FERDINAND PORSCHE
FERN FH

Voraussetzungen für den Einsatz von Public Cloud Lösungen in den Kernprozessen der Versicherungsbranche

Masterarbeit

eingereicht von: **Markus Zimmer, BA**
Matrikelnummer: 51807208

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH GmbH

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Dipl.-Ing. Thomas Györgyfalvay, BA, MBA

Zweitgutachten: Thomas Krabina, MSc

Wiener Neustadt, Mai 2019

Ehrenwörtliche Erklärung

Ich versichere hiermit,

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

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

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

Wr. Neustadt, Mai, 2019 _____

Unterschrift

Kurzzusammenfassung: Voraussetzungen für den Einsatz von Public Cloud Lösungen in den Kernprozessen der Versicherungsbranche

Die hohen IT Kosten in den Versicherungsunternehmen zwingen diese, Alternativen zu den im Moment angewandten Techniken zu suchen. Eine davon ist die Umsetzung ihrer Kernprozesse mittels Public Cloud Umgebungen. Es sind vor allem die Flexibilität, die Skalierbarkeit und die Kosten ein treibender Faktor. Um dies allerdings umsetzen zu können, gibt es einige gesetzliche Vorschriften wie die Datenschutzgrundverordnung zu beachten.

In dieser Arbeit soll nun untersucht werden, welche technischen und organisatorischen Maßnahmen nun notwendig sind, um die Versicherungskernprozesse unter Einhaltung der Datenschutzgrundverordnung in Public Cloud Lösungen umsetzen zu können.

Dazu werden einerseits Fachliteraturen und Internetrecherchen und andererseits ExpertInnen Interviews durchgeführt. Aus den Auswertungen dieser wird einerseits ein Framework entworfen, mittels diesem es möglich ist eine Implementierung zu prüfen beziehungsweise zu entwerfen.

Als Ergebnis wurden drei Gruppen von Maßnahmen identifiziert, diese wären vertragliche, organisatorische und technische Maßnahmen. Es hat sich gezeigt, dass es möglich ist, unter Beachtung der erarbeiteten Maßnahmen, die Kernprozesse der Versicherungen, der Datenschutzgrundverordnung entsprechend, in Public Cloud Umgebungen umzusetzen. Als Aussicht auf die weitere Entwicklung kann angenommen werden, dass durch die Weiterentwicklung der Public Cloud Provider, diese Umgebungen immer stärker in der Versicherungs-IT eingesetzt werden.

Schlagwörter:

Public Cloud, DSGVO, Versicherungsprozesse, Datenschutz, IT-Security, Framework

Abstract: Requirements for the use of public cloud solutions in the insurance industry

The high IT costs in insurance companies require them to look for alternatives replacing currently used techniques. One of those is the implementation of their core processes using public cloud environments. Flexibility, scalability and costs are the main cost drivers. However, in order to be able to implement this, there are some legal regulations, such as the General Data Protection Regulation, to be observed.

In this work it will be examined, which technical and organizational measures are necessary to be able to implement the insurance core processes within public cloud solutions in compliance with the General Data Protection Regulation.

There will be done an analysis of literature and internet research as well as expert interviews. Based on the evaluations a framework will be designed which will give assistance for testing and designing of a public cloud implementation.

As a result, three sets of measures have been identified, which are contractual, organizational and technical measures. It has shown that it is possible to implement the core processes of insurance companies in public cloud environments, in accordance with the Data Protection Regulation, taking into account the measures that have been developed. As a further prospect, it can be assumed that the further development of public cloud providers means that these environments are increasingly being used within the IT of insurance companies.

Keywords:

public cloud, GDPR , insurance process, data privacy, it-security, framework

Inhaltsverzeichnis

1. Einleitung

In der Versicherungsbranche gibt es ein sehr breites Angebot an Versicherungsprodukten. Dieses breite Angebot und die hohe Komplexität der Produkte verursacht sehr hohe IT-Kosten. Dies bedeutet, dass Versicherungen einen hohen Anteil (in Deutschland im Jahr 2005 ein IT-Kostenverhältnis von 4%) ihres Budget für diese Kosten ausgeben. Laut einer Studie des Frauenhofer Instituts (Weidmann, et al., 2010) wurden Synergie Effekte beobachtet, die bei steigender Anzahl von Polizzen die IT Kosten pro Stück sinken lassen. Modelle wie zum Beispiel Software as a Service, Infrastructure as a Service oder Plattform as a Service werden mit derzeit internen Rechenzentrumsmodellen konkurrieren (Weidmann, et al., 2010, S. 11). Diese neuen Technologien sollen eine erhebliche Effizienzsteigerung in der Versicherungsbranche ermöglichen. Allerdings entstehen dadurch einige organisatorische und rechtliche Anforderung (A-SIT, 2016). Diese entstehen einerseits durch die ständige Steigerung der Datenmengen, aber auch durch gesetzliche Vorschriften (Datenschutzgesetz). Beispiele dafür wären eine flexible Skalierbarkeit und eine hohe Sensibilisierung für den Umgang mit den Daten (von Diemar, et al., 2011). Der Hauptfokus dieser Arbeit ist der Umgang mit diesen Daten.

Durch die am 25.5.2018 in Kraft getretene Datenschutzgrundverordnung werden unter anderem sehr hohe Anforderungen an die Speicherung, Verarbeitung und Bereitstellung von personenbezogenen Daten gestellt. In dieser Verordnung wird auf die Notwendigkeit des Einsatzes von „State of the Art“ Technologie zum Schutz der Daten verwiesen (EUR-Lex, 2016). In dieser Arbeit wird auch erarbeitet, was aus jetzigem Stand der Technologie zur Sicherung der Daten bezeichnet wird, unter der Berücksichtigung der möglichen Weiterentwicklung. Als Beispiel wären die Übertragung und Verschlüsselung von Daten zu erwähnen.

In dieser Arbeit werden zunächst die Kernprozesse der Versicherungsbranche dargestellt. Dabei wird besonders auf die Speicherung, Verarbeitung und Bereitstellung von Daten und auf den Bezug der rechtlichen Vorschriften, fokussiert.

Der zu betrachtende Datenbereich wird auf die in der Datenschutzgrundverordnung erwähnten personenbezogenen Daten (DSGVO und DSG und sensiblen Daten (besonders schutzwürdige Daten wie in DSG) begrenzt (EUR-Lex, 2016). Auf Basis der Datenschutzgrundverordnung können unter anderem branchenübliche Standards geschaffen werden, vergleichbar der Verhaltensregeln in der DSGVO Artikel 40, die die Grundlage für einen sichern Cloudbetrieb bieten können. Es soll eine Möglichkeit geschaffen werden Cloud Lösungen zu prüfen, beziehungsweise bewerten zu können.

Um dieses Thema bearbeiten zu können sind einige Gegenstände aus dem Curriculum des Wirtschaftsinformatik Studiums relevant. Es sind die Lehrveranstaltungen im Zusammenhang mit rechtlichen Themen (RE411 Rechtsfragen und Rechtsprobleme in der Wirtschaftsinformatik, RE422 Internationales Vertragsrecht u. Europarechtsmaterien in der WI) relevant, aber auch die Lehrveranstaltungen IT523 Verteilte Systeme und IT422 Technische Sicherheitsaspekte haben einen hohen Bezug.

1.1 Arbeitsziel

Das konkrete Ziel der Arbeit ist es darzustellen, welche technischen beziehungsweise organisatorischen Maßnahmen notwendig sind, um Public Cloud Lösungen für die Kernprozesse der Versicherungsbranche, nach den gesetzlichen Vorschriften einsetzen zu können.

Es soll ein Framework entstehen, mit dem überprüft werden kann, ob die gesetzten technischen und organisatorischen Maßnahmen für die Einhaltung der gesetzlichen Vorschriften ausreichen oder nicht.

Anhand dieses Frameworks können die von der Versicherungs-IT gesetzten technischen und organisatorischen Maßnahmen und auch die des Cloud Providers überprüft, beziehungsweise bewertet werden.

In der Datenschutzgrundverordnung wird grundsätzlich nur auf „State of the Art“ Technologie verwiesen (EUR-Lex, 2016). In dieser Arbeit soll auch beschrieben werden, wie dieser feststellbar ist, beziehungsweise definiert werden kann.

1.2 Forschungsfrage

Unter welchen technischen und organisatorischen Voraussetzungen kann eine Public Cloud Lösung, unter Einhaltung der Anforderungen, die sich auf Grund der Datenschutzgrundverordnung (DSGVO) und dem Datenschutzgesetz (DSG) ergeben, für die Kernprozesse der Versicherungsbranche eingesetzt werden?

1.3 Methodische Vorgangsweise

Die Methoden, die in dieser Arbeit angewendet werden, sind einerseits Literaturrecherche und andererseits Experten Interviews. (Vogt & Werner, 2014)

Es sollen durch Literaturrecherche und Befragungen von Versicherungs- und Rechtsexperten, die Information zu den Kernprozessen und der Datenverwendung (Datenspeicherung, Datenverarbeitung und Datenbereitstellung), und die rechtlichen Vorschriften erhoben werden.

Bezüglich technischer Lösungen und die zukünftige Entwicklung werden in Zusammenarbeit mit Experten aus dem Bereich Security, IT-Security und Cloudprovider durch Interviews, sowie Literatur- und Internetrecherche die nötigen Informationen erarbeitet.

Bevor die Interviews durchgeführt werden, wird ein Entwurf eines Frameworks erstellt, welcher mit den Experten geprüft wird. Die Erkenntnisse dieser Prüfung werden danach in Erstellung des fertigen Frameworks berücksichtigt.

Die Interviews werden alle mit einem Leitfaden gestützt durchgeführt. (Vogt & Werner, 2014) Es werden dazu aus den vorhandene Themen wie Datenschutz, IT-Sicherheit und Cloud Themenblöcke gebildet und mit den erarbeiteten Informationen in Form von Brainstorming offene Fragen erarbeitet. Wichtig wird

sein, den kompletten notwendigen Informationsbereich abzudecken. Diese Fragen werden danach in einen zeitlichen Ablauf gebracht. Dieser stellt den Leitfaden dar und liefert das Gerüst um die Interviews vergleichbar und auswertbar zu machen. Eine Aufgabe für den Interviewer besteht darin, flexibel mit den Fragen umzugehen. Als Beispiel wäre zu nennen, wenn eine kommende Frage schon im Gespräch beantwortet wurde, sollte diese auch nicht mehr gestellt werden und umgekehrt, wenn ein zusätzliches Thema auftaucht, sollte dieses auch behandelt werden (Zepke, 2016, S. 51-53). Der zu erfragende Inhalt wird in Kapitel 0 genauer definiert.

Zur Überprüfung der Datenverwendung der Versicherungsprozesse werden ebenfalls Leitfaden gestützte Interviews mit Versicherungsfachkräften geführt. In diesem werden die erarbeiteten Informationen bezüglich der Kernprozesse überprüft und dazu die Datenverwendung in den einzelnen Leistungsprozessen erfragt.

1.4 Aufbau der Arbeit

Der Aufbau der Arbeit gliedert sich in einen theoretischen Teil, der die Analyse der Kernprozesse der Versicherung, der Datenschutzgrundverordnung und der möglichen Public Cloud Implementation als Inhalt hat. Ein weiterer Teil ist die Erhebung beziehungsweise die Erarbeitung der Datennutzung in den einzelnen Kernprozessen der Versicherung.

Der praktische Teil beinhaltet neben den Ergebnissen der theoretischen Analyse auch die Auswertung der Experten Interviews, aus dem Bereich Datenschutz, IT-Sicherheit und Public Cloud sowie die Zusammenführung der Resultate aus beiden Formen. Aus den Ergebnissen beider Teile werden Checklisten zur Überprüfung beziehungsweise Planung solcher Implementierungen erstellt.

Im abschließenden Teil wird danach noch einmal eine Übersicht der notwendigen Maßnahmen erstellt. Es soll vor allem auch die Information der Spezialisten mit eingearbeitet werden. Am Ende der Arbeit erfolgt noch ein Ausblick in Bezug auf Public Cloud Lösungen im Versicherungsumfeld und auf die mögliche Erweiterung dieser Arbeit beziehungsweise der Checklisten.

2. Kernprozesse der Versicherung

In diesem Kapitel werden einerseits die Kernprozesse der Versicherung sowie deren Inhalte und auch die verschiedenen Versicherungssparten dargestellt.

2.1 Prozessübersicht in der Versicherung

In Versicherungen gibt es, wie in jedem Unternehmen, verschiedenste Arten von Prozessen. In dieser Arbeit sollen die Prozesse, die das Kerngeschäft der Versicherung darstellen, genauer untersucht werden, um die Voraussetzungen für die Abbildung dieser Prozesse in IT-Systemen in der Public Cloud zu erläutern. Um diese Prozesse zu identifizieren muss die Prozesslandschaft analysiert werden. Welche grundlegen Prozesse gibt es in Versicherungsunternehmen?

Wie in Abbildung 1 dargestellt können die Prozesse anhand der Wertschöpfungskette analysiert werden.

Abbildung 1 Darstellung der Prozesse nach Wertschöpfungskette (Allenspach, 2015)

Was beinhalten nun diese Gruppierungen der Prozesse (Allenspach, 2015).

