziert. Dies wiederum setzt auch das Vorhandensein von Richtlinien voraus.

Interpretation

In erster Linie sehen sich die Experten mit organisatorischen Herausforderungen konfrontiert, aus denen sich folglich vergleichsweise wenige technische Herausforderungen ableiten lassen. Besonders kritisch wird allerdings die **technische Umsetzung des Rechts auf Vergessenwerden** gesehen. Aber auch hier liegt die Begründung in mangelnder Rechtssicherheit, **mangelnder Vorgaben und Handlungsempfehlungen** von Behörden bzw. dem nationalen Gesetzgeber.

Organisatorische Grundsatzthemen wie Schaffung von Awareness, mangelnde Ressourcen und Organisationsstrukturen etc. wurden vor allem auch von Interviewpartnern in frühen Projektphasen genannt, denn wie wir bereits bei der Untersuchung der Rahmenbedingung erkennen konnten befinden sich die betrachteten Unternehmen in unterschiedlichen **Projektfortschrittsphasen**. Umgekehrt sieht man, dass abgesehen von der Herausforderung bzgl. des Rechts auf Vergessenwerden, andere technische Herausforderungen nur von der Rechtsberaterin E3 sowie dem Experten E6, der sich bereits in einem weit fortgeschrittenen Umsetzungsprojekt befindet, angeführt wurden. Von diesen beiden Experten wurden auch die aufwändigen Arbeitsschritte, wie die „Selbstverantwortliche Erhebung von personenbezogenen Verarbeitungstätigkeiten und Entscheidung hinsichtlich des Führens im Verarbeitungsregister und der Durchführung der PIA“ oder die „Überarbeitung von Dienstleister-, Lieferanten-, Mitarbeiter- und Kundenverträgen sowie der Einholung der Zustimmungserklärung beim Betroffenen“ als organisatorische Herausforderungen genannt. Es ist daher naheliegend anzunehmen, dass viele Interviewpartner noch gar nicht mit dem vollen Umfang der auf sie zukommenden Herausforderungen vertraut sind. Folglich würde dies erst nach den frühen Projektphasen bzw. Analyseprojekten deutlich werden.

Interessant ist auch die Erkenntnis, dass die Herausforderung bzgl. der Einführung und Ausgestaltung der Rolle des Datenschutzbeauftragten in den Interviews nicht genannt wurde. Auffällig ist, dass dieses Thema in der Literatur dezidiert adressiert und in den Interviews nicht mit einer entsprechenden Gewichtigkeit genannt wurde. Wenn, dann wurde es im größeren Kontext hinsichtlich allgemeiner Organisationsstruktur-Themen behandelt.

5.1.3 Kategorie „Budget“

Beim Thema Budget ging es um die Erhebung des Budgetrahmens sowie die Art der Ermittlung des Budgets. In Verbindung mit dieser Kategorie steht die folgende Subforschungsfrage:

Subforschungsfrage 3:
Welchen Aufwand kalkulieren die untersuchten Unternehmen um den Herausforderungen gerecht zu werden?

Zu dieser Kategorie konnten im Rahmen der Untersuchung, entweder theoriegestützt oder im Rahmen der qualitativen Inhaltsanalyse folgende Variablen erkannt werden:

Variablen	Entwicklung
Budgetrahmen	theoriegeleitet entwickelt
Budgetermittlung	theoriegeleitet entwickelt

Tabelle 11: Variablen der Kategorie "Budget"[234]

Bzgl. des **Budgetrahmens** konnte im ersten Schritt ermittelt werden, dass an sich alle Unternehmen, die im Rahmen der Interviews thematisiert wurden, ein Budget zur Verfügung haben. Teilweise ist es kein formal freigegebenes Budget, wie bei E4. Das liegt daran, dass die zu ergreifenden Maßnahmen im Rahmen eines kontinuierlichen Verbesserungsprozesses aus den laufenden Betriebskosten heraus finanziert werden und nicht über ein eigenes Projekt mit Projektbudget. Auch E2 sprach von einem Budget, aber dieses belief sich deutlich unter dem angegebenen Rahmen der Studie. Die Besonderheit bei E2 und E4 im Vergleich zu anderen Experten von betroffenen Unternehmen ist die Tatsache, dass dort das Management bevorzugte, dass die Arbeiten in House und ohne Einbindung von externen Beratern und / oder Juristen zu erfolgen hat.

[234] Quelle: eigene Darstellung

Experte	Variablenausprägung
E1	Im Rahmen der Studie bis deutlich darüber
E2	Deutlich unter dem Rahmen der Studie
E3	Im Rahmen der Studie
E4	Deutlich unter dem Rahmen der Studie
E5	Voraussichtlich im Rahmen der Studie
E6	Im Rahmen der Studie
E7	Im Rahmen der Studie

Tabelle 12: aufgetretene Merkmalausprägungen zum Budgetrahmen[235]

Die anderen Interviewpartner hatten im Gegensatz zu E2 und E4 ein Budget im Rahmen der Studie vorzuweisen. Der Interviewpartner E1 hat ein Budget im Rahmen der Studie für das Projekt vorgesehen, allerdings rein für das Organisationsprojekt auf Konzernebene. Wenn man die zusätzlichen, in den einzelnen Standorten vorgesehen Budgets dazu kalkuliert, wird man einen Betrag erhalten, der voraussichtlich deutlich über dem Rahmen der Studie liebt. E3, E6 und E7 geben an, dass sie Budget im Rahmen der Studie zur Verfügung haben. E6 führt dabei ein zweigeteiltes Projekt durch. Die Analysephase wurde aber schon im Frühjahr 2017 mit Empfehlungen und Aufwandschätzungen abgeschlossen. Im Anschluss wurde nahtlos das Umsetzungsprojekt gestartet. Das Budget dafür ist daher bereits freigegeben und befindet sich im Rahmen der Studie. Beim Interviewpartner E5 ist das Projekt ebenfalls in zwei Projektteile geteilt, wobei man sich derzeit im ersten, eher analyse-lastigen Teil des Projekts befindet. Für die Analysephase wurde bereits ein Budget freigegeben, für die Umsetzungsphase ist dies im Oktober geplant. Dabei ist davon auszugehen, dass das Gesamtbudget sich im Rahmen der Studie bewegen wird. Daher rührt die Formulierung „Voraussichtlich im Rahmen der Studie“.

Bei der Frage nach der **Budgetermittlung** gaben alle bis auf E2 und E7 an, sich nach dem Optimalprinzip mit dem risikobasierten Ansatz zu richten, bzw. wurde teilweise (E5 und E6) erklärt, dass sogar ein zweistufiges Verfahren angewandt wurde, wie E5:

„Ich denke wir haben da eine Mischung drinnen. Ich würde sagen die [...] das gesamte Projekt Analyse inklusive Umsetzung begehen wir nach dem Optimalprinzip. Also wir analysieren jetzt welche Maßnahmen sind erforderlich. Welches Risiko soll zukünftig genommen werden, würden dann daraus im Endeffekt den Projektplan schneiden und hier zur Budgetschätzung kommen. Also da würde ich eigentlich grundsätzlich sagen sind wir im Optimalprinzip unterwegs. Die Analysephase selbst haben wir meiner Meinung nach aus dem Minimalprinzip heraus gemacht. Also wir haben definiert was das Ergebnis der Ana-

[235] Quelle: eigene Darstellung

lysephase sein soll und anhand dessen dann im Endeffekt mehrere Vergleichsangebote schätzen lassen oder eingeholt“

E2 hat das Budget nur anhand von Erfahrungswerten geschätzt, dem gingen aber keine risikobasierten Überlegungen voraus. Bei E7 wurden die budgetären Mittel vorgegeben und E7 versucht in diesem Rahmen die Mittel bestmöglich einzusetzen.