- Management Prozesse beinhalten folgende Inhalte:
  - Strategisches Management
  - Unternehmensentwicklung
  - Netzwerkmanagement
  - Führung

- Unterstützungsprozesse beinhalten diese Inhalte:
    - Personalführung
    - IT
    - Rechnungswesen
    - Controlling
    - Sourcing
    - Rückversicherung
    - Logistik und Infrastruktur
    - Verkaufsunterstützung
    - Management Information
- Geschäftsprozesse stellen folgende Inhalte dar.
    - Produktentwicklung und Marktbearbeitung
    - Betrieb
    - Schadensmanagement
    - Asset Management

In dieser Arbeit wird gezielt auf die Geschäftsprozesse eingegangen, da auf diesen der Hauptfokus der Geschäftstätigkeit, beziehungsweise der Wertschöpfung des Versicherungsunternehmens liegt. (Allenspach, 2015)

2.2 Geschäftsprozesse der Versicherung

Die in Kapitel 2.1 dargestellten Geschäftsprozesse werden nun genauer beschrieben.

2.2.1 Produktentwicklung und Marktbearbeitung

In diesem Bereich sind folgende Aktivitäten beziehungsweise Teilprozesse von Bedeutung (Allenspach, 2015, S. 9).

- Die Produktentwicklung beinhaltet Marktforschung, Zielgruppenanalyse, Aktuariat und Portfolio Koordination.
- Kommunikation und Marketing beinhaltet Zielmarkt- und Kundendefinition, Preisgestaltung und Branding.
- Vertrieb beinhaltet Vertriebssteuerung, Kundenberatung, Verkauf und die Vertriebsunterstützung

Der Vertrieb ist der Startpunkt für den eigentlich Leistungsprozess der Versicherung. In Versicherungsunternehmen übernimmt der Vertrieb zahlreiche relevante Aufgaben. In diesem Prozess währen zum Beispiel die Marktforschung, Absatzplanung, Absatzkanalmanagement, Kommunikations- und Servicepolitik zu erwähnen. Der Start des Leistungsprozesses einer Versicherung ist immer der Abschluss des Versicherungsvertrages (Schradin & Malik, 2008, S. 52 - 54).

2.2.2 Betrieb

Im Betrieb von Versicherungsunternehmen werden begleitende Aktivitäten für die Leistungsprozesse Risikoprüfung, Annahme, Angebotsentscheidung und laufende Verwaltung der Versicherungsbestände durchgeführt. Diese beinhalten die innerbetriebliche Begleitung des Absatzprozesses, die anschließende Erstbearbeitung, die Folgebearbeitung sowie die Schlussbearbeitung. (Schradin & Malik, 2008, S. 54).

In der Erstbearbeitung sind alle Prozesse, die in der Absatzdurchführung enthalten sind, welche üblicherweise durch den Eingang eines Versicherungsantrages ausgelöst werden.

Der nächste Schritt wäre die Folgebearbeitung welche alle regelmäßigen und unregelmäßigen Leistungsprozesse für bestehende Versicherungsgeschäfte beinhaltet. Ausgelöst werden diese entweder vom Versicherer, Versicherungsunternehmer oder Dritten. Als Hauptbestandteil kann der Informationsaustausch zwischen Versicherungsunternehmen und Versicherungsnehmer genannt werden (zum Beispiel Adressänderung, Gefahrenerhöhung,….)

Der letzte Schritt wäre die Schlussbearbeitung, welche alle Leistungsprozesse, die zum Beenden des Versicherungsvertrages notwendig sind beinhaltet.

Daraus ergibt sich, dass in der späteren Analyse vor allem folgende Prozesse genauer analysiert werden müssen.

Erstbearbeitung enthält folgende Leistungsprozesse.

- Risikoprüfung
- Annahmeentscheidung

Folgebearbeitung enthält folgenden Leistungsprozess.

- Verwaltung und Service

Schlussbearbeitung enthält folgenden Leistungsprozess.

- Kündigungsabwicklung

2.2.3 Schadensmanagement

Das Schadensmanagement stellt eines der elementarsten Bereiche in den Versicherungen dar. Die Schadensbearbeitung der Schadensabteilung ist üblicherweise der einzige Anknüpfungspunkt für den Kunden zur Beurteilung der Qualität des Versicherungsschutzes. Des Weiteren stellen die im Schadensmanagement entstehenden Kosten die Hauptkostenkomponente der versicherungstechnischen und betrieblichen Leistungserstellung dar.

Aus diesem Grund sollte auf Hinsicht der Fortführung des Vertrags und gesamtunternehmerischer Zielerreichung, auf die effiziente und sachgerechte Schadensbearbeitung geachtet werden. Alle Leistungsprozesse, die nach einem Eingang einer Schadensmeldung beziehungsweise Schadensanzeige durchgeführt werden, sind in diesem Bereich abgedeckt (Schradin & Malik, 2008, S. 55).

Die Inhalte des Schadensmanagements sind die Feststellung eines Versicherungsfalles, Überprüfung der Ansprüche und die Abwicklung der Regulierung beziehungsweise Auszahlungen des Schadens (Schradin & Malik, 2008, S. 55).

2.2.4 Asset Management

Ein nicht unwesentlicher Bereich in Versicherungen ist das Asset Management, beziehungsweise das Kapitalmanagement. Da zwischen Zahlungen von Versicherungsprämien und der Auszahlung bei Schäden oder bei Ablauf der Versicherung oft ein großer zeitlicher Unterschied liegt, muss auch eine dementsprechende Bearbeitung erfolgen. Die Erlöse aus diesen Kapitalgeschäften beeinflussen die Rendite und Risiko- Situation und wirken dadurch auf Produkt- und Preisgestaltung (Schradin & Malik, 2008, S. 55 - 56). Da dies aber für den Datenschutz und IT-Rechtsbereich keinen direkten Einfluss hat, wird dieser Teilbereich in dieser Arbeit nicht näher erläutert.

2.2.5 Übersicht der zu analysierenden Prozesse

Nach den ersten Analysen wurde festgestellt, dass vor allem die Prozesse, die mit dem Kunden stattfinden, die sind, die am meisten mit Datenverarbeitung in Zusammenhang stehen und deshalb für diese Arbeit von Bedeutung sind.

Aus diesem Grund wird in Abbildung 2 der Sollprozess eines Versicherungsvertrags Lifecycle und Leistungen dargestellt.

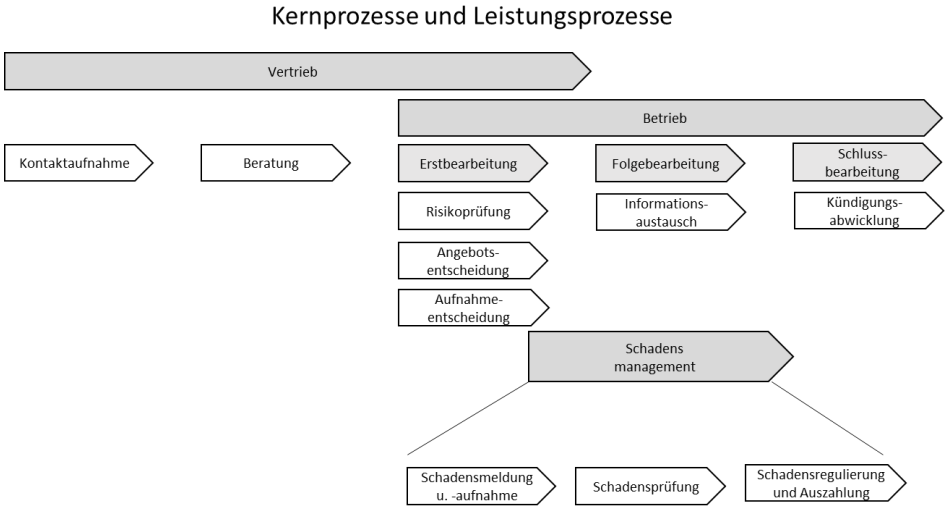

Abbildung 2 Lifecycle Versicherungsvertrag und Leistungen

Wie in Abbildung 2 dargestellt werden folgende Prozesse auf Datenverarbeitung genauer analysiert.

- Im Vertrieb werden die Kontaktaufnahme und die Beratung analysiert.
- Im Betrieb werden die Risikoprüfung, Angebotsentscheidung Aufnahmeentscheidung, der Informationsaustausch und die Kündigungsabwicklung analysiert.
- Im Schadensbereich sind es die Schadensmeldung und -aufnahme, Schadensprüfung, Schadensregulierung und Auszahlung.

2.3 Versicherungssparten

Es müssen zur Bestimmung der Daten unbedingt auch die verschieden Sparten von Versicherungen berücksichtigt werden.

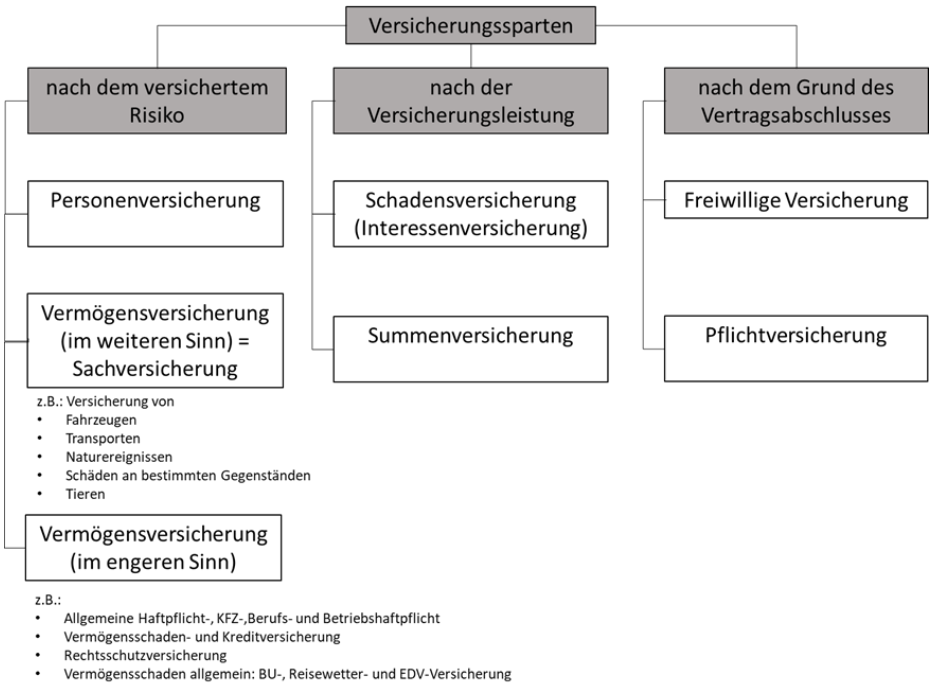

Abbildung 3 Versicherungssparten (Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2008, S. 28)

Wie in Abbildung 3 aus den Skripten der Bildungsakademie der österreichischen Versicherungswirtschaft ersichtlich, können die Sparten nach drei verschiedenen Arten betrachtet werden.

Dies wird nach dem versicherten Risiko, nach der Versicherungsleistung oder nach dem Grund des Vertragsabschlusses durchgeführt. (Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2008, S. 28).

In dieser Arbeit werden in der Analyse der Datenverwendung, die Versicherungsarten betrachtet, die von privaten Versicherungsunternehmen angeboten werden. Es werden nicht die Leistungen der staatlichen Pflichtversicherungen analysiert. Die Versicherungssparten werden aus Sicht des versicherten Risikos zur weiteren Analyse verwendet.

In diesem Sinne wird zwischen Personenversicherungen, Sachversicherung und Vermögensversicherungen unterschieden. Wobei der Fokus auf die Daten, die darin verwendet werden, gelegt wird.

Bei Personenversicherungen handelt es sich um Versicherungsleistungen, die direkt einer Person zuzuteilen sind. Dies wären zum Beispiel Unfall-, Lebens-, Kranken,-Sterbe-, Pflege-, Berufsunfähigkeit-, Private Kranken-Versicherungen. An den Namen dieser Versicherungen ist schon erkennbar, dass in diesen Arten, die Verarbeitung besonderer Kategorien von personenbezogenen Daten (sensible Daten) notwendig ist.

In den Sachversicherungen handelt es sich um die Abdeckung von Schäden an Sachen. Diese könnten zum Beispiel Feuer-, Haushalts-, KFZ Kasko-, Transport beinhalten (Wagner, 2018). In diesen Arten von Versicherungen muss analysiert werden, welche personenbezogenen Daten verwendet werden.

3. Datenschutzgrundverordnung und Datenschutzgesetz

In diesem Kapitel werden in kurzer Form die Datenschutzgrundverordnung (DSGVO) und das Datenschutzgesetz (DSG) vorgestellt. Danach wird eine Kategorisierung der Daten, die von dieser Verordnung beziehungsweise diesem Gesetz betroffen sind erstellt. Diese Kategorisierung wird nach dem Schutzbedarf und notwendigen Absicherung der Daten vorgenommen. Mit dieser Kategorisierung werden in den folgenden Kapiteln, die Einteilung der technischen und organisatorischen Maßnahmen vorgenommen.

3.1 Datenschutzgrundverordnung (DSGVO)

„Die Datenschutz-Grundverordnung (vollständiger Titel: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG) ist ab dem 25. Mai 2018 die Grundlage des allgemeinen Datenschutzrechts in der EU und Österreich. Im Gegensatz zur alten Datenschutzrichtlinie ist die Datenschutz-Grundverordnung (kurz DSGVO) in Österreich unmittelbar anwendbar. Das Datenschutzgesetz ergänzt die DSGVO nur". (Österreichische Datenschutzbehörde (DSB), 2018)

Die Datenschutzgrundverordnung besteht aus insgesamt aus elf Kapitel, mehreren Abschnitten und insgesamt 99 Artikel. Die Inhalte der Kapitel gliedern sich folgendermaßen auf (Österreichische Datenschutzbehörde (DSB), 2018).

- KAPITEL I: allgemeine Bestimmungen (Gegenstand und Ziele, Anwendungsbereich, Definitionen, Begriffsbestimmungen)
- KAPITEL II: Grundsätze (Rechtmäßigkeit der Verarbeitung, Bedingungen für die Einwilligung, Einwilligung von Kindern, Besondere Kategorien personenbezogener Daten, Identifizierung von Personen)

- KAPITEL III: Rechte der betroffenen Person (Transparenz, Informationspflichten, Auskunftsrechte, Löschungsrechte (Recht auf Vergessen werden), Widerspruchsrecht, Beschränkungen)
- KAPITEL IV: Verantwortlicher und Auftragsverarbeiter (Transparenz, Informationspflichten, Auskunftsrechte, Löschungsrechte (Recht auf Vergessenwerden), Widerspruchsrecht, Beschränkungen)
- KAPITEL V: Datenübermittlung in Drittländer oder int. Organisationen (Allgemeine Grundsätze der Datenübermittlung, Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses, Datenübermittlung vorbehaltlich geeigneter Garantien, verbindliche interne Datenschutzvorschriften, Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung)
- KAPITEL VI: Unabhängige Aufsichtsbehörden (Unabhängigkeit, Zuständigkeit, Aufgaben und Befugnisse)
- KAPITEL VII: Zusammenarbeit und Kohärenz (Zusammenarbeit, Kohärenz, Europäischer Datenschutzausschuss)
- KAPITEL VIII: Rechtsbehelfe, Haftung und Sanktionen (Recht auf Beschwerde bei einer Aufsichtsbehörde, Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde, Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter, Vertretung von betroffenen Personen, Aussetzung des Verfahrens, Haftung und Recht auf Schadenersatz, Allgemeine Bedingungen für die Verhängung von Geldbußen, Sanktionen)
- KAPITEL IX: Vorschriften für besondere Verarbeitungssituationen (Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit, Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten, Verarbeitung der nationalen Kennziffer, Datenverarbeitung im Beschäftigungskontext, Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken,

Geheimhaltungspflichten, Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften)

- KAPITEL X: Delegierte Rechtsakte und Durchführungsrechtakte (Ausübung der Befugnis Übertragung, Ausschussverfahren)
- KAPITEL XI: Schlussbestimmungen (Aufhebung der Richtlinie 95/46/EG, Verhältnis zur Richtlinie 2002/58/EG, Verhältnis zu bereits geschlossenen Übereinkünften, Berichte der Kommission, Überprüfung anderer Rechtsakte der Union zum Datenschutz, Inkrafttreten und Anwendung.

3.2 Analyse der Datenschutzgrundverordnung (DSGVO)

In diesem Kapitel wird nun die Datenschutzgrundverordnung analysiert. Es sollen diese Bereiche genauer ausgeführt werden, die für das Verständnis und diese Arbeit notwendig sind. Es werden bewusst die Kapitel VI bis XI nicht betrachtet, da sie aus Sicht des Autors, bezüglich der notwendigen Maßnahmen zur Umsetzung der Versicherungskernprozesse nicht relevant sind. Als Beispiel kann hier Kapitel VIII Rechtsbehelfe, Haftung und Sanktionen genannt werden.

3.2.1 Anwendungsbereich der DSGVO

Der Anwendungsbereich der DSGVO wird in sachlichen und räumlichen Bereich aufgeteilt (EUR-Lex, 2016).

- Sachlicher Anwendungsbereich

Es kann zusammenfassend dargestellt werden, dass diese Verordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, als auch für die nichtautomatisierte Verarbeitung dieser, wenn sie in einem Dateisystem gespeichert sind oder werden, gilt (EUR-Lex, 2016).

Ausnahme sind, wenn diese Verarbeitung (EUR-Lex, 2016):

- nicht in der Rechtsprechung der europäischen Union fällt,
- durch natürliche Personen für privat oder familiär erfolgt,
- durch Behörden im Rahmen von Behandlung von Straftaten oder Strafverfolgung oder Schutz vor oder Abwehr von Gefahren für die Öffentlichkeit erfolgt.

- Räumlicher Anwendungsbereich

Bei Verarbeitung von Daten, tritt das Datenschutzgesetz dann in Kraft, wenn sich entweder die Verarbeitung, Verantwortung der Verarbeitung, die Verarbeitung in Zusammenhang mit angebotenen Waren oder Dienstleistungen an Personen in der europäischen Union oder in einem Staat dessen Völkerrecht dem eines Mitgliedslandes der europäischen Union unterliegt, erfolgt.

3.2.2 Personen bezogene Daten laut DSGVO

Personenbezogene Daten sind all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind, wodurch Rückschlüsse auf deren Persönlichkeit möglich sind.

„„personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann". (EUR-Lex, 2016)

Als eigenes Kapitel dargestellt, ist die Regelung zur Verarbeitung von besonderen Kategorien von personenbezogener Daten.

„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt". (EUR-Lex, 2016)

Es gibt dazu allerdings auch gewisse Ausnahmen. Diese wären zum Beispiel (EUR-Lex, 2016):

- Wenn die Person ausdrücklich eingewilligt hat.
- Es erforderlich ist damit der Verantwortliche oder die betroffene Person die ihm, beziehungsweise ihr, aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen beziehungsweise ihren, diesbezüglichen Pflichten nachkommen kann.
- Wenn die Daten von der betroffenen Person offensichtlich öffentlich gemacht wurden.
- Wenn es zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist.
- Wenn es zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

3.2.3 Prinzipien der DSGVO

Folgende Prinzipien werden in der DSGVO beschrieben (Österreichische Datenschutzbehörde (DSB), 2018).

1) Rechtmäßigkeit, Gerechtigkeit und Transparenz. Die Verarbeitung von personenbezogenen Daten muss legal, fair und transparent sein. Informationen über die Zwecke, Methoden und Mengen der Verarbeitung personenbezogener Daten sollten zugänglich und so einfach wie möglich angegeben werden.

2) Beschränkung des Zwecks. Daten müssen ausschließlich für die vom Unternehmen angegebenen Zwecke erhoben und genutzt werden.

3) Minimierung der Daten. Es besteht keine Berechtigung, personenbezogene Daten in einem größeren Umfang als für die Verarbeitung erforderlich zu sammeln.

4) Genauigkeit. Personenbezogene Daten, die ungenau sind, müssen gelöscht oder korrigiert werden.

5) Speicherbeschränkung. Personenbezogene Daten dürfen in einer Form, die es ermöglicht, betroffene Personen zu identifizieren, nur so lange verarbeitet werden, wie es für den jeweiligen Zweck erforderlich ist.

6) Integrität und Vertraulichkeit. Personenbezogene Daten müssen vor unbefugter oder rechtswidriger Verarbeitung, Zerstörung und Beschädigung geschützt werden.

3.2.4 Einsatzgebiet der DSGVO

Die DSGVO ist eine Verordnung, die für alle Mitglieder der Europäischen Union bindend ist. Auch Nationen, die sich gerade im oder vor ihrem Beitrittsprozess befinden, streben bereits danach die Vorschriften dieser Verordnung vorbereitend in nationales Gesetz umzusetzen (Österreichische Datenschutzbehörde (DSB), 2018).

Folgende Bestimmungen sind in der DSGVO festgehalten (Österreichische Datenschutzbehörde (DSB), 2018).

- eine Niederlassung in der EU haben und personenbezogene Daten verarbeiten.
- personenbezogene Daten von Personen verarbeiten, die sich in der EU befinden.
- außerhalb der EU niedergelassen sind, der Ort der Niederlassung jedoch aufgrund des Völkerrechts dem Recht eines Mitgliedsstaats unterliegt.

3.2.5 Ziele der DSGVO

Das Ziel der DSGVO ist der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Dazu enthält diese Verordnung Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. Innerhalb der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten, der freie Verkehr personenbezogener Daten nicht eingeschränkt beziehungsweise verboten werden (Österreichische Datenschutzbehörde (DSB), 2018).

3.2.6 Organisatorische und technische Vorschriften der DSGVO

Es gibt folgende organisatorische und technische Anforderungen, die sich aus der DSGVO ergeben.

Die größte Änderung ist, die unter Umständen notwendige Verpflichtung, einer für den Datenschutz verantwortliche Person. Diese wird als Datenschutzbeauftragte beziehungsweise Datenschutzbeauftragter bezeichnet. Wenn die Kerntätigkeit des Unternehmens, die Verarbeitung von personenbezogenen Daten ist, muss diese Rolle besetzt werden. Dies gilt grundsätzlich für alle natürlichen oder juristischen Personen, Behörden, Einrichtungen oder andere Stellen, die über die Verarbeitung von personenbezogenen Daten entscheiden (Im Gesetzestext als „Verantwortlicher" bezeichnet) oder im Auftrag anderer verarbeiten (Im Gesetzestext als „Auftragsverarbeiter" bezeichnet). Die genaue Regelung dazu ist in Artikel 37 zu finden (Österreichische Datenschutzbehörde (DSB), 2018).

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

> *a) „die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,*
> *b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder*
> *c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht".* (Österreichische Datenschutzbehörde (DSB), 2018)

Eine weitere notwendige Verpflichtung ist das Führen eines Registers, in dem alle Verarbeitungstätigkeiten angeführt werden müssen. Jeder Verantwortliche muss die Tätigkeiten ihrer Zuständigkeit, in diesem Verzeichnis führen. Dazu gibt es eine Reihe von Angaben, die diese enthalten müssen (Österreichische Datenschutzbehörde (DSB), 2018).

Eine kurze Übersicht der notwendigen Inhalte dieses Verzeichnisses aus der Verordnung sind:

- Info über Verantwortlichen und gegebenenfalls seines Vertreters und des Datenschutzbeauftragten (Name und Kontaktdaten).
- Angabe des Verarbeitungszwecks
- Kategorie der personenbezogenen Daten und Kategorien der Empfänger.
- Kategorien der Empfänger der personenbezogenen Daten.
- Info über Übermittlung von personenbezogenen Daten in ein Drittland oder zu einer internationalen Organisation mit dieser.
- Vorgesehene Fristen der Löschung, wenn möglich.
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Unter Berücksichtigung von Stand der Technik, Kosten, Umfang und Umständen der Verarbeitung, aber auch Eintrittswahrscheinlichkeit und Risiken, muss der Verantwortliche zum Zeitpunkt der Ermittlung und aber auch der Verarbeitung, technische und organisatorische Maßnahmen treffen, um dieser Verordnung zu entsprechen (zum Beispiel Datenminimierung, Pseudonymisierung) (Österreichische Datenschutzbehörde (DSB), 2018).

In Bezug auf die Verarbeitung müssen geeigneten technische und organisatorischen Maßnahmen gesetzt werden um sicherzustellen, dass nur die personenbezogenen Daten verarbeitet werden, die für diesen bestimmten Verarbeitungszweck notwendig sind.

Dies soll sicherstellen, dass ohne Zutun einer Person diese Daten nicht einer unbestimmten Anzahl von Personen zu Verfügung gestellt, beziehungsweise zugänglich gemacht werden. (Österreichische Datenschutzbehörde (DSB), 2018)

Die Informationspflicht bei Verletzungen des Schutzes von personenbezogener Daten an die Aufsichtsbehörde ist eine weitere organisatorische Maßnahme. Die Meldung muss unverzüglich erfolgen und es müssen bestimmte Inhalte wie Beschreibung der Verletzung, Anzahl der betroffenen Personen, Kategorien der Datensätze angegeben werden. Weiters die Kontaktdaten der Datenschutzbeauftragten, Folgen der Verletzung und ergriffene, beziehungsweise vorgeschlagene Maßnahmen. Es müssen alle Informationen und Maßnahmen dokumentiert werden. Die Meldung muss spätestens 72 Stunden nach Feststellung erfolgen, anderenfalls muss eine Begründung der Verzögerung hinzugefügt werden. Dies wird in Artikel 33 der DSGVO beschrieben. Diese Meldung muss in klarer einfacher Sprache die Art der Verletzung beschreiben (Österreichische Datenschutzbehörde (DSB), 2018).

Artikel 32 ist der Artikel, der einen sehr großen Einfluss auf die technische Ausführung von IT Lösungen hat. Dieser beinhaltet Vorgaben, die für die Umsetzung von Verarbeitungen von personenbezogenen Daten notwendig sind (Österreichische Datenschutzbehörde (DSB), 2018).

Diese möglichen Maßnahmen könnten zum Beispiel die Folgenden sein (Österreichische Datenschutzbehörde (DSB), 2018):

- Die personenbezogenen Daten werden pseudonymisiert und verschlüsselt.
- Die Systeme stellen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit im Zusammenhang mit der Verarbeitung auf Dauer sicher.
- Die personenbezogenen Daten können bei Problemen rasch wiederhergestellt werden.
- Es gibt die Möglichkeit der Prüfung, Bewertung und Evaluierung der getroffenen Maßnahmen um die Sicherheit zu gewährleisten.

3.2.7 Vorschriften der DSGVO zur Übermittlung von Daten

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird (Österreichische Datenschutzbehörde (DSB), 2018).