Interpretation

Budgets für die Vorhaben sind prinzipiell in allen Interviews genannt worden. In der Regel befinden sich die Budgets auch im angegebenen Rahmen der im Kapitel 3.2 Kosten und Budgets thematisierten Studie der TRUSTe Inc., d.h. zwischen ca. € 90.000, -- und €445.000, --. Interessant ist die Erkenntnis hinsichtlich der Tatsache, dass es tatsächlich bei allen betroffenen Unternehmen **ein Budget gibt** und dieses, bis auf Ausnahmen, auch **angemessen bemessen** wird und das obwohl das Gesundheitswesen unter stetigem Kostendruck steht.

Ein Experte gab sogar an, dass das Budget über den Gesamtkonzern gesehen sogar über dem Budgetrahmen der Studie liegt. Es nannten nur zwei Experten einen deutlich niedrigeren Wert. Dies ist dort der Fall, wo bereits ein gut entwickeltes DSMS existiert, das nur adaptiert werden muss bzw. dort wo wenig Management-Awareness für die Komplexität der Herausforderungen besteht. In beiden Fällen werden hier keine externen Berater zum Projekt hinzugezogen außer in Spezialfällen, wodurch das Budget schlank gehalten werden soll. Das Budget liegt in diesen Fällen deutlich unter dem Rahmen der angeführten Studie. **Externe Dienstleistungen** können daher als **Kostentreiber** für Vorhaben zur Herstellung der EU-DSGVO-Compliance erkannt werden.

Eine Begründung für niedriges Budget kam von E2, der erklärte, dass mangelnde Management-Awareness aufgrund eines mangelnden Verständnisses hinsichtlich der Projektkomplexität eine Ursache dafür sei. Weiters sieht sich dieses Unternehmen als öffentliche Stelle nicht mit den **exorbitant hohen Strafdrohungen** konfrontiert. Als Schluss aus den Aussagen von E2 scheint das fehlende Strafausmaß sich auf die Awareness und das Commitment des Managements auszuwirken. Eine Korrelation dieser Faktoren könnte in weiterer Forschungsarbeit genauer beleuchtet und ggf. mit qualitativen Analysen überprüft werden (siehe dazu auch 5.2 Erkannte mögliche Korrelationen). Ein anderes betrachtetes Unternehmen, das an sich auch als öffentliche Stelle gilt, aber in einem Beschäftigungsbereich als Betreiber von Gesundheitseinrichtungen etwaige Strafen derzeit nicht gänzlich ausschließen kann, sieht dennoch ein der Studie nach ausreichendes Budget vor. Hier ist die Management-Awareness sowie das Commitment vorhanden.

Der Experte der für dieses Unternehmen sprach erklärte, dass bei diesem Unternehmen die Vermeidung von Nachteilen jedenfalls im Vordergrund stünde.

Interessant war, dass nur einmal erklärt wurde, dass das **Maximalprinzip** zur Anwendung kam. Das **Minimalprinzip** in seiner reinen Form zählte bei keinem interviewten Experten zu seiner praktischen Erfahrung. Wenn, dann tauschte es nur in Kombinationsform mit dem Optimalprinzip auf (E3 und E5), dort wo z.B. ein zweiteiliges Projekt vorzufinden ist, wie bei E5. In der Regel wurde dem **Optimalprinzip** gefolgt. Dem risikobasierten Ansatz wurde häufig Rechnung getragen (E1, E3, E4, E5 und E6).

5.1.4 Kategorie „Chancen“

Bei den Chancen ging es um die Generierung von zusätzlichen Vorteilen, neben der Vermeidung des Risikos. In Verbindung mit dieser Kategorie steht die folgende Subforschungsfrage:

Subforschungsfrage 4:
Liegt der Nutzen in der Herbeiführung der EU-DSGVO-Compliance nur in der Vermeidung von Nachteilen aus Datenschutzverletzungen oder erkennen die untersuchten Unternehmen weitere Chancen?

Zu dieser Kategorie konnten im Rahmen der Untersuchung, entweder theoriegestützt oder im Rahmen der qualitativen Inhaltsanalyse folgende Variablen erkannt werden:

Variablen	Entwicklung
Wissenschaft	während Analyse entdeckt
neue Drittmarktleistung	während Analyse entdeckt
Wettbewerbsfähigkeit	während Analyse entdeckt
Gesteigerter Unternehmenswert	während Analyse entdeckt
Digitalisierung	theoriegeleitet entwickelt

Tabelle 13: Variablen der Kategorie "Chancen"[236]

Die Chancen konnten dabei in ganz unterschiedlichen Bereichen erkannt werden. Zum einen wurde auf die **Vermeidung von Nachteilen** eingegangen. Diese Beantwortung der ersten Teilfrage der Frage 8 aus dem Experteninterview wird im Folgenden bei der Beleuchtung der Kategorie Nutzen (5.1.5 Kategorie „Nutzen“) näher eingegangen. Andererseits wurden auch zusätzliche erkannte Chancen genannt:

[236] Quelle: eigene Darstellung

Ein Aspekt der in der Bearbeitung der Theorie bereits betrachtet wurde und daher empirisch hinterfragt wurde, ist das Thema **Digitalisierung**. Der Gesetzgeber geht davon aus, mit der Richtlinie eine das Datenschutzniveau generell und speziell auch für Big Data und Profiling Anwendungen zu heben. Dies war auch als eine international zu betrachtende, wettbewerbsfördernde Maßnahme gesehen. Bzw. geht man davon aus, dadurch auch die Voraussetzungen für zukünftige vertrauenswürdige IT-Services vor allem im Zusammenhang mit Cloud-Diensten zu schaffen. In der Praxis sind diese Vorteile noch nicht spürbar. E1 sagt beispielsweise dazu:

„[…] worum geht's – es geht darum erhebliche wichtige Daten auch von unseren Kunden zu sammeln und auszuwerten und die EU-Datenschutz-Grundverordnung wird diese Datensammlung und -auswertung auf jeden Fall komplizierter machen."

Die neue Gesetzgebung wird hier wohl eher als Verhinderer wahrgenommen. E5 erkannte Vorteile, da er Synergien zwischen dem aktuellen EU-DSGVO-Compliance Projekt sowie einem Projekt zur Erneuerung der IT-Landschaft nutzen kann. Im Rahmen des Compliance Projekts können juristische Ressourcen parallel herangezogen werden um Fragen zur EU-DSGVO-konformen Ausgestaltung der neuen IT-Landschaft mit zu nutzen. Dies ist zwar ein positiver Nebeneffekt, erzeugt aber wahrscheinlich keinen echten wertsteigernden Beitrag für das Unternehmen. Auch E6 erkennt einen ähnlichen Effekt. Er hat sich in diesem Zusammenhang darüber Gedanken gemacht, dass die Speicherkapazitäten im Zuge der notwendigen Datenlöschung, der aufgrund der voranschreitenden Digitalisierung immer stärker zunehmenden Datenmengen im Unternehmen, reduziert werden kann. Damit können Speichermedien eingespart werden. Aber auch hier ist kein nachhaltiger Effekt erkennbar der dazu führen könnten den Wert des Unternehmens nachhaltig zu steigern.