Weiters wird in Artikel 45 besagt, dass wenn die Kommission, das angemessene Schutzniveau eines Drittlandes oder internationalen Organisation festgestellt hat, Daten ohne besondere Genehmigung übermittelt werden dürfen (Österreichische Datenschutzbehörde (DSB), 2018).

3.2.8 Rechte der betroffenen Person

In der DSGVO werden den betroffenen Personen einige Recht zugestanden (EUR-Lex, 2016). Diese werden nun in den nächsten Unterkapiteln vorgestellt.

3.2.8.1 Informationspflicht

Die Informationspflicht gibt an welche Informationen der Person bei der Erhebung der Daten übermittelt werden müssen. Dies sind zusammengefasst alle Daten zu den Verantwortlichen, Datenschutzbeauftragten und den Zweck, für den die Daten erhoben werden sollen. Wie lange Daten gespeichert werden oder zumindest das Kriterium der Festlegung der Dauer.

Des Weiteren müssen die Informationen erfolgen, welche Möglichkeiten für die faire und transparente Verarbeitung zu Verfügung stehen. Als Beispiele wären das Auskunftsrecht, die Löschung, die Einschränkung der Verarbeitung, das Widerspruchsrecht und das Beschwerderecht zu nennen. Weiters beinhaltet das Kapitel auch die Erklärung des Auskunftsrechts der betroffenen Person (EUR-Lex, 2016).

Eine weiter Information ist notwendig, wenn die Daten nicht von der betroffenen Person selbst kommen. In diesem Fall muss auch die Information der Quelle bekannt gegeben werden und dies muss maximal nach einem Monat oder bei Kontakt der Person erfolgen (EUR-Lex, 2016).

3.2.8.2 Auskunftsrecht

Das Auskunftsrecht besagt, dass eine betroffene Person jederzeit Auskunft über die folgenden Informationen zu seinen Daten bekommen muss.

- *die Verarbeitungszwecke;*
- *die Kategorien personenbezogener Daten, die verarbeitet werden;*
- *die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;*
- *falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;*
- *das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;*
- *das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;*
- *wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;*

- *das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.* (EUR-Lex, 2016)

3.2.8.3 Recht auf Berichtigung

Dieser Artikel besagt, dass eine betroffene Person das Recht hat, vom Verantwortlichen das unverzügliche Berichtigen von unrichtigen personenbezogenen Daten zu verlangen. Sie hat das Recht die Vervollständigung unvollständiger personenbezogener Daten zu verlangen (EUR-Lex, 2016).

3.2.8.4 Recht auf Löschung („Recht auf Vergessenwerden“)

Eine betroffene Person hat das Recht zu verlangen, dass personenbezogene Daten unverzüglich gelöscht werden. Der Verantwortliche ist auch grundsätzlich dazu verpflichtet dem Verlangen unverzüglich nachzukommen.

Es gibt dazu allerdings einige Ausnahmen die in diesem Artikel beschrieben sind (EUR-Lex, 2016).

- *zur Ausübung des Rechts auf freie Meinungsäußerung und Information;*
- *zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;*
- *aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;*

- *für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.*

3.2.8.5 Recht auf Einschränkung der Verarbeitung

Eine Person hat das Recht, die Einschränkung der Verarbeitung der Daten zu verlangen. Dies ist zum Beispiel, wenn die Richtigkeit der personenbezogenen Daten bestritten wird, wenn die Löschung wegen Geltendmachung von Rechtsansprüchen benötigt wird oder wenn die Person Widerspruch gegen die Verarbeitung eingelegt hat.

Wenn diese Einschränkung gemäß den oben angeführten Gründen erwirkt wurde, muss der Verantwortliche die Person informieren, sobald die Einschränkung aufgehoben wird (EUR-Lex, 2016).

3.2.8.6 Recht auf Datenübertragung

Eine betroffene Person hat das Recht, alle sie betreffenden personenbezogenen Daten im strukturierten, gängigen und maschinenlesbaren Format zu erhalten, beziehungsweise dass diese direkt an einen anderen Verantwortlichen übermittelt werden. Dies beruht allerdings darauf das die Verarbeitung auf einer Einwilligung beruht und die Übermittlung mithilfe automatisierter Verfahren erfolgt (EUR-Lex, 2016).

3.2.9 Allgemeine Bedingungen für die Verhängung von Geldbußen

In der DSGVO wird ebenfalls der mögliche Strafrahmen bei Verstößen geregelt. Dieser schreibt Strafen bis zu 20 Millionen Euro oder 4 % des weltweiten Gesamtumsatzes eines Unternehmens vor (EUR-Lex, 2016).

3.3 Zusammenfassung Datenschutzgrundverordnung (DSVGO)

Zusammenfassend kann im Bezug zu dieser Arbeit gesagt werden, dass für die Verarbeitung von Daten in den Kernprozessen der Versicherung, das Datenschutzgesetz dann in Kraft tritt, wenn sich entweder die Verarbeitung, Verantwortung der Verarbeitung, die Verarbeitung in Zusammenhang mit angebotenen Waren oder Dienstleistungen an Personen in der europäischen Union oder in einem Staat dessen Völkerrecht dem eines Mitgliedslandes der europäischen Union unterliegt, erfolgt.

Die Erkenntnis der Analyse der Datenschutzgrundverordnung ist, dass es für die Einhaltung dieser, einige technische und organisatorische Maßnahmen für Versicherungsunternehmen gibt. Diese beziehen sich einerseits auf den Cloudprovider zum Beispiel in vertraglicher Hinsicht, aber auch in der innerbetrieblichen Organisation und technischen Umsetzung.

In Abbildung 4 wird nun eine Aufstellung von personenbezogenen Daten, die für die Versicherungsprozesse relevant sind, dargestellt.

		personen bezogene Daten	besonders schützenswerte personenbezogene Daten
Basis Personendaten	• Vollständiger Name	x	
	• Alter / Geburtsdatum	x	
	• Geschlecht	x	
	• Adresse	x	
	• Kontakt Details	x	
	• Identitätsnachweis (z. B. Reisepass)	x	
	• Staatsangehörigkeit	x	
	• Beruflicher Status	x	
	• Angaben zum Führerschein	x	
Familie und soziale Umstände	• Familienstand	x	
	• Angehörige / Ehepartner / Partner / Familienangaben	x	
	• Nächste Angehörige / Notfallkontakt	x	
	• Geburtsurkunden, Heraitsurkunden,…	x	
	• Ethnizität		x
	• Religion / religiöse Überzeugungen		x
	• Sexuelle Orientierung		x
	• Andere Informationen zu Diversität und Gleichstellung		x
	• besondere Freizeitgestaltung (gefährliche Sportarten)		x
Finanz und staatliche Verischerungsdaten	• Kontoauszüge		x
	• Bankkonto Information		x
	• Kreditkarteninformation		x
	• Bonitätsprüfung		x
	• Sozialversicherungsnummer		x
Gesundheitsdaten	• Angaben zur körperlichen und psychischen Gesundheit		x
	• Details zu Behinderung, Zugang und besonderen Anforderungen		x
sonstige Daten	• Foto- und Videobilder z.B. Schadensbilder von Gebäuden,KfZ		x
	• Standort- / Tracking-Daten		x
	• Genetische oder biometrische Daten		x

Abbildung 4 Aufstellung von Datengruppierungen

Aufbauend werden noch einige Beispiele bezüglich der „Angaben zur körperlichen und psychischen Gesundheit“ und „den Details zur Behinderung, Zugang und besonderen Anforderungen „in Abbildung 4 gesammelt als Gesundheitsdaten beschrieben. Dazu wären als Beispiele der Gesundheitszustand, frühere Krankheiten, Unfälle, Körperschäden, Ablehnung eines Antrages auf Krankenversicherung, Krankenversicherung bei einem anderen Versicherer zu nennen. (Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018, S. 40)

3.4 Datenschutzgesetz (DSG)

Das Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999 idgF., ist das geltende österreichische Datenschutzgesetz und ergänzt die Datenschutz-Grundverordnung (DSGVO) (Österreichische Datenschutzbehörde (DSB), 2018).

Das Datenschutzgesetz wurde durch das Datenschutz Anpassungsgesetz 2018, BGBI. I Nr. 120/2017, stark verändert (Österreichische Datenschutzbehörde (DSB), 2018). Es kann in Bezug auf diese Arbeit vernachlässigt werden, da die Hauptfaktoren, die der Forschungsfrage dienen, in der DSVGO enthalten sind.

4. Datenaufbereitung

In den folgenden Kapiteln werden nun die Versicherungssparten, auf die in Kapitel 2.3 eingegrenzt wurde, auf Datenverwendung analysiert und den in Kapitel 3.3. erstellten Kategorien zugeteilt.

4.1 Analyse der Versicherungssparten auf Datenverwendung

In diesem Bereich werden nun die Versicherungssparten auf die notwendige Datenverwendung analysiert.

4.1.1 Sachversicherung

Folgende Versicherungen sind in diesem Bereich als Beispiele genannt und werden auf verwendete Daten analysiert.

- Feuer, Haushaltsversicherung

  Personenbezogene Daten sind folgende zu nennen (Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018).
  - Basis Personendaten
  - Daten aus dem Bereich Familien und soziales Umfeld
  - Daten aus Finanz und staatliche Versicherungsdaten
  - sonstige Daten

- KFZ Kaskoversicherung

  Personenbezogene Daten sind folgende zu nennen (Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018).
  - Basis Personendaten
  - Daten aus dem Bereich Familien und soziales Umfeld
  - Daten aus Finanz und staatliche Versicherungsdaten
  - sonstige Daten

4.1.2 Personenversicherungen

Folgende Versicherungen sind in diesem Bereich als Beispiele genannt und werden auf verwendete Daten analysiert.

- Private Krankenversicherung

  Personenbezogene Daten sind folgende zu nennen (Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018).

  - Basis Personendaten
  - Daten aus dem Bereich Familien und soziales Umfeld
  - Daten aus Finanz und staatliche Versicherungsdaten
  - Gesundheitsdaten
  - sonstige Daten

- Lebensversicherung

  Personenbezogene Daten sind folgende zu nennen (Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018).

  - Basis Personendaten
  - Daten aus dem Bereich Familien und soziales Umfeld
  - Daten aus Finanz und staatliche Versicherungsdaten
  - Gesundheitsdaten
  - sonstige Daten

4.2 Analyse der Prozesse auf Datenverwendung

Wie in Kapitel 2.2.5 Übersicht der zu analysierenden Prozesse schon angeführt sind es folgende Prozesse, die über ihre Datennutzung genauer analysiert gehören.

- Vertrieb
    - Kontaktaufnahme
    - Beratung
- Betrieb
    - Risikoprüfung
    - Angebotsentscheidung
    - Aufnahmeentscheidung
    - Informationsaustausch
    - Kündigungsabwicklung
- Schaden
    - Schadensmeldung und -aufnahme
    - Schadensprüfung
    - Schadensregulierung und Auszahlung

Auf den folgenden Seiten werden nun die Versicherungsarten in Bezug auf Prozesse und Datenverwendung dargestellt.

- Abbildung 5 Sachversicherungen
- Abbildung 6 Personenversicherungen
- Abbildung 7 Lebensversicherungen

Sachversicherung:

		Sachversicherung											
		Datenart		Vertrieb		Betrieb					Schaden		
Typ	Beschreibung	pbD	besonders schützenswerte pbD	Kontakt aufnahme	Beratung	Risiko prüfung	Angebots-entscheidung	Aufnahme-entscheidung	Informations-austausch	Kündigungs-abwicklung	Schadens-meldung und aufnahme	Schadens prüfung	Schadens regulierung
Basis Personendaten	Vollständiger Name	x		x	x	x	x	x	x		x	x	x
	Alter / Geburtsdatum	x				x	x	x	x		x	x	x
	Geschlecht	x		x	x	x	x	x	x		x	x	x
	Adresse	x		x	x	x	x	x	x		x	x	x
	Kontakt Details	x		x	x	x	x	x	x		x	x	x
	Identitätsnachweis (z. B. Reisepass)	x			x	x	x	x	x		x	x	x
	Staatsangehörigkeit	x			x	x	x	x	x		x	x	x
	Beruflicher Status	x			x	x	x	x	x		x	x	x
	Unterschrift / Willenserklärungen	x		x	x	x	x	x	x		x	x	x
	Angaben zum Führerschein	x			x	x	x	x	x		x	x	x
Familie und soziale Umstände	Familienstand	x			x	x	x	x	x		x	x	x
	Angehörige / Ehepartner / Partner / Familienangaben	x				x	x	x	x		x	x	x
	Nächste Angehörige / Notfallkontakt	x											
	Geburtsurkunden, Heiratsurkunden,…	x											
	Ethnizität		x										
	Religion / religiöse Überzeugungen		x										
	Sexuelle Orientierung		x										
	Andere Informationen zu Diversität und Gleichstellung		x										
	besondere Freizeitgestaltung (gefährliche Sportarten)		x			x	x	x	x		x	x	x
Finanz und staatliche Versicherungs daten	Kontoauszüge		x										
	Bankkonto Information		x			x	x	x	x		x	x	x
	Kreditkarteninformation		x										
	Bonitätsprüfung		x			x	x						
	Sozialversicherungsnummer		x										
Gesundheits-daten	Angaben zur körperlichen und psychischen Gesundheit		x										
	Details zu Behinderung, Zugang und besonderen Anforderungen		x										
sonstige Daten	Foto- und Videobilder z.B. Schadensbilder von Gebäuden,KfZ		x			x	x	x	x		x	x	x
	Standort- / Tracking-Daten		x			x	x	x	x		x	x	x
	Genetische oder biometrische Daten		x										

Abbildung 5 Datenverwendung Sachversicherungen

Personenversicherung:

		Personenversicherungen											
		Datenart		Vertrieb		Betrieb					Schaden		
Typ	Beschreibung	pbD	besonders schützenswerte pbD	Kontakt aufnahme	Beratung	Risiko prüfung	Angebots-entscheidung	Aufnahme-entscheidung	Informations-austausch	Kündigungs-abwicklung	Schadens-meldung und aufnahme	Schadens-prüfung	Schadens-regulierung
Basis Personendaten	Vollständiger Name	x		x	x	x	x	x	x	x	x	x	x
	Alter / Geburtsdatum	x			x	x	x	x	x	x	x	x	x
	Geschlecht	x		x	x	x	x	x	x	x	x	x	x
	Adresse	x		x	x	x	x	x	x	x	x	x	x
	Kontakt Details	x		x	x	x	x	x	x	x	x	x	x
	Identitätsnachweis (z. B. Reisepass)	x			x	x	x	x	x	x	x	x	x
	Staatsangehörigkeit	x			x	x	x	x	x	x	x	x	x
	Beruflicher Status	x			x	x	x	x	x	x	x	x	x
	Unterschrift / Willenserklärungen	x		x	x	x	x	x	x	x	x	x	x
	Angaben zum Führerschein	x			x	x	x	x	x	x	x	x	x
Familie und soziale Umstände	Familienstand	x				x	x	x	x		x	x	x
	Angehörige / Ehepartner / Partner / Familienangaben	x				x	x	x	x		x	x	x
	Nächste Angehörige / Notfallkontakt	x				x	x	x	x		x	x	x
	Geburtsurkunden, Heiratsurkunden,…	x				x	x	x	x				
	Ethnizität		x										
	Religion / religiöse Überzeugungen		x										
	Sexuelle Orientierung		x										
	Andere Informationen zu Diversität und Gleichstellung		x										
	besondere Freizeitgestaltung (gefährliche Sportarten)		x		x	x	x	x	x	x	x	x	x
Finanz und staatliche Versicherungs daten	Kontoauszüge		x										
	Bankkonto Information		x			x	x	x	x	x	x	x	x
	Kreditkarteninformation		x										
	Bonitätsprüfung		x			x	x	x					
	Sozialversicherungsnummer		x										
Gesundheits-daten	Angaben zur körperlichen und		x		x	x	x	x	x		x	x	x
	Details zu Behinderung, Zugang und besonderen Anforderungen		x		x	x	x	x	x		x	x	x
sonstige Daten	Foto- und Videobilder z.B. Schadensbilder von Gebäuden,KfZ,		x								x	x	x
	Standort- / Tracking-Daten		x										
	Genetische oder biometrische Daten		x										

Abbildung 6 Datenverwendung Personenversicherungen

Lebensversicherungen:

		Lebensversicherung											
		Datenart		Vertrieb		Betrieb					Schaden		
Typ	Beschreibung	pbD	besonders schützenswerte pbD	Kontakt-aufnahme	Beratung	Risiko prüfung	Angebots-entscheidung	Aufnahme-entscheidung	Informations-austausch	Kündigungs-abwicklung	Schadens-meldung und aufnahme	Schadens-prüfung	Schadens-regulierung
Basis Personendaten	Vollständiger Name	x		x	x	x	x	x	x	x	x	x	x
	Alter / Geburtsdatum	x			x	x	x	x	x	x	x	x	x
	Geschlecht	x		x	x	x	x	x	x	x	x	x	x
	Adresse	x		x	x	x	x	x	x	x	x	x	x
	Kontakt Details	x		x	x	x	x	x	x	x	x	x	x
	Identitätsnachweis (z. B. Reisepass)	x			x	x	x	x	x	x	x	x	x
	Staatsangehörigkeit	x			x	x	x	x	x	x	x	x	x
	Beruflicher Status	x			x	x	x	x	x	x	x	x	x
	Unterschrift / Willenserklärungen	x		x	x	x	x	x	x	x	x	x	x
	Angaben zum Führerschein	x			x	x	x	x	x	x	x	x	x
Familie und soziale Umstände	Familienstand	x				x	x	x	x		x	x	x
	Angehörige / Ehepartner / Partner / Familienangaben	x				x	x	x	x		x	x	x
	Nächste Angehörige / Notfallkontakt	x				x	x	x	x		x	x	x
	Geburtsurkunden, Heiratsurkunden,…	x				x	x	x	x				
	Ethnizität		x										
	Religion / religiöse Überzeugungen		x										
	Sexuelle Orientierung		x										
	Andere Informationen zu Diversität und Gleichstellung		x										
	besondere Freizeitgestaltung (gefährliche Sportarten)		x		x	x	x	x	x	x	x	x	x
Finanz- und staatliche Versicherungs daten	Kontoauszüge		x										
	Bankkonto Information		x			x	x	x	x	x	x	x	x
	Kreditkarteninformation		x										
	Bonitätsprüfung		x			x	x	x					
	Sozialversicherungsnummer		x										
Gesundheits-daten	Angaben zur körperlichen und psychischen Gesundheit		x		x	x	x	x	x		x	x	x
	Details zu Behinderung, Zugang und besonderen Anforderungen		x		x	x	x	x	x		x	x	x
sonstige Daten	Foto- und Videobilder z.B. Schadensbilder von Gebäuden,KfZ		x								x	x	x
	Standort- / Tracking-Daten		x										
	Genetische oder biometrische Daten		x										

Abbildung 7 Datenverwendung Lebensversicherungen

4.3 Zusammenfassung der Datenverwendung

Die Erkenntnis aus der Analyse der Datenverwendung ist, dass es grundsätzlich notwendig ist, in allen Prozessen und Teilprozessen sowie, in allen Versicherungssparten, personenbezogene Daten zu verarbeiten. Aus dieser Erkenntnis heraus muss im kompletten Verlauf der Kernprozesse mit den Daten nach den Vorgaben der DSGVO umgegangen werden.

Zusätzlich wird vor allem im Teilprozess Risikoprüfung eine systematische und umfassende Bewertung der persönlichen Aspekte (Profilling) einer natürlichen Person durchgeführt. Diese dient als Grundlage für die Berechnung der Kosten für den Kunden und der Entscheidungen für die Annahme eines Versicherungsantrags für das Versicherungsunternehmen.

5. Public Cloud Lösungen

Als erstes wird in diesem Kapitel eine Darstellung von Cloud Computing durchgeführt. Am Ende des Kapitels werden die für diese Arbeit notwendigen Public Cloud Lösungen genauer dargestellt.

5.1 Definition Cloud Computing

Gemäß der Definition des National Institute of Standards and Technology (NIST) des U.S. Departement of Commerce lautet die Definition von Cloud Computing folgendermaßen.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. (Mell & Grance, 2011, S. 3)

In Abbildung 8 wird die Zusammenstellung der Eigenschaften und möglichen Implementierungen von Cloud Lösungen dargestellt.

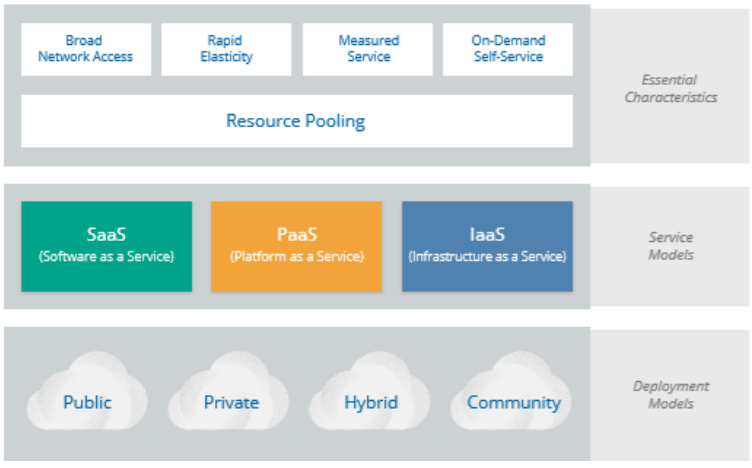

Abbildung 8 Cloudsysteme und ihre Eigenschaften (Cloud Security Alliance, 2017, S. 10)

Wie in der Definition beschrieben verfügt Cloud Computing über fünf wesentliche Merkmale. Diese wären folgende (Cloud Security Alliance, 2017, S. 10):

- **On-Demand Self-Service** bedeutet, dass ohne Interaktion des Anbieters benötigte Leistungen, je nach Bedarf angefordert werden können. Als Beispiel kann die Rechenleistung oder der Speicher angeführt werden.
- **Broad Network Access** bedeutet, dass die Services über das Netzwerk verfügbar sind und mit Standardressourcen zugegriffen werden kann.
- **Ressource Pooling** würde übersetzt Ressourcenzusammenlegung bedeuten. Dies bedeutet, dass der Provider eine Architektur verwendet, mit der, an einer oder weniger Stellen, Ressourcen gebündelt werden. Das bedeutet, dass je nach Nachfrage in unterschiedlicher Ausprägung, virtuelle Ressourcen individuell und dynamisch dem Nutzer zugewiesen werden. Weiters kann in den meisten Fällen der Nutzer auch keinen Einfluss darauf nehmen. Durch die Nichtnachvollziehbarkeit kommt ein Gefühl der Standortunabhängigkeit auf.
- **Rapid Elasticity** bedeutet die Fähigkeit flexibel und schnell auf Anforderungen reagieren zu können.
- **Measured Service** bedeutet, dass Cloud-Systeme die Ressourcennutzung automatisch steuert und optimiert. Weiters ist die Nutzung transparent für den Provider und die Nutzer, da diese überwacht, kontrolliert und darüber ein Reporting durchgeführt wird.

Zusätzlich zu den Charakteristika, die das National Institute of Standards and Technology (NIST) anführt, listet die ISO/IEEC 17788 noch die Mandantenfähigkeit („multitenancy“) auf. (Cloud Security Alliance, 2017, S. 10)

5.2 Modelle von Cloud Lösungen

Wie in der Definition in Abbildung 8 dargestellt, gibt es verschieden Modelle von Cloud Lösungen. Anschließend eine Aufstellung und kurze Beschreibung der verschiedenen Modelle und die Verantwortungsverteilung zwischen Provider und Nutzern (Cloud Security Alliance, 2017, S. 11 - 12).

- **Software as a Service**
  damit wird die Verwendung einer Applikation verstanden, die in einer Cloud Infrastruktur läuft und die Verwaltung und Wartung dem Cloud Provider unterliegt. Bei diesem Modell ist der Cloud Provider für alle sicherheitsrelevanten Themen verantwortlich, da der Anwender nur einen Zugang hat und die Verwendung der Software steuern kann (Cloud Security Alliance, 2017, S. 20).
- **Plattform as a Service**
  darunter wird die Bereitstellung von Infrastruktur und Werkzeugen (Programme und Applikationen) zum Entwickeln und Betreiben von eigenen Applikationen verstanden.
  Bei dieser Form ist der Cloudprovider für die sicherheitsrelevanten Themen bezüglich der Plattform und der Nutzer für alles andere verantwortlich. Als Beispiel kann die Verwendung einer Datenbank genannt werden.
  Der Cloud Provider ist verantwortlich für die grundlegende Sicherheit, Patches und die Grundkonfiguration und der NutzerInnen für die Sicherheitsfunktionen der Datenbank, der Kontenverwaltung und möglicherweise sogar für die Authentifizierungsmethode (Cloud Security Alliance, 2017, S. 20).
- **Infrastructure as a Service**
  ist die Bereitstellung von Infrastruktur. Management und Wartung liegt in der Verantwortung des Providers und die Nutzer haben die Kontrolle über eingesetzte Betriebssysteme, Speicher und Anwendungen. Der größere Teil der Verantwortung liegt in diesem Modell bei den Cloud Benutzern.
  Der Cloud Provider ist in diesem Fall nur für die grundlegende Sicherheit verantwortlich.

Als Beispiel kann angeführt werden, dass der Provider zwar seine IT-Systeme auf Angriffe überwacht, allerdings die Nutzer verantwortlich sind, ihre virtuellen Netze zu definieren und zu implementieren. (Cloud Security Alliance, 2017, S. 20).