Einen echten Vorteil im Zusammenhang mit Digitalisierung kann man aber im Bereich der **Forschung** verzeichnen. Generell erwartet man sich in diesem Bereich, der Aussage von E2 nach, verbesserte Patientenbehandlung durch Big Data Analysen. Und durch den sogenannte broad consent (zu Deutsch: breit formulierte Einwilligungserklärung[237]), kann mehr Rechtssicherheit hinsichtlich der erweiterten Forschungszwecke entstehen. Denn die Weiterverarbeitung von personenbezogenen Daten die eigentlich für andere Zwecke erhoben wurden, ist dann nicht unvereinbar mit dem ursprünglichen Zweck, wenn die Weiterverarbeitung der Forschung dient d.h. wissenschaftliche Forschungszwecke benötigt wird. Daher sollen auch allgemein gehaltene Einwilligungserklärungen im Forschungsbe-

[237] vgl Medizinische Universität Wien: 3/SN-322/ME XXV. GP - Stellungnahme zu Entwurf, https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_12276/imfname_641705.pdf, Abfragedatum 10.09.2017

reich zulässig sein, weil der Zweck der wissenschaftlichen Verarbeitung zum Zeitpunkt der Datenerhebung oft noch nicht vollständig angegeben werden kann.[238] Obwohl E2 auch in diesem Bereich eine fehlende Guidance und Unklarheiten bzgl. EU-DSGVO-Definitionen und Entwicklungen im Kontext mit Big Data zu verzeichnen sieht.

Zwei der sieben Interviewpartner (E1 und E4) erklärten, dass es auch von der Art der Branche her in der die beiden tätig sind, es sinnvoll ist das gewonnene Knowhow im Rahmen des Umsetzungsprojekts der EU-DSGVO auch mit **Beratungsdienstleistung am Drittmarkt** anzubieten. Dadurch kann ein positiver Wertbeitrag für das Unternehmen generiert werden, der in weiterer Zukunft auch dazu beitragen kann die Kosten des Projekts mit Gewinnen aus Drittmarktleistung abzudecken und somit eventuell auch einen positiven Wertbeitrag für das Unternehmen zu erzielen.

Einige Experten konnten Vorteile im Sinne der **Wettbewerbsfähigkeit** aus den Vorhaben rund um die Einführung der EU-DSGVO-Compliance ableiten. Im Bereich der Forschung zum Beispiel erkannte E2, dass ein umfangreicher wertvoller Datenbestand wie er auch über den broad consent rechtssicher generiert werden kann, dabei hilft Mittel zu generieren. Sie es durch größeres Interesse am Drittmarkt oder durch staatliche Gelder. E3 und E4 erklärten, dass eine nachweisliche EU-DSGVO-Compliance bei Ausschreibungen zukünftig durchaus entscheidend sein könne. Diese hat man bereits auch mit anderen Bereichen wie dem Informationssicherheitsmanagement gemacht. Das Vorweisen von externen Auditberichten und etwaigen Zertifikaten wird als Qualitätsmerkmal wahrgenommen und dies führt der Meinung von E4 nach auch zu einem gesteigerten Vertrauen beim Kunden. E7 erkannte Wettbewerbsvorteile, da man zukünftig auch Bewerbern vermitteln kann, dass man nicht nur die Daten der Patienten, sondern auch der Mitarbeiter und Bewerber höchstmöglich schützt und vertrauensvoll damit umgeht.

Weiters erkannte E7 eine **Steigerung des Unternehmenswertes** allgemein. Der Meinung von E7 nach wird das gesamte Unternehmen wertvoller, durch stärker sensibilisierte Mitarbeiter im Bereich Datenschutz und Informationssicherheit, die sich sicher fühlen bei der Behandlung des Patienten, weil sie klare Vorgaben haben.

[238] vgl Ennöckl, D. (2017): S.97

Interpretation

Ein paar Chancen aus der EU-DSGVO-Compliance heraus wurden in den Reihen der befragten Experten wahrgenommen. Ob man sagen kann, dass eine bahnbrechende Chance dabei war, liegt im Auge des Betrachters. Eine Euphorie hingehend neu erkannter Chancen konnte die Autorin der Arbeit bei den Interviewpartnern nicht wahrnehmen. Eher entstand der Eindruck, dass man sich diesbezüglich noch gar nicht allzu viele Gedanken gemacht hatte.

Denn in der Praxis wird die EU-DSGVO nur begrenzt als ein Förderer der Digitalisierungsthemen, vor allem im Zusammenhang mit Big Data, wahrgenommen. Unter den Interviewpartnern fand sich nur ein Experte aus der Forschung, der hier Chancen erkennen konnte. Andere Chancen wurden in neuen Möglichkeiten für Dienstleistungsangebote erkannt bzw. hinsichtlich Wettbewerbsvorteile, aufgrund von einem zusätzlichen Qualitätsmerkmal in Form von attestierten Datenschutz-Compliance im Zuge von Ausschreibungen und bei der Mitarbeitersuche. In zwei der Interviews die Aussage, dass man davon ausgehe Chancen verstärkt in einer zweiten Phase, nach einer grundlegenden Herstellung der Compliance, generieren zu können. Diese Aussage wurde aber von den beiden Experten getätigt die auch Beratungsdienstleistung am Markt anbieten.

Alle weiteren genannten Vorteile beschränkten sich auf operative unternehmensinterne Belange, wie Bereinigungen, Synergieeffekte projektübergreifender Natur, Effizienzsteigerungen und einem gesteigerten Unternehmenswert durch handlungssichere Mitarbeiter mit klaren Vorgaben.

5.1.5 Kategorie „Nutzen“

Die Kategorie Nutzen thematisiert die Frage, ob neben der Vermeidung von Risiken auch eine geplante Hebung von zusätzlichen neuen Chancen aus der EU-DSGVO heraus bei den betroffenen Unternehmen vorgesehen ist. In Verbindung mit dieser Kategorie steht die folgende Subforschungsfrage:

Subforschungsfrage 5: Wie planen die untersuchten Unternehmen den erkannten Nutzen zu realisieren und kann der erkannte Nutzen die entstehenden Aufwände decken?

Zu dieser Kategorie konnten im Rahmen der Untersuchung, entweder theoriegestützt oder im Rahmen der qualitativen Inhaltsanalyse folgende Variablen erkannt werden:

Variablen	Entwicklung
Risikovermeidung	theoriegeleitet entwickelt
Realisierung von weiteren Chancen	theoriegeleitet entwickelt

Tabelle 14: Variablen der Kategorie "Nutzen"[239]

In erster Linie wird das Thema **„Vermeidung von Nachteilen“** von den Unternehmen für welche die Interviewpartner sprachen, forciert. E4 sagt dazu im Interview:

„Ich denke wir sind ganz klar bei der Vermeidung von Nachteilen. […] die gesetzliche Komponente gesetzeskonform unterwegs zu sein steht in dem Projekt ganz ganz klar im Vordergrund. Wird auch so im ganzen Haus eigentlich grundsätzlich gesehen.“

Und weiters sorgt man sich um das Thema des Imageverlusts, das E3 wie folgt erklärt:

„[…] und bei großen Unternehmen ist es dann natürlich auch der Imageschaden, der vermieden werden muss und … Verlust von Kunden, Anfalles und […] Markenwertverlust auch […]“

Das wird auch bei E2 als zentrales Ziel gesehen, da die öffentliche Stelle nicht in dem Umfang von Strafausmaßen betroffen ist. Aber bei Reputationsverlust ist nicht ausschließbar, dass z.B. Drittmittel-finanzierte Forschungen ausbleiben. E6 sieht zudem die Gefahr, dass Patienten ausbleiben würden bzw. nicht ausschließbare Konsequenzen für die Führungsebene eintreten könnten, auch wenn er ggf. nicht existenzbedrohend für das Unternehmen wäre.