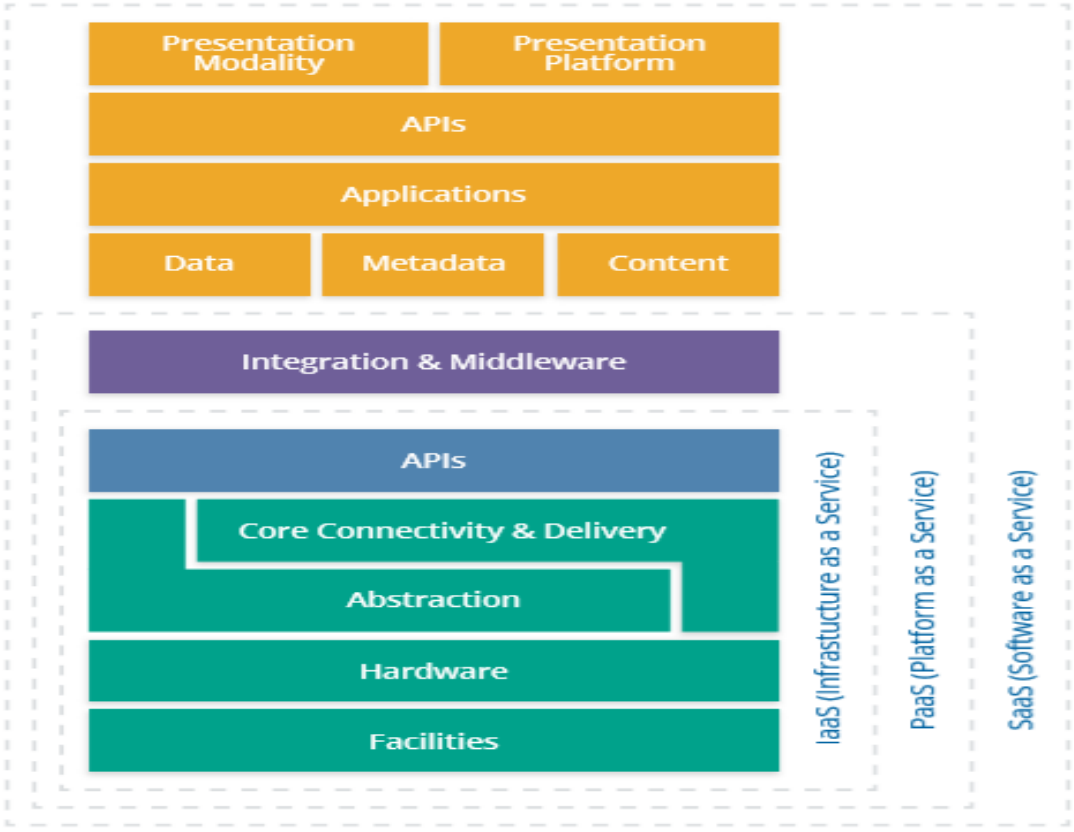

Abbildung 9 Darstellung Modelle von Cloud Computing (Cloud Security Alliance, 2017, S. 13)

5.3 Arten der Implementierung von Cloud Lösungen

Die Implementierung von Cloud-Lösungen kann auf vier verschiedene Arten erfolgen. Diese werden bezeichnet nach der Art der Anwender denen sie zu Verfügung gestellt wird. (Hammer, 2017, S. 9 - 11)

- **Private Cloud** ist die Bereitstellung von Infrastruktur ausschließlich für eine Organisation.
- **Community Cloud** ist die Bereitstellung von Infrastruktur für eine gemeinsame Verwendung in einer bestimmten Gemeinschaft von Verbraucherinnen und Verbrauchern.
- **Public Cloud** ist die Bereitstellung für die Öffentlichkeit. Es handelt sich um die wohl häufigste Form. In dieser Form ist durch die Verwendung von vielen Nutzerinnen beziehungsweise Nutzern eine individuelle Anpassung kaum möglich und dadurch ist die Entstehung von Skaleneffekten erst möglich.
- **Hybrid Cloud** ist eine Mischform aus den vorher genannten Implementierungsformen. In dieser Form können die Vorteile verschiedener anderen Implementierungsformen kombiniert werden. Allerdings steigt dadurch auch die Komplexität der Datentrennung.

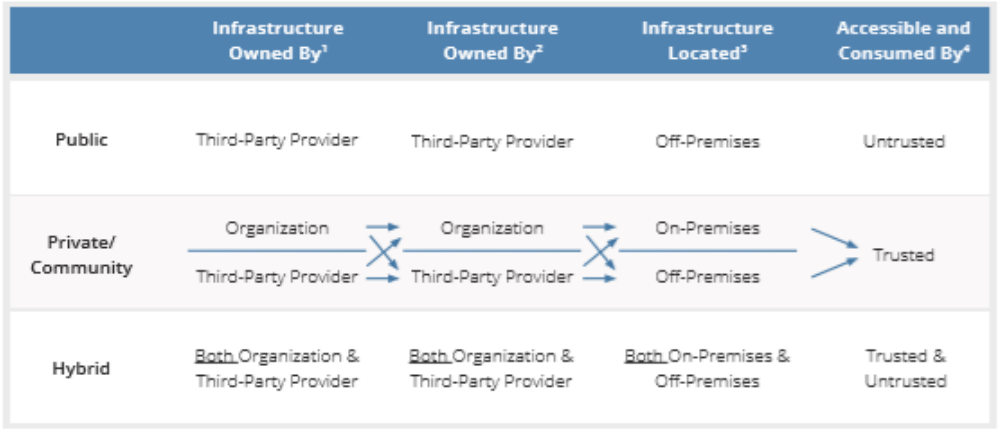

Abbildung 10 Darstellung Implementierungsart Cloud Systeme (Cloud Security Alliance, 2017, S. 12)

Da in der Forschungsfrage speziell die Implementierungsart Public Cloud angeführt wird, werden in den nächsten Kapiteln nur die Themen betrachtet, die sich speziell auf diese Implementierungsart beziehen.

5.4 Public Cloud

Die Public Cloud ist die einfachste Form aller Cloud Implementierungen. Die Nutzer kaufen je nach Bedarf Ressourcen, Plattformen oder Services bei Cloud Anbieter ein. Damit wird über Hardware des Anbieters Infrastruktur, Rechenleistung, Storage oder Anwendungen virtualisiert und zusammengefasst per Internet oder dedizierte Netzwerkanbindung zu Verfügung gestellt.

Das wiederum bedeutet, dass der Kunde nicht in den Betrieb und Sicherung involviert ist und auch keinen Besitz von Infrastruktur hat. Er hat nur Vereinbarungen zur Nutzung von Ressourcen und zahlt nach dem Verbrauch dieser (Red Hat, 2018).

Die Public Cloud hat eine Vielzahl von Vorteilen (Karlstetter & Luber, 2017).

- Einfache Installation und einfaches Setup der Services
- Kosten können als Betriebsausgaben und nicht als Kapitalausgaben verbucht werden.
- In der Regel gibt es auch eine höhere Verfügbarkeit der Infrastruktur als im eigenen Rechenzentrum
- Bereitstellung nahezu unbegrenzter Ressourcen ohne größere Verwaltungsverantwortlichkeiten und flexible Skalierbarkeit.
- Eine gesteigerte Agilität zwischen Entwicklungs- und Betriebsteams
- Bereitstellung nahezu unbegrenzter Ressourcen ohne größere Verwaltungsverantwortlichkeiten wie zum Beispiel Störungsbehebung.
- Anbieter implementieren moderne Sicherheitskonzepte und erhöhen die Sicherheit.

Allerdings gibt es bei der Benutzung von Public Clouds auch einige Nachteile, die beachtet werden müssen. Das Auslagern von Daten, beziehungsweise ihre Verwaltung und Verarbeitung durch einen Cloudprovider, bringt zahlreiche Risiken mit sich. Es kann zum Beispiel durch strenge gesetzliche Datenschutzregelungen in bestimmten Branchen untersagt sein, Daten an externe Dienstleister zu übertragen, wenn diese nicht den strengen Richtlinien der europäischen Datenschutzverordnung entsprechen.

5.5 Sicherheits-Risiken in Public Cloud Lösungen

Es gibt im Zusammenhang mit Public Cloud Lösungen einige Sicherheits-Risiken, die beachtet werden müssen (Schweinoch & Störtkuhl, 2015).

- Verletzung Vertraulichkeit und Integrität der Daten
  Da die Lokalisierung der Daten nicht mehr einfach möglich ist, muss der Schutz der Daten auf allen Ebenen (Infrastruktur, Plattform und Applikationsebne) gewährleistet sein. Eine ausreichende Zugriffskotrolle kann nur schwer umgesetzt werden. Weiters wäre es möglich, dass die Infrastruktur selbst angegriffen wird.

- Löschung von Daten
  Unter bestimmten Voraussetzungen (gesetzliche Bestimmungen) kann es möglich sein, dass Daten gelöscht werden müssen. Es besteht jedoch immer ein Restrisiko, dass die Daten nicht ausreichend, beziehungsweise vollständig, gelöscht werden, beziehungsweise ist es oftmals nicht lückenlos nachvollziehbar, wo die Daten überall gespeichert wurden.

- Ungenügende Mandantentrennung
  Es besteht die Gefahr, wenn eine unzureichende Mandantentrennung vorhanden ist, dass Dritte unautorisiert Daten einsehen können. Dies ist in Public Cloud Lösungen möglich, da keine physikalische Trennung erfolgt.

- Verletzung Compliance

  Da grundsätzlich nicht bekannt ist wo die Daten gespeichert beziehungsweise verarbeitet werden, ist durch verschiedene Gesetzgebungen möglich, dass Compliance Richtlinien verletzt werden. Dies ist allerdings eine der wichtigsten Anforderung an einen Public Cloud Provider.

- Verletzung Datenschutzgesetz

  Es kann die Aussage des vorigen Punktes herangezogen werden. Da nicht klar ist, wo und wie die Daten verarbeitet oder gespeichert werden, ist es auch nicht klar, ob die Gefahr von Datenschutzverletzungen bestehen.

- Insolvenz des Providers

  Im Falle einer Insolvenz des Cloudproviders, ist es Wahrscheinlich, dass die Infrastruktur an einen neuen Provider übergeben wird. In diesem Fall ist somit nicht sichergestellt, dass die Daten weiter vor nicht autorisierten Zugriff geschützt sind.

- Problematik der Subunternehmer

  Es besteht die Möglichkeit das der Public Cloud Provider bestimmte Leistungen an Subunternehmer abgibt und der Cloud Nutzer keinerlei Informationen darüber hat.

- Beschlagnahmung von Hardware des Providers

  Auch bei diesem Risiko ist es nicht sicher, ob die Daten vor unberechtigten Zugriff geschützt sind.

- Erpressungsversuche des Providers

  Die Gefahr von Erpressung steigt, da es mehr Personen mit Administratoren Rechten gibt. Es sind allgemein IT und auch speziell Angriffe wie zum Beispiel Ransomware zu erwähnen.

5.6 Anbieter von Public Cloud Lösungen

Es gibt viele Anbieter von Public Cloud Lösungen. In Abbildung 11 werden die größten Anbieter von Public Cloud Lösungen weltweit und nach Region dargestellt (Synergy Research Group, 2018).

Public Cloud Leadership by Region – Q1 2018

Rank	Worldwide	North America	EMEA Region	APAC Region	Latin America
Leader	AWS	AWS	AWS	AWS	AWS
#2	Microsoft	Microsoft	Microsoft	Alibaba	Microsoft
#3	Google	Google	Google	Microsoft	Google
#4	Alibaba	IBM	IBM	Google	Salesforce
#5	IBM	Salesforce	Salesforce	Tencent	IBM

Abbildung 11 Führende Public Cloud Anbieter (Synergy Research Group, 2018)

Die weiteren Analysen bezüglich Datenschutzgrundverordnung soll in Bezug auf Amazon Web Service, den in Europa größten Public Cloudanbieter, erfolgen.

5.7 Datenschutz in der Public Cloud

Es ist anzumerken, dass es eine große Palette von Services, die der Sicherheit dienen, in den Public Cloud Lösungen zu Verfügung stehen. In Abbildung 12 eine Darstellung und kurze Erklärung der angebotenen Security Services, die in der AWS Cloud angeboten werden (Amazon Web Services, Inc, 2018).

Service	Produkttyp	Beschreibung
AWS Artifact	Compliance-Berichte	AWS Artifact ist ein Portal, auf dem Benutzer bei Bedarf AWS Sicherheits- und Compliance-Dokumente (Auditartefakte) abrufen können.
AWS Certificate Manager	SSL-/TLS-Zertifikate	AWS Certificate Manager ist ein Service, mit dem Sie problemlos SSL-(Secure Sockets Layer-) und TLS-(Transport Layer Security-)Zertifikate bereitstellen und verwalten können.
Amazon Cloud Directory	Verzeichnis	Mit Amazon Cloud Directory können Sie flexible Cloud-Verzeichnisse für das Organisieren von Datenhierarchien in mehreren Dimensionen erstellen.
AWS CloudHSM	Schlüsselspeicherung und -verwaltung	Der AWS CloudHSM-Service unterstützt Sie mithilfe dedizierter Hardware-Sicherheitsmodul-(HSM-)Appliances beim Einhalten gesetzlicher, regulatorischer und vertraglicher Vorschriften für die Datensicherheit in der AWS Cloud.
Amazon Cognito	Benutzerregistrierung und -anmeldung	Mit Amazon Cognito können Sie die Registrierung und Anmeldung von Benutzern und die Zugriffskontrolle schnell und einfach Ihren Web- und mobilen Anwendungen hinzufügen.
AWS Directory Service	Verzeichnis	Mit AWS Directory Service für Microsoft Active Directory (Enterprise Edition), auch als AWS Microsoft AD bezeichnet, können Sie in der AWS Cloud für Ihre verzeichnisfähigen Verarbeitungslasten und AWS-Ressourcen ein verwaltetes Active Directory verwenden.
AWS Firewall Manager	WAF Management	AWS Firewall Manager ist ein Sicherheitsmanagementservice, der die zentrale Konfiguration und Verwaltung von AWS WAF-Regeln für Ihre Konten und Anwendungen vereinfacht.
Amazon GuardDuty	Gefahrenerkennung	Amazon GuardDuty ist ein verwalteter Gefahrenerkennungsservice, mit dem Sie Ihre AWS-Konten und -Workloads genauer und einfacher dauerhaft überwachen und schützen können.
AWS Identity and Access Management (IAM)	Zugriffssteuerung	Nutzen Sie AWS Identity and Access Management (IAM), um den Benutzerzugriff auf AWS Services zu steuern. Erstellen und verwalten Sie Benutzer und Gruppen und erteilen oder verweigern Sie Zugriffe.
Amazon Inspector	Sicherheitsbewertung	Amazon Inspector ist ein automatisierter Service für die Sicherheitsprüfung, der die Verbesserung von Sicherheit und Compliance von Anwendungen unterstützt, die auf AWS bereitgestellt werden.
AWS Key Management Service	Schlüsselspeicherung und -verwaltung	AWS Key Management Service (KMS) ist ein verwalteter Service, der Ihnen die Erstellung und Kontrolle der für die Datenverschlüsselung verwendeten Verschlüsselungsschlüssel erleichtert.
Amazon Macie	Sensible Datenklassifizierung	Amazon Macie ist ein durch maschinelles Lernen gesteuerter Sicherheitsservice, der vertrauliche Daten erkennt, klassifiziert und schützt.
AWS Organizations	Verwaltung mehrerer Konten	AWS Organizations bietet richtlinienbasierte Verwaltung für mehrere AWS-Konten. Mit Organizations können Sie Kontengruppen erstellen und anschließend Richtlinien für diese Gruppen anwenden.
AWS Shield	DDoS-Schutz	AWS Shield ist ein verwalteter Service, der auf AWS ausgeführte Webanwendungen vor Distributed Denial of Service (DDoS)-Angriffen schützt.
AWS Secrets Manager	Secrets-Management	AWS Secrets Manager ermöglicht es Ihnen, Datenbankanmeldeinformationen, API-Schlüssel und andere geheime Informationen während ihres gesamten Lebenszyklus einfach durchzuwechseln, zu verwalten und abzurufen.
AWS Single Sign-On	Single Sign-On (SSO)	AWS Single Sign-On (SSO) ist ein Cloud-SSO-Service, der die zentrale Verwaltung des SSO-Zugriffs auf mehrere AWS-Konten und Geschäftsanwendungen erleichtert.
AWS WAF	Webanwendungs-Firewall	AWS WAF ist eine Webanwendungs-Firewall, die Ihre Webanwendungen vor verbreiteten Internet-Bedrohungen schützt, die die Verfügbarkeit der Anwendung oder die Sicherheit beeinträchtigen bzw. Ressourcen exzessiv belasten können.

Abbildung 12 Security Services AWS (Amazon Web Services Inc., 2018)

Aus den Informationen des Anbieters lässt sich schließen, dass die sicherheitstechnischen Voraussetzungen mit den Services des Anbieters grundsätzlich umsetzbar sind. Es soll nun einerseits, in den Experteninterviews die Möglichkeit der Verwendung dieser Sicherheits-Services abgefragt werden.

6. Technische und organisatorische Maßnahmen aus DSVGO in Bezug auf die Verwendung von Public Cloud Lösungen

In diesem Kapitel sollen die Maßnahmen ausgearbeitet werden, die notwendig sind, um eine Verwendung von Public Cloud Systemen, im Sinne der DSGVO sicher gestalten zu können. Diese Maßnahmen sind wie schon in Kapitel 3.3 angeführt, in technische, organisatorische und vertragliche Maßnahmen unterteilt.

6.1 technische Maßnahmen

Die Arten der Umsetzung der technischen Maßnahmen sind in der DSGVO, wie bereits in Kapitel 3.2.3 Prinzipien der DSGVO beschrieben, sehr auf die Grundprinzipien aufgebaut.

Hier nun diese Grundprinzipien bezogen auf die technischen Maßnahmen.

- Vertraulichkeit

  Es sind vor allem der Zugriffschutz, Zugang und Zutritt in physischer und virtueller Form anzuführen.

- Integrität

  Jegliche Änderung muss autorisiert und dokumentiert sein.

- Verfügbarkeit

  Die Daten müssen, wenn sie gebraucht werden, schnell und einfach verfügbar sein. Zusätzlich soll auch auf die Sicherung und Wiederherstellung der Daten Rücksicht genommen werden.

- Privacy by Default („datenschutzfreundliche Voreinstellung“)

  Es soll durch Voreinstellungen sichergestellt werden, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden.

  Es ist wie in Kapitel 3.2.3 Prinzipien der DSGVO auch die Datenminimierung beziehungsweise Sparsamkeit bei der Verwendung von personenbezogenen Daten gemeint.

- Privacy by Design („Datenschutz durch Technikgestaltung“)

  Vor der eigentlichen Datenverarbeitung sollten schon geeignete technische und organisatorische Maßnahmen getroffen werden.

Durch den Einsatz von Technik, die am aktuellen Stand der Technik ist und unter der Berücksichtigung der wirtschaftlichen Vertretbarkeit, sollte der angemessene Schutz gewährleistet sein.

In dieser Arbeit werden nun die technischen Maßnahmen auf mehrere Bereiche aufgeteilt, um mögliche detaillierte Beschreibungen der Maßnahmen evaluieren zu können.

Die Bereiche werden auf folgende Themen aufgeteilt.

- Zugriff
  - Authentifizierung
  - Benutzer und Rollenkonzept
- Datenübertragung
- Datenspeicherung, -sicherung und -wiederherstellung
- Netzwerk

6.2 organisatorische Maßnahmen

Die organisatorischen Maßnahmen sind einerseits, in der vertraglichen Gestaltung mit dem Cloudprovider, aber auch in der Unternehmensorganisation selbst zu sehen. Allerdings müssen die Änderung in der Unternehmensorganisation auch durchgeführt werden, wenn die IT-Infrastruktur in eigenen Rechenzentren betrieben wird. Aus diesem Grund werden diese nur kurz beschrieben und die vertraglichen Themen genauer dargestellt. Als notwendige Anpassungen in der Unternehmensorganisation sind vor allem personelle und organisatorische Anpassungen zu verstehen. Diese können auf folgende Bereiche aufteilt werden:

- Personelle Maßnahmen:
    - Regelung der Verarbeitungs-, Nutzungs- und Übermittlungsrechte
    - Einschränkungen für Lese-, Schreib- und Änderungsrechte
    - Berechtigung und Rollenzuweisung nach Erforderlichkeitsprinzip
    - Vertreterregelungen
    - Verpflichtung der Mitarbeiter auf Einhaltung des Datenschutzes
    - Schulungen zu DSGVO und IT-Sicherheit
- Organisatorische Maßnahmen
    - Anpassungen der Prozessabläufe für die Bewahrung der Betroffenenrechte und Grundsätze. Vor allem für die Verpflichtungen des Datenverarbeiters und die Rechte des Betroffenen wie in Kapitel 3.2.8. beschrieben.
        - Informationspflicht
        - Einwilligungspflicht
        - Auskunftsrecht
        - Berichtigungsrecht
        - Recht auf Löschung (Recht auf Vergessen werden)
        - Recht auf Einschränkung der Verarbeitung
        - Recht auf Wiederspruch

Anpassungen bezüglich interner Unternehmensorganisation

- Eintritts- und Austrittsprozesse von Mitarbeitern (Zugriff)
- Aufzeichnung und Dokumentation aller Zugriffe und Änderungen
- Aufbau Notfallorganisation und miteinbeziehen des Cloud Providers

6.3 vertragliche Maßnahmen bezogen auf den Public Cloud Provider

Die vertraglichen Inhalte können in vier grundsätzliche Blöcke gegliedert werden (BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2014, S. 4).

- Die Cloud Leistungen beinhalten Leistungsbeschreibung und Nutzungsumfang.
- Service Levels beschreiben die Leistungsgüte und Folgen bei unzureichender Leistungserbringung.
- Ein weiterer Block sind die kaufmännischen Inhalte, wie Vergütung, Laufzeit, Vergütungsparameter und deren Anpassung bei Veränderung.
- Sonstige Regelungen beinhalten zum Beispiel die Gewährleistung, Haftung, Rechtswahl, Datenschutz und Verzugsregelungen.

Laut Gesetz müssen Verträge, je nach Art, einen gewissen Mindestinhalt haben. In Bezug auf Public Cloud Lösungen, würde das allerdings nicht praxisgerecht und nicht den Anforderungen von Providern und Dienstleistungsnutzern entsprechen.

Hier ein Ansatz der notwendigen Inhalte eines Cloud Computing Vertrages (BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2014, S. 7).

- Bezeichnung der Vertragspartner in genauer Form (Handelsregisterauszug)
- Vertragsgegenstand
    - Bezeichnung
    - Service Level
    - Weitere Leistungspflichten (zum Beispiel Backup, Helpdesk,..)
- Art und Umfang der Nutzung (beinhaltet auch Nutzungsrechte)
- Nutzungsvoraussetzungen sollten als Beispiel den Übergabepunkt der Leistung definieren. Es wäre als Beispiel der Internetzugang des Nutzers für die Erreichung des Übergabepunktes des Providers zu nennen, aber möglicherweise auch eine VPN Verbindung zur Absicherung der Datenübertragung.
- Mitwirkungspflichten des Kunden beinhalten möglicherweise Informationen, die der Provider braucht, um die nutzungsmäßige Abrechnung durchzuführen.
- Vergütungs- und Zahlungsmodalität
- Vertragslaufzeit
- Gewährleistung für Sach- und Rechtsmängel
- Haftung
- Datenschutz
- Es sollte zu Vertraulichkeit und Datensicherheit ein Mindestschutzniveau im Vertrag verankert sein. Als Beispiel könnte eine Verhinderung der Vermischung von Daten durch physische Trennung oder die Notwendigkeit von Zugriffkontrollen genannt werden. Es sollte auch die Überprüfung der Einhaltung von Sicherheitsstandards und deren Kontrolle angeführt sein.

  Als Referenz kann der in Kapitel 6.4 beschriebene Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung ISO/IEC 27018 herangezogen werden.

- Einschaltung von Subunternehmern und die Vereinbarung der Regelungen für Governance und Notfall-Management mit diesen.
- Regelung für Transition und Exit Management
- Gerichtsstand
- Rechtswahl
- Vertragssprache

Da viele Maßnahmen, technische und organisatorische, in der Verantwortung des Cloud Providers liegen und diese nur sehr schwer vom Cloud Nutzer mittels Audits überprüfbar sind, ist es notwendig diese vertraglich festzulegen. Hierzu könnte auf eine unabhängige Überprüfung der Umsetzung nach entsprechenden Normen durch unabhängige Prüfer gefordert werden.

Es gibt zu diesem Thema einige Normen beziehungsweise Leitfäden. Anschließend eine kurze Auflistung und Erklärung zu den bekanntesten und am meisten Angewandten.

BSI Anforderungskatalog Cloud Computing(C5):

Dieser Anforderungskatalog beinhaltet die Mindeststandards, auf die ein Cloud Anbieter verpflichtet werden sollte. Dieser Anforderungskatalog wurde vom Bundesamt für Sicherheit in der Informationstechnik in Deutschland herausgegeben. Die Grundlage sind einige nationale (Deutschland) und internationale Standards, es sind vor allem die ISO/IEC 27001, CSA und der BSI IT-Grundschutz anzuführen (Bundesamt für Sicherheit in der Informationstechnik – BSI, 2019, S. 1 -17).

CSA Cloud security alliance:

Die Cloud Security Alliance (CSA) ist eine gemeinnützige Organisation mit folgendem Ziel. "Förderung des Einsatzes bewährter Methoden zum Gewährleisten von Sicherheit beim Cloud Computing und zum Informieren über die Einsatzmöglichkeiten von Cloud Computing zum Absichern aller anderen Formen der Datenverarbeitung."

Sie betreibt Zertifizierungsprogramme für Cloud Anbieter wie CSA Security, Trust & Assurance Registry (STAR). Dieses aus einem dreistufigen Verfahren, das von Self-Assessment über Prüfung durch Dritte und kontinuierliche Überwachung, besteht (Cloud Security Alliance, 2019).

ISO/IEC 27018:2014 Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung:

Dieser Leitfaden setzt auf die ISO/IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen“ und „IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management (ISO/IEC FDIS 27002:2013)“ auf und wurde entwickelt um Organisationen beim Implementieren und Umsetzen von Maßnahmen zum Schutz personenbezogener Daten, speziell in der Form Datenverarbeitung in Public Cloud Systemen, zu unterstützen. (DIN Deutsches Institut für Normung e.V., 2017)

Die großen Public Cloud Anbieter, wie zum Beispiel AWS oder Microsoft, sind nach den gängigsten Normen beziehungsweise Frameworks zertifiziert beziehungsweise überprüft. Die Zertifizierung nach ISO 27001, ISO 27017 und ISO 27018 sind ebenfalls enthalten. Eine genauer Auflistung kann von AWS auf ihrer Homepage zu Verfügung gestellten Whitepaper (Amazon Web Service, 2017, S. 7 - 13) oder von Microsoft auf ihrer Homepage (Microsoft Corporation , 2018) nachgelesen werden.

Da die ISO 27018 ein weltweit anerkannter Leitfaden ist und dieser speziell auf den Schutz bei der Verarbeitung von personenbezogenen Daten eingeht, wird in den nächsten Kapiteln vertieft auf diesen eingegangen und für die Erstellung des Frameworks verwendet.