Die **Generierung von Nutzen aus den weiteren erkannten Chancen** wurde, wenngleich einige Chancen erkannt wurden (5.1.4 Kategorie „Chancen“), von den Unternehmen für die die Interviewpartner sprachen bisher noch wenig betrachtet. E1 erklärte, dies sei erst in einem zweiten Schritt geplant. Dann würde man sich, wie bereits im Kapitel 5.1.4 Kategorie „Chancen“ erwähnt, um Dienstleistungsprojekte am Drittmarkt bemühen, um das gewonnene Knowhow aus dem EU-DSGVO-Compliance Projekt gewinnbringend zu verwerten.

Von den anderen Experten wurden eher Vorteile im Rahmen der Projektdurchführung erkannt wie, Synergieeffekte (E5: Modernisierung IT-Infrastruktur und juristische Absicherung der Neuerungen über das EU-DSGVO Projekt; E7: Angedachtes Nachfolgeprojekt zur Einführung eines ISMS mit vielen Synergien), Effizienzerhöhung im Risikomanage-

[239] Quelle: eigene Darstellung

ment (E5) und die Notwendigkeit zur Abarbeitung lästig überfälliger, wenig beliebter Aufgaben (E6).

Interpretation

Als zu generierender Nutzen überwiegt die Kategorie „Vermeidung von Nachteilen“ und dies in erster Linie aus der Vermeidung der sehr hohen Strafandrohungen heraus, aber auch ein denkbarer Imageschaden ist gefürchtet. Die gennannte Effizienzsteigerungen durch das Vorhaben zur EU-DSGVO-Compliance helfen zwar das Projekt langfristig positiv im Unternehmen zu platzieren, generieren aber keinen Umsatz.

Die Frage nach der Deckung der Kosten durch den erkannten Nutzen, kann positive bejahend mit Blick auf die Vermeidung von, in aller ersten Linie, exorbitant hohen Strafen, aber auch Reputationsschäden beantwortet werden. Darauf wird im Folgenden auch nochmals detaillierter eingegangen:

5.1.6 Kategorie „Wirtschaftlichkeit“

Über die Kategorie Wirtschaftlichkeit soll ermittelt werden ob ein monetärer Nutzen entsteht und ob in der Praxis Kosten-Nutzen-Analysen durchgeführt werden. In Verbindung mit dieser Kategorie steht die folgende Subforschungsfrage:

Subforschungsfrage 6:
Versuchen die untersuchten Unternehmen einen wirtschaftlichen Mehrwert dabei zu generieren, sollen rein die Kosten gedeckt werden oder wird dies nicht betrachtet?

Zu dieser Kategorie konnten im Rahmen der Untersuchung, entweder theoriegestützt oder im Rahmen der qualitativen Inhaltsanalyse folgende Variablen erkannt werden:

Variablen	Entwicklung
monetäre Nutzenbewertung	theoriegeleitet entwickelt
Kosten-Nutzen-Analyse	theoriegeleitet entwickelt

Tabelle 15: Variablen der Kategorie "Wirtschaftlichkeit"[240]

Keiner der Interviewpartner gab an, dass der erkannte Nutzen im jeweiligen Unternehmen monetär bewertet wurde. Nicht alle Interviewpartner machten dazu eine Aussage, aber fünf von sieben Experten bestätigten, dass **keine monetäre Nutzenbewertung** durchgeführt wurde. Auch diejenigen die Marktchancen erkennen, bewerten diese nicht monetär. Auch im Bereich der Forschung und der dort identifizierten Zukunftschancen hinsichtlich

[240] Quelle: eigene Darstellung

Big Data gab es keine bisherigen Überlegungen zu monetären Nutzenbewertungen. Einzig E6 erklärte, dass das Risikomanagement zurzeit zwar nicht monetär bewertet wird, es aber den Wunsch seitens Vorstand dazu gibt.

Aber der denkbare Schaden im Sinne einer etwaigen **Strafe wird monetär bewertet**. D.h. es wurde in manchen Interviews erklärt, dass man Überlegungen anstellt „wie viel Sicherheit“ man nicht um das Eintreten einer möglichen Strafe erhalten würde, wie E6 im Folgenden ausführt:

„[…] da ist dann der Vergleich zwischen einigen € 100.000, -- an Investition und riesigen Schadensandrohungen... da muss man dann schauen, dass man nicht den Bezug zur Realität verliert... man muss die Kirche schon im Dorf lassen... wie ich am Anfang schon erwähnt habe, ich glaube nicht dass uns eine 20 Millionen € Strafe droht. Es wird halt um den Faktor 1000 höher werden, wahrscheinlich ... jetzt waren die Strafen bei € 500, -- ca. bei Datenschutzvergehen wo sich niemand wirklich darum gekümmert hat, weil da wären die Maßnahmen in jedem Fall teurer gewesen. In Zukunft ist es dann so, dass es eine halbe Million ist und da geht sich schon einiges aus. […] Um dieses Geld bekommt man dann schon einige technische Mittel ... wo man vielleicht das Risiko minimieren kann.“

Bei keinem Unternehmen für welches die Interviewpartner sprachen wurde eine explizite Wirtschaftlichkeitsbetrachtung im Sinne einer **Kosten-Nutzen-Analyse durchgeführt**.
E3 erklärte, dass bei ihren Klienten die Herstellung der EU-DSGVO-Compliance in der Regel eher als „mühseliges Vorhaben“ mit Fokus auf Vermeidung der Schäden gesehen wird und hier in der Regel kein Gedanke an einen positiven Wertbeitrag entsteht.
E4 und E6 sind der Meinung, dass die Kosten durch den Nutzen jedenfalls gerechtfertigt werden würden. E4 erklärte, dass für ihn der positive Wertbeitrag durch die Vermeidung der großen, vor allem auch immateriellen Risiken klar außer Frage steht. E6 sah auch, dass sich die Kosten unter Berücksichtigung der Strafen rechnen. Wenngleich er darauf hinwies, dass die Wahrscheinlichkeit des tatsächlichen Eintretens einer 20 Mio. Euro Strafe mitberücksichtigt werden muss. Formal wird dies im Unternehmen des E6 aber noch nicht gemacht. E7 erklärte, dass all diese Überlegungen im ersten Schritt außer Frage standen, wesentlich ist es für das Unternehmen den Schaden zu vermeiden.

Interpretation

Eine monetäre Nutzenbewertung wird in der Regel nicht durchgeführt. Nur der vermeidbare Schaden wird monetär beziffert, sofern es um Strafen geht. Eine Gegenüberstellung der

Kosten vs. dem Nutzen erfolgt daher wenn, dann nur im Sinn der Gegenüberstellung denkbarer Strafen zu notwendigen Investitionen.