6.4 Inhalte des Leitfadens zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung ISO/IEC 27018

Spezifische Anleitungen und Informationen für die Umsetzung einer Cloud Lösung in Bezug auf die DSGVO sind der Inhalt dieser Norm. Wie schon in Kapitel 6.3 erwähnt, ist diese aufbauend auf die Normen ISO/IEC 27001 & ISO/IEC 27002. In den nächsten Kapiteln werden nun die besonderen Ziele und Maßnahmen auf die Verwendung von Public Cloud Lösungen beschrieben.

6.4.1 Informationssicherheitsrichtlinien

Security Policies sollten definiert sein, die vom Management freigegeben, veröffentlicht und an die Mitarbeiter, Lieferanten und andere relevante externe Beteiligten, kommuniziert sind. Eine genaue Auflistung ist in der ISO 27002 im Kapitel 5.1.1 dargestellt (DIN Deutsches Institut für Normung e. V, 2014, S. 10 - 12). In Bezug auf Public Cloud sind noch folgende besonderen Maßnahmen zusätzlich zu erwähnen (DIN Deutsches Institut für Normung e.V., 2017, S. 14 - 15).

- Die Richtlinien sollen eine Aussage beinhalten, dass die geltenden Gesetze zum Schutz der personenbezogenen Daten zwischen Provider und Nutzer vereinbarten Vertragsbedingungen unterstützen und als Verpflichtung angesehen werden.
- Die Verantwortlichkeiten sollen unter Berücksichtigung der Art des betreffenden Cloud-Dienstes (z. B. IaaS-, PaaS- oder SaaS-Dienst, Kategorie der Cloud-Computing-Referenzarchitektur) eindeutig festgelegt sein.
- Der Vertrag soll sicherstellen, dass der Provider verpflichtet wird, die Einhaltung zu unterstützen und zu verwalten. Als Beispiel kann festgelegt werden, dass die Umsetzung einer internationalen Norm (z.B. ISO/IEC 27002) entsprechen muss und dies von unabhängiger Seite überprüft werden soll.

6.4.2 Organisation der Informationssicherheit

Die organisatorischen Maßnahmen bezüglich Informationssicherheit in Bezug auf Public Cloud sind die gleichen Ziele wie in „IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management (ISO/IEC FDIS 27002:2014) unter Kapitel 6.1. (DIN Deutsches Institut für Normung e.V., 2017, S. 12 - 14). Als Erweiterung sollte der Public Cloud Provider eine Anlaufstelle bekannt geben, die als Ansprechperson bezüglich Datenschutzes relevanter Themen dient (DIN Deutsches Institut für Normung e.V., 2017, S. 15).

6.4.3 Personalsicherheit

In diesem Bereich sind es vor allem die Ziele, die in ISO/IEC FDIS 27002:2013 Kapitel 7.1. und 7.2. dargestellt sind. Die beschriebenen Maßnahmen müssen sicherstellen, dass alle betroffenen Mitarbeiter über Folgen der Verfehlungen gegen die Regeln und Verfahren zu Datenschutz oder Informationssicherheit (DIN Deutsches Institut für Normung e. V, 2014, S. 18 - 23). In Bezug auf Public Cloud vor allem auch diejenigen, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten stehen. Wobei es sich um die Folgen für Unternehmen, Mitarbeiter und Betroffene handelt (DIN Deutsches Institut für Normung e.V., 2017, S. 16).

Erwähnenswert sind in diesem Zusammenhang auch die Teils empfindlichen Geldstrafen, wie in Kapitel 3.2.9 beschrieben, die Unternehmen von Datenschutzbehörden auferlegt werden können. Diese können für Unternehmen existenzbedrohend werden.

6.4.4 Verwaltung der Werte

Dieser Bereich wird in der ISO/IEC FDIS 27002:2013 unter Kapitel 8 abgebildet und es sind in Bezug auf Public Cloud keine zusätzlichen Maßnahmen relevant (DIN Deutsches Institut für Normung e. V, 2014, S. 23 - 30).

6.4.5 Zugangsprüfung

Der Bereich Zugangsprüfung ist einer der umfangreichsten und kritischsten Bereiche und wird in der der ISO/IEC FDIS 27002:2013 unter Kapitel 9 bearbeitet (DIN Deutsches Institut für Normung e.V., 2017, S. 30 - 41). Dazu werden nun die Bereiche kurz dargestellt, die Besonderheiten bezüglich Public Cloud dargestellen.

- Benutzerzugangsverwaltung

  Es ist je nach Public Cloud Architektur möglich, dass der Dienstleistungskunde für Teile oder Gesamt für das Zugangsmanagement verantwortlich ist und deshalb sollte der Public Cloud Provider den Dienstleistungskunden ermöglichen die Zugangsrechte für die Nutzer selbst zu verwalten (DIN Deutsches Institut für Normung e.V., 2017, S. 17).

  Als besonders erwähnenswert ist folgender Unterpunkt angeführt.
  - Registrierung und Deregistrierung von Benutzern

    Die Durchführung bei Kompromittierung der Benutzerkontrolle (z.B. unbeabsichtigte Offenlegung) sollte unbedingt mit einbezogen werden. Ein weiterer Punkt ist die Regelmäßigkeit der Überprüfung auf ungenutzte Zugangsdaten (DIN Deutsches Institut für Normung e.V., 2017, S. 17).

- Zugangssteuerung für Systeme und Anwendungen
  - Sichere Anmeldeverfahren

    Der Public Cloud Provider muss sichere Anmeldeverfahren, für alle von Dienstleistungskunden beantragten Nutzer Konten, zu Verfügung stellen. Als Beispiel wäre die zwei Faktoren Authentifikation zu erwähnen (DIN Deutsches Institut für Normung e.V., 2017, S. 18).

6.4.6 Kryptographie

- Kryptographische Maßnahmen
    - Richtlinie zum Gebrauch von kryptographischen Maßnahmen

      Der Public Cloud Provider sollte den Dienstleistungskunden klar darstellen, wie und wann er kryptographische Verfahren anwendet, um die personenbezogenen Daten zu schützen. Es ist möglich, dass es gesetzlich notwendig ist, kryptographische Verfahren zum Schutz von besonderen Arten von personenbezogener Daten zu verlangen (DIN Deutsches Institut für Normung e.V., 2017, S. 19).

      Aus Sicht des Autors ist es ein unbedingtes Muss kryptographische Verfahren bezüglich Speicherung, Übertragung und Sicherung von Daten anzuwenden.

6.4.7 Physische und umgebungsbezogene Sicherheit

- Geräte und Betriebsmittel
    - Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

      Es sollte darauf geachtet werden, dass zur sicheren Entsorgung und Wiederverwendung von Speichermedien, wo nicht klar ist, ob personenbezogene Daten vorhanden sind, diese gleich behandelt werden wie wenn dies der Fall wäre (DIN Deutsches Institut für Normung e.V., 2017, S. 20).

6.4.8 Betriebssicherheit

- Betriebsabläufe und -verantwortlichkeiten
    - Trennung von Entwicklungs-, Test- und Betriebsumgebungen

      Dabei ist besonders zu achten, ob die Verwendung von personenbezogenen Daten für Tests notwendig ist, wenn es so ist, müssen dazu Maßnahmen gesetzt werden, um die zu erwartenden Risiken zu minimieren. Eine sinnvolle Maßnahme wäre es die Daten zu

anonymisieren, da für Tests in den meisten Fällen keine realen Daten notwendig sind (DIN Deutsches Institut für Normung e.V., 2017, S. 21).

- Datensicherung
  - Sicherung von Informationen

    Ein Dienstleistungsnehmer, der eine Dienstleistung auf Basis Public Cloud Computing nutzt, wird zusätzliche Verfahren zur Datensicherung außerhalb des physischen Standorts des Public Cloud Providers zum Schutz seiner Daten erwägen. Es soll damit sichergestellt werden, dass bei einem Störereignis, die Datenverarbeitung weiter durchgeführt werden kann, beziehungsweise die rasche Wiederherstellung der Funktion gewährleistet ist. Diese Verantwortungen können beim Dienstleistungsnehmer liegen, aber auch Public Cloud Provider bieten diese Dienste an. In diesem Fall müssen von Seiten des Providers klare Informationen über die Leistung bezüglich Sicherung und Wiederherstellung der Daten vorliegen. Dazu sollte es Verfahren geben, die in einem definierten Zeitraum die Wiederherstellung ermöglichen und die in regelmäßigen Abständen überprüft werden (DIN Deutsches Institut für Normung e.V., 2017, S. 21-22).

    Ein weiterer Punkt ist, dass die Daten beziehungsweise die Sicherungskopien der Daten auch von Unterauftragsnehmern verarbeitet beziehungsweise gespeichert werden können und diese daher ebenfalls zur Einhaltung verpflichtet werden müssen.

    Es ist auch notwendig, dass die Anforderung der ordnungsgemäßen Löschung und Vernichtung von Sicherungskopien von personenbezogenen Daten umgesetzt ist (DIN Deutsches Institut für Normung e.V., 2017, S. 21 - 22).

- Protokollierung und Überwachung
  - Ereignisprotokollierung

    Die Ereignisprotokolle sollten über einen definierten Prozess in regelmäßigen Abständen auf Unregelmäßigkeiten überprüft und daraus Abhilfemaßnahmen vorgeschlagen werden.

    In den Protokollen sollten folgende Aktion und Informationen gespeichert werden, die in Bezug auf personenbezogenen Daten stehen.

      - Wurden personenbezogene Daten geändert (hinzugefügt, geändert oder gelöscht)?
      - Wenn ja, wer hat sie geändert?

    Der Public Cloud Provider sollte zusätzlich Kriterien festlegen, ob, wann und wie die Protokolldateien den Dienstleistungskunden zu Verfügung gestellt werden. Der Provider muss sicherstellen, dass der Dienstleistungskunde nur auf die Daten Zugriff hat oder nur diese zu Verfügung gestellt bekommt, die ihn persönlich betreffen (DIN Deutsches Institut für Normung e.V., 2017, S. 22).

  - Schutz der Protokollinformation

    Der Public Cloud Provider sollte Maßnahmen festlegen, in denen sichergestellt wird, dass die protokollierten Daten nur für die vorgesehenen Zwecke verwendet werden.

    Weiters sollte eine automatisiertes Verfahren zur Löschung dieser Daten innerhalb eines festgelegten und dokumentierten Zeitraums eingeführt werden (DIN Deutsches Institut für Normung e.V., 2017, S. 22 - 23).

6.4.9 Kommunikationssicherheit

- Informationsübertragung
    - Richtlinien und Verfahren zur Informationsübertragung

      Wenn physische Datenträger zur Datenübertragung von personenbezogenen Daten eingesetzt werden, sollte eine Protokollierung des Ein- und Ausgangs der physischen Datenträgern eingeführt werden. In diesem sollten mindestens der Datenträgertyp, der autorisierte Sender/Empfänger, das Datum und die Uhrzeit und die Anzahl der Datenträger dokumentiert werden. Der Dienstleistungsnutzer sollte zusätzliche Maßnahmen (z.B. Verschlüsselung) einführen um den alleinigen Zugriff am Bestimmungsort sicherzustellen (DIN Deutsches Institut für Normung e.V., 2017, S. 23 - 24).

    - Vertraulichkeits- oder Geheimhaltungsvereinbarungen

      Es muss sichergestellt sein, dass alle Personen die unter Aufsicht des Public Cloud Providers Zugriff auf personenbezogene Daten haben, zur Geheimhaltung verpflichtet sind (DIN Deutsches Institut für Normung e.V., 2017, S. 24).

6.4.10 Handhabung von Informationssicherheitsvorfällen

- Handhabung von Informationssicherheitsvorfällen und Verbesserungen

  In diesem Bereich wird es notwendig sein, dass der Public Cloud Provider mit den Dienstleistungsnutzer, bei der Handhabung von Informationssicherheitsvorfällen und der Umsetzung von Verbesserungen zusammenarbeitet. Es wird dazu die Ausübung von verteilten Rollen notwendig sein (DIN Deutsches Institut für Normung e.V., 2017, S. 24 - 25).

    - Verantwortlichkeiten und Verfahren

      Um einen möglichen Bruch der Vertraulichkeit, Integrität oder Verfügbarkeit von personenbezogener Daten bei einen Informationssicherheitsvorfall festzustellen, sollte eine Überprüfung

durch den Public Cloud Provider als Teil der Handhabung von Informationssicherheitsvorfälle festgelegt sein (DIN Deutsches Institut für Normung e.V., 2017, S. 24 - 25).

6.4.11 Informationssicherheitsaspekte des Managements zur Aufrechterhaltung des Geschäfts im Krisenfall

Dieser Bereich wird in der ISO/IEC FDIS 27002:2013 unter Kapitel 17 abgebildet und es sind in Bezug auf Public Cloud keine zusätzlichen Maßnahmen relevant (DIN Deutsches Institut für Normung e. V, 2014, S. 93 - 95).

6.4.12 Regelkonformität

- Einhaltung von rechtlichen und vertraglichen Anforderungen

Dazu sollte vom Public Cloud Auftragsbearbeiter festgelegt werden, in welchen Ländern die personenbezogenen Daten gespeichert werden können und dürfen. Deshalb ist es wichtig, dass die genauen gesetzlichen Bestimmung definiert und die möglichen Speicherorte vertraglich vereinbart sind. Bei Änderungen sollte der Dienstleistungskunde zeitgerecht informiert werden, um wenn notwendig die Möglichkeit zu haben, diese Änderungen abzulehnen oder den Vertrag zu kündigen (DIN