Hierbei muss man aber auch eine Eintrittswahrscheinlichkeit für das Entstehen einer sehr hohen Strafdrohung mitberücksichtigen. Es liegt auf der Hand, dass vor allem bei Unternehmen wie den betrachteten, nicht zwangsläufig immer die Höchststrafe anfallen würde, vor allem weil sich diese Unternehmen durch ihre Projekte bereits vor grober Fahrlässigkeit zu schützen versuchen. Dennoch ist ungewiss mit wie vielen Anfragen der Betroffenen zukünftig zu rechnen sein wird und wie hart in Zukunft gestraft wird.

5.2 Erkannte mögliche Korrelationen

Im Folgenden werden aus den Ergebnissen der Experteninterviews weitere Schlussfolgerungen gezogen. Dabei ergaben sich an einigen Stellen neue Hypothesen, die in weiterführender Forschung genutzt und überprüft werden könnten.

5.2.1 Korrelation Management-Awareness und Management-Commitment

Hypothese 1:

Wenn in Unternehmen nicht die notwendige Management-Awareness zu einem Vorhaben geschaffen wird, dann führt dies zu mangelhaftem Management-Commitment, was inkludiert, dass ein Projekt nicht ausreichend mit den benötigten Ressourcen ausgestattet wird.

Im Rahmen der Interviews wurde nahezu bei allen Interviewpartnern vorhandenes Management-Commitment als auch Management-Awareness angeführt. Nur beim Experten E2 war ein grundsätzliches Commitment zwar gegeben, aber der Experte gab eine mangelnde Awareness des Managements vor allem hinsichtlich der Komplexität des Vorhabens an. Ein einziger Fall lässt natürlich noch keine Hypothese bestätigen. Daher würde diese Thematik eine spannende Frage für eine weitere Forschungsarbeit darstellen, ggf. in Kombination mit der nächsten vermuteten Korrelation:

5.2.2 Korrelation Strafausmaß und Commitment

Hypothese 2:

Wenn das Strafausmaß in einer exorbitanten Höhe vorgesehen ist, dann ist ein Commitment sowohl beim Management als auch auf anderen Unternehmensebenen für ein Compliance-Vorhaben leichter zu generieren.

Oder anders gesagt, es ergab sich im Zuge der Analysen das Bild, dass die betroffenen Unternehmen EU-DSGVO Projekte in erster Linie zur Vermeidung von Strafen umsetzen. Und zwar nicht wegen einfachen Verwaltungsstrafen in vergleichsweise niedriger Höhe von wenigen zehntausend Euros, sondern aufgrund der exorbitant hohen Strafen, mit denen die EU-DSGVO droht und die in Österreich für nicht öffentliche Stellen gelten. Weiters wird die Hypothese dadurch gestützt, dass ein Interviewpartner (E2) zu einem Unternehmen einer öffentlichen Stelle berichtete und dort auch anführte, dass aufgrund mangelnden Management-Commitment auch nur wenig Ressourcen zur Verfügung gestellt wurden. Es wäre interessant zu in einer weiterführenden Untersuchung an öffentlichen Stellen zu hinterfragen, ob rein die monetäre Strafe oder auch andere Faktoren, wie z.B. der Imageschaden als Treiber wirken bzw. wie stark der jeweilige Faktor als Treiber zur Generierung von Management-Commitment wirken kann.

6. Fazit

Aus der Analyse der Sub-Forschungsfragen ergab sich das im folgenden beschriebene Bild, sowie die persönliche Meinung der Autorin, Erkenntnisse über den Beitrag der Arbeit und weitere Fragestellungen deren Beantwortung über weiterführende Forschungsarbeiten spannend erscheinen.

6.1 Zusammenfassung

Die Antwort auf die Forschungsfrage "**Welchen Herausforderungen und Chancen begegnen österreichische Verantwortliche und Auftragsverarbeiter im Sinne des Art. 4 EU-DSGVO in der stationären Krankenversorgung bei der Herbeiführung der EU-DSGVO-Compliance bis zum 25. Mai 2018 und wie werden die damit verbundenen Kosten und Nutzen im Sinne des Wirtschaftlichkeitsprinzips gegenübergestellt?"** fällt daher wie folgt aus:

Alle interviewten Experten von betroffenen Unternehmen befinden sich aktuell in einem Analyse-, Umsetzungs- oder Anpassungsvorhaben zur Erreichung der EU-DSGVO-Compliance. Wobei sich ein überwiegender Teil der betroffenen Unternehmen (4 von 7) in einer noch sehr frühen Phase des Vorhabens befindet. Generell ist der „Tone from the Top“, eines der wichtigsten Voraussetzungen um ein jedes Projekt dieser Größenordnung in einem Unternehmen erfolgreich umzusetzen, in der Regel gegeben. Die Begründung scheint vor allem im hohen drohenden Strafausmaß zu liegen und diese Erklärung hilft auch dabei das Commitment weiterer Unternehmensebenen zu gewinnen.

Auch wenn tatkräftig an Vorhaben zu diesem Thema gearbeitet wird, so gibt es doch viel Ungewissheit und folglich Unsicherheiten. Zentrale Vorgaben und klare Handlungsempfehlungen fehlen den Unternehmen. Dies geht so weit, dass Projektziele bei vielen vom Interview betroffenen Unternehmen nicht klar formuliert wurden. In der Regel ist der erwartete Output des Vorhabens klar, aber ein Beurteilung des Outcomes im Sinne der Wirksamkeit der Maßnahmen ist nicht möglich. Folglich herrscht eine unklare Situation, wann die Ziele tatsächlich erreicht sind bzw. wie man den Nachweis dafür erbringen kann.

Viele Herausforderungen sowohl im technischen als auch organisatorischen Themenbereichen wurden genannt. Experten mit viel Projektexpertise adressierten dabei bereits andere Herausforderungen, als Experten in frühen Phasen der Compliance-Vorhaben. Es ist

naheliegend anzunehmen, dass die zweite Gruppe noch gar nicht mit allen Herausforderungen des Projekts vertraut ist. Nahezu alle Experten sind sich aber einig (5 von 7), dass die technische Umsetzung des Recht auf Vergessenwerden eine besondere Herausforderung darstellen wird. Auch hier liegt der Grund wieder in einer Ermangelung an detaillierten gesetzlichen Regelungen, Vorgaben und Handlungsempfehlungen seitens Gesetzgeber bzw. Behörde.
Weiters scheint allen noch eines klar zu sein: Es liegt viel Arbeit in knapper Zeit vor ihnen, da gerade im Gesundheitswesen eine Menge an Daten verarbeitet werden die einer detaillierten und nachweislich dokumentierten Betrachtung zu unterziehen sind und damit auch viele organisatorische Vorkehrung zu treffen sind. Kaum einer ist der Auffassung mit 25.05.2018 alle Arbeiten endgültig abgeschlossen zu haben, zumindest Evaluierungs- und Nacharbeitsphasen sind angedacht.

Die anberaumten Budgets lagen bei fünf von sieben Interviewpartnern in einem Rahmen von € 95.000, -- und € 445.000, --, was aufgrund der Tatsache des stetigen Kostendrucks im Gesundheitswesen doch sehr erstaunlich ist und wieder auf den Zusammenhang zwischen Strafausmaß und Management-Commitment hindeutet. Bei der Ermittlung der Budgets wurde überwiegend ein risikobasierter Ansatz entsprechend des Optimumprinzips angewandt.

Von neu erkannten, bahnbrechenden Chancen im Zusammenhang mit dem EU-DSGVO Vorhaben konnten die interviewten Praktiker nicht berichten. Im Bereich der Forschung, in Zusammenhang mit Big Data, könnten sich positive Entwicklungen ergeben. Und die Experten die für Unternehmen im Gesundheitswesen tätig sind, die auch Beratungsdienstleistung am Drittmarkt anbieten, sehen neues Beratungs- und Umsatzpotential darin ihr gewonnenes EU-DSGVO-Wissen am Markt zu vertreiben. Ansonsten rechnet man durch eine nachweislich hergestellte Compliance mit besseren Chancen in Ausschreibungen, oder am Bewerbermarkt und mit Effizienz im Unternehmen.

Folglich hält sich auch die Euphorie über den erkannten Nutzen aus neuen Chancen im Zaum. Treiber für die Umsetzungsprojekte ist klar der Nutzen aus der Vermeidung von Nachteilen, wie exorbitant hohen Strafen oder drohendem Imageverlust. In den Interviews wurde auch angesprochen, dass man davon ausgeht zukünftig etwaigen weiteren Nutzen in einem zweiten Schritt zu generieren. Aktuell fokussiert man sich aber auf die Herstellung der EU-DSGVO-Compliance um Nachteile zu vermeiden.

Eine monetäre Nutzenbewertung fehlt in der Regel, außer einer Bewertung etwaiger anfallender Strafen. In diesem Fall müsste man formal korrekt dann aber auch Eintrittswahrscheinlichkeiten hinsichtlich des Risikos bedenken. Aber, auch hinsichtlich dieser Überlegungen zur Rechtfertigung der entstehenden Kosten durch etwaige Strafandrohungen, wird in den interviewten Unternehmen kein „Business Case“ gerechnet, viel eher wird hier maximal eine Art „Milchmädchenrechnung“ angestellt.

Im Kapitel 3.3 Chancen und Nutzen haben wir uns mit den Erwartungen des Gesetzgebers hinsichtlich des Nutzens aus der EU-DSGVO beschäftigt. Zum einen wurde hier erhoffte Einsparungen für die Wirtschaft im Ausmaß von 2,3 Billionen Euro sowie einheitliche Rechtsdurchsetzung genannt. Bei den Praktikern aus dem Gesundheitswesen ist dieser Nutzen aus der EU-DSGVO-Compliance wohl noch nicht greifbar. Derzeit entstehen hohe Kosten zur Herstellung der Compliance und ein bahnbrechender zusätzlicher Nutzen konnte im ersten Schritt von keinem der Experten genannt werden. Die einheitliche Rechtsdurchsetzung wird sich in der Zukunft weisen, aber bis dahin kämpfen Unternehmen mit Rechtsunsicherheit. Dies wurde sowohl im Bereich international agierender Unternehmen genannt (E1), die mit unterschiedlichen Datenschutz-Anpassungsgesetzen in den einzelnen EU-Mitgliedstaaten konfrontiert sind, so wie in allen Unternehmen, die auf mangelnde Umsetzungsunterstützung z.B. in Form von Guidelines seitens der Behörden warten.

6.2 Ausblick und persönliche Meinung

Wenn am Ende des Tages die Erkenntnis bleibt, dass neue Chancen und zusätzlicher Nutzen aus der EU-DSGVO-Compliance recht eingeschränkt erkennbar sind und auch ein positiver Wertbeitrag daraus - zumindest in dieser ersten Phase der Compliance-Einführung – im Gesundheitswesen kaum wahrgenommen werden kann, dann muss man sich mit der Feststellung, die Meyer in seinem Fachbeitrag stellt auseinandersetzen[241]:

"Ob ein derartiges Bedrohungsszenario durch einen extrem hohen Bußgeldrahmen im Sinne des Patienten ist, darüber lässt sich trefflich streiten!"

Denn durch die hohen drohenden Strafen und notwendigen Umsetzungsprojekte zu ihrer Vermeidung, fehlen diese Budgets zukünftig womöglich in der Finanzierung eines komple-

[241] Meyer, S. (2017, S.29

xen stationären Versorgungsprozesses im Körpersektor bzw. einer Daseins-Vorsorgeeinrichtung. Dieser Versorgungsprozess sollte aber gerade den Patienten zugutekommen und da nicht davon auszugehen ist, dass mehr Geld zur Verfügung stehen wird kann man so argumentieren, dass die EU-DSGVO-Umsetzungsprojekte in der stationären Krankenversorgung zu Lasten der Patientenversorgung gehen[242].
Die Fragestellung dieser Arbeit war kurzgefasst „Wie wirtschaftlich ist die EU-DSGVO-Compliance im Gesundheitswesen umsetzbar?“. Auf Basis der Ergebnisse der Arbeit schließt sich der Autorin hier eine kritische neue Frage an „Wie viel mehr Compliance im Gesundheitswesen ist denn überhaupt noch vertretbar?“. Leider würde eine wissenschaftlich fundierte Beantwortung dieser Frage wohl den Rahmen dieser Arbeit sprengen.

Anderseits wurde aufgrund der vorgenommenen Beobachtungen bereits die Hypothese aufgestellt, dass es ohne die derart hohe Strafdrohung zu keinem ausreichenden Management-Commitment kommen würde (siehe Hypothese 2), um Projekte dieser Art umzusetzen. Wenn dies recht behält, dann ist dies notwendig um einen Change in Bereich Datenschutz, aber auch -sicherheit erst überhaupt herbeiführen zu können. Und es braucht nicht die zitierte Studie die bestätigt, dass das Gesundheitswesen im Bereich der Datensicherheit hinterherhinkt. Es genügt die Zeitung aufzuschlagen und von Malware-Attacken zu lesen, die Krankenhausbetriebe lahmlegen. Dass hier genauso ein Schaden am Patienten entstehen kann, weil dieser z.B. aufgrund eines ausgefallenen Computersystems keine Operation erhalten kann, liegt auf der Hand.

Meine persönliche Meinung ist, dass durch die EU-DSGVO langfristig gesehen, über den Druck der Verantwortlichen auf die Dienstleister, datenschutzrechtlich sicherere Anwendungen entstehen bzw. angeboten werden. Davon bzw. durch das Konzept Datenschutz durch Technikgestaltung, wird jedenfalls auch der Bereich der Datensicherheit profitieren. Damit sind Anwendungsfelder wie Cloud-Computing, Big Data und Profiling nachhaltig reguliert und vertrauenswürdiger. Wir profitieren somit alle in Zukunft von sichereren Anwendungen. Und das hilft auch dem Patienten im Gesundheitswesen. Es gibt bereits jetzt eine Vielzahl an Anwendungsfällen bei denen man den Patienten z.B. über Tele-Rehabilitationsprogramme via Smartphone-App und Cloud Service nachhaltig besser therapieren könnte, weil man seine Behandlungsfortschritte durch das Tragen von Wearables und über das ortsungebundene und zeitlich unmittelbare zur Verfügung stellen von Daten daraus besser nachverfolgen kann. Heute fehlt oft noch das Vertrauen in diese neuen

[242] vgl Meyer, S. (2017), S.29

Technologien, der Meinung der Autorin nach auch zurecht. Aber die EU-DSGVO kann dazu beitragen hier für mehr Sicherheit zu sorgen.

6.3 Beitrag der Arbeit und mögliche weiterführende Forschungen

Die Autorin dieser Arbeit hofft, durch die Aufarbeitung der Theorie und die empirischen Studien einen Beitrag zur Beleuchtung der Praxis, hinsichtlich der Auswirkungen der Herbeiführung der EU-DSGVO-Compliance auf das Gesundheitswesen, eingeschränkt auf den stationären Bereich, gegeben zu haben. Die Erkenntnisse könnten dazu genutzt werden die Frage zu stellen, warum die Intention des Gesetzgebers derzeit nicht die gezeigte Praxis trifft und was dagegen getan werden kann. Bzw. führen der Ergebnisse der Arbeit dazu zu hinterfragen, ob denn die Sinnhaftigkeit aller Vorgaben auch für das stationäre Gesundheitswesen gegeben ist.

Zu den beiden Hypothesen, Hypothese 1 zu „Korrelation Management-Awareness und Management-Commitment“ und Hypothese 2 zu „Korrelation Strafausmaß und Commitment“ die diese Arbeit generiert hat, wäre es interessant eine Überprüfung in einer weiterführenden Forschungsarbeit mit quantitativen empirischen Methoden durchzuführen.

Weiters wäre es auch spannend mit den interviewten sieben Experten nach dem 25. Mai 2018 nochmals ein Interview zur Nachbetrachtung der Vorhaben zur Herbeiführung der EU-DSGVO-Compliance durchzuführen, um zu sehen wie es ihnen am weiteren Weg erging und ob die Auswertung der Faktoren für eine erfolgreiche Compliance-Einführung recht behielt.

7. Literatur

7.1 Selbstständige Werke

Atteslander, P. (2006): Methoden der empirischen Sozialforschung, 11. Aufl, Berlin, Erich Schmidt Verlag.

Dierlamm, J. (2011): IT Governance und IT Compliance – die wichtigsten Normen und Regelwerke, Köln, TÜV Media.

Feiler, L., Forgó, N. (2017): EU-DSGVO: EU-Datenschutz-Grundverordnung, Wien, Verlag Österreich.

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

Kaltenböck, M., & Thurner, T. (2011). Open Government Data Weissbuch. Wien: Edition Donau-Universität Krems.

Klotz, M. (2009): IT-Compliance: Ein Überblick, Heidelberg, dpunkt.verlag.

Mankiw, N. G., Taylor M. P. (2012): Grundzüge der Volkswirtschaftslehre, 5. Aufl, Stuttgart, Schäffer-Poeschler Verlag.

Mayring, P. (2015): Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12. Aufl, Weinheim und Base, Beltz.

Pachinger, M. M., Beham, G. (Hrsg) (2016): Datenschutz-Audit: Recht - Organisation - Prozess – IT: Der Praxisleitfaden zur Datenschutz-Grundverordnung, Wien, LexisNexis.

Piekenbrock, D., Henning, A. (2013): Einführung in die Volkswirtschaftslehre und Mikroökonomie, 2. Aufl, Berlin Heidelberg, Springer-Verlag.

Pollirer, H.-J., Weiss, E., Knyrim, R., Haidinger, V. (Hrsg) (2017): DSGVO: Datenschutz-Grundverordnung, Wien, Manz.

Rath, M., Sponholz, R. (2014): IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen, 2. Aufl, Berlin, Erich Schmidt Verlag

Stockinger, G. (2013): Potentiale von Open Government Data im österreichischen Gesundheitswesen am Beispiel der Kinder- und Jugendgesundheit, Krems, FH Krems, Master‘s Thesis.

7.2 Beiträgen in Sammel- und Nachschlagewerken

Bergauer, C. (2016): Personenbezogene Daten: Begriff und Kategorien, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Bogendorfer, R.J. (2016): Der Dienstleister wird zum Auftragsverarbeiter: Und was ändert sich für Dienstleister mit der DSGVO noch?, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Haidinger, V. (2016): Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Art 15-21 DSGVO), in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Hötzendorfer, W. (2016): Privacy by Design and by Default: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Hldjk, J. (2016): Sachlicher und räumlicher Anwendungsbereich der DSGVO, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Horn, B. (2016): Gemeinsam für die Verarbeitung Verantwortliche, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Illibauer, U. (2016): Geldbußen und andere Sanktionen, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Kastelitz, M. (2016): Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 5-11 DSGVO), in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Klotz, M., Dorn, D.-W. (2008): IT-Compliance – Begriff, Umfang und relevante Regelwerke, In: HMD – Praxis der Wirtschaftsinformatik, 2008, Jg. 45, Heft 263, S. 5-14.

König, G. (2016): Der Datenschutzbeauftragte: Die interne Beratungs- und Kontrollfunktion, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Krisch, A. (2016): DSGVO: Chancen und Risiken für die IT-Wirtschaft, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Mühlenkamp, H. (2011): Wirtschaftlichkeit und Wirtschaftlichkeitsuntersuchungen im öffentlichen Sektor, Speyer Arbeitsheft Nr. 2014 der Deutschen Hochschule für Verwaltungswissenschaften Speyer 2011, Berlin, Speyer.

Oman, M. (2016): Daten weg – was nun? Data Breaches und ihre DSGVO-Folgen gem Art 33,34 DSGVO, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Pollirer, H.-J. (2016): Sicherheit der Verarbeitung (Art 32 DSGVO), in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Selk, R. (2016): Verzeichnis von Verarbeitungstätigkeiten (Art 30 DSGVO): Wer muss es haben, wie hat es auszusehen?, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Steinmaurer, K. M. (2016): Big Data und Profiling: Chancen und Risiken in der Datenschutz-Grundverordnung, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

Trieb, G. (2016): Datenschutz-Folgeabschätzung und vorherige Konsultation der Aufsichtsbehörde: Von der Registrierungspflicht zur weitgehenden Selbstregulierung, in Knyrim, R. (Hrsg): Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien, Manz.

7.3 Aufsätze in Zeitschriften

Böhm, M. (2008): IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT, In: HMD – Praxis der Wirtschaftsinformatik, 2008, Jg. 45, Heft 263, S.15-29

Ennöckl, D. (2017): Die Verarbeitung von personenbezogenen Gesundheitsdaten nach der DSGVO, Heft 3/2017, Manz, S.88ff

Kastelitz, M. (2016a): Die Datenschutz-Grundverordnung im Gesundheitsbereich – ein erster Überblick, JMG 0-2016, S.71ff

Meyer, S. (2017): Datenschutz-Grundverordnung - eine sinnvolle Herausforderung oder Provokation für Kliniken und Krankenhäuser, BvD-News Ausgabe 2/2017, Berlin, S.27ff

Pollirer, H-J. (2015): Die Datenschutz-Grundverordnung: Der Datenschutzbeauftragte (Teil II), Dako 2015/37 Heft 3/2015, S.65ff

Pollirer, H-J. (2015a): Die Datenschutz-Grundverordnung: Die Datenschutz-Folgenabschätzung (Teil III), Dako 2015/47 Heft 4/2015, S.88ff

Rüpin, S. (2015): Big Data in Medizin und Gesundheitswesen, Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz, Volume 58, Issue 8, S. 794-798

Wagner, B. (2015): Die Datenschutz-Grundverordnung: die Betroffenenrechte (Teil IV), Dako 2015/59 Heft 5/2015, S.112ff

7.4 Internet-Quellen

Bücking, J. (2014): Datenschutz, Datensicherheit und Compliance am Beispiel Islands, https://files.vogel.de/vogelonline/vogelonline/files/8058.pdf, Abfragedatum 05.07.2017

Döring, S., Heintz, L. (2012): Compliance im Gesundheitswesen: Krankenhäuser stärker im Blick, http://www.pwc.de/de/gesundheitswesen-und-pharma/compliance-im-gesundheitswesen-krankenhaeuser-staerker-im-blick.html, Abfragedatum 14.07.2017

Dr. Datenschutz (2017): Sachlicher Anwendungsbereich: Die DSGVO gilt, wenn ..., https://www.datenschutzbeauftragter-info.de/sachlicher-anwendungsbereich-die-dsgvo-gilt-wenn/, Abfragedatum 30.05.2017

DSB (2017): Meldung beim Datenverarbeitungsregister, https://www.dsb.gv.at/meldung-beim-dvr, Abfragedatum 20.08.2017

European Central Bank, 2004, Annual Report: 2004, ECB, Frankfurt, Glossary. https://www.ecb.europa.eu/pub/pdf/annrep/ar2004en.pdf?4cc01c9b5ba4f31492c002bd7b5c954e, Abfragedatum 04.07.2017

EY (2016): Bereit für die EU-Datenschutzgrundverordnung? Studie zum Reifegrad von Datenschutzmanagementsystemen in Unternehmen, http://www.ey.com/Publication/vwLUAssets/ey-bereit-fuer-die-eu-datenschutzgrundverordnung/$FILE/ey-bereit-fuer-die-eu-datenschutzgrundverordnung.pdf, Abfragedatum 30.07.2017

FMA (2011): Rundschreiben zum risikoorientierten Ansatz zur Prävention von Geldwäscherei und Terrorismusfinanzierung, https://www.fma.gv.at/download.php?d=82, Abfragedatum 07.08.2017

Medizinische Universität Wien: 3/SN-322/ME XXV. GP - Stellungnahme zu Entwurf, https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_12276/imfname_641705.pdf, Abfragedatum 10.09.2017

Gabler Wirtschaftslexikon (2017), Stichwort: Gesundheitswesen, http://wirtschaftslexikon.gabler.de/Archiv/55801/gesundheitswesen-v9.html, Springer Gabler Verlag (Hrsg), Abfragedatum 30.06.2017

Gabler Wirtschaftslexikon (2017a), Stichwort: Digitalisierung, http://wirtschaftslexikon.gabler.de/Archiv/-2046143105/digitalisierung-v3.html, Springer Gabler Verlag (Hrsg), Abfragedatum 16.08.2017

Gabler Wirtschaftslexikon (2017b), Stichwort: Big Data, http://wirtschaftslexikon.gabler.de/Archiv/-2046774198/big-data-v4.html, Springer Gabler Verlag (Hrsg), Abfragedatum 16.08.2017

Gabler Wirtschaftslexikon (2017c): Wirtschaftlichkeitsprinzip, http://wirtschaftslexikon.gabler.de/Definition/wirtschaftlichkeitsprinzip.html, Abfragedatum 21.05.2017

Ittensohn, D. (2013): Compliance im Gesundheitswesen: "Wandel von der Schuldkultur über die Fehlerkultur zur Sicherheitskultur", eHealth Summit 2013, https://www.eiseverywhere.com/file_uploads/6694b88b292804fcea7a871a0fa437fe_Ittensohn_ComplianceimGesundheitswesen.pdf, Abfragedatum 14.07.2017

Knyrim, R., Trieb, G. (2014): Das künftige EU-Datenschutzrecht / Neue Anforderungen an die unternehmerische Compliance, http://www.preslmayr.at/tl_files/Publikationen/2014/Das%20kuenftige%20EU-Datenschutzrecht%20-%20Neue%20Anforderungen%20an%20die%20unternehmerische%20Compliance_Knyrim_Trieb.pdf, Abfragedatum 05.02.2017

KPMG (2015): Health Care and Cyber Security: Increasing Threats Require Increased Capabilities, https://www.kpmg-institutes.com/content/dam/kpmg/healthcarelifesciencesinstitute/pdf/2015/cyber-healthcare-survey.pdf, Abfragedatum 17.07.2017

Öffentliches Gesundheitsportal Österreich (2017): Gesundheitswesen, https://www.gesundheit.gv.at/gesundheitssystem/gesundheitswesen/inhalt, Abfragedatum 17.07.2017

Öffentliches Gesundheitsportal Österreich (2017a): Das Gesundheitswesen im Überblick, https://www.gesundheit.gv.at/gesundheitssystem/gesundheitswesen/gesundheitssystem, Abfragedatum 17.07.2017

Palmethofer, W., Semsrot, A., Alberts, A. (2017): Der Wert persönlicher Daten: Ist Datenhandel der bessere Datenschutz? Sachverständigenrat für Verbraucherfragen, http://www.svr-verbraucherfragen.de/wp-content/uploads/Open_Knowledge_Foundation_Studie.pdf, Abfragedatum 14.08.2017

TRUSTe Inc (2015): Research Report: Preparing fort h EU General Data Protection Regulation: Assessing Awareness, Readiness & Impact of the Proposed Changes in US, UK, France & Germany, https://info.trustarc.com/Web-Resource-GDPR-Research-Report_LP.html, Abfragedatum 14.08.2017

Quality Austria (2015): ISO 9001 Revision einfach erklärt – Konzept des "risikobasierten Denkens", http://www.qualityaustria.com/index.php?id=5085, Abfragedatum 07.08.2017

Schmalzer, T., ua: Die dritte Säule im Österreichischen Gesundheitssystem: Eine Studie für den Raum Graz am Beispiel des Ärzte-Center Graz, http://wko.at/wien/drittesauele.pdf, Abfragedatum 17.07.2017

Spyra, G. (2016): Die EU-DSGVO: Alter Wein in neuen Schläuchen?, Vortrag auf der 16. Conhit, https://gmds.de/fileadmin/user_upload/Aktivitaeten_Themen/Medizinische_Informatik/dgi/workshops/20160418/02-04_spyra_20160418.pdf, Abfragedatum 20.08.2017

Standard: Wundersame Welt der "-omics" vom 12. September 2004, http://derstandard.at/1783795/Wundersame-Welt-der--omics, Abfragedatum 16.08.2017

Weill, P., Woodham, R. (2002): Don't Just Lead, Govern: Implementing Effective IT Governance (April 2002). MIT Sloan Working Paper No. 4237-02. https://ssrn.com/abstract=317319 or http://dx.doi.org/10.2139/ssrn.317319, Abfragedatum 17.07.2017

Wirtschaftskammer Österreich (2017): EU-Datenschutz-Grundverordnung, Kurzüberblick und Zeitplan, https://www.wko.at/Content.Node/Service/Wirtschaftsrecht-und-Gewerberecht/Verwaltungs--und-Verfassungsrecht/Datenschutz/EU-Datenschutz-Grundverordnung.html, Abfragedatum 05.02.2017

7.5 Rechtsquellen

VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 2016/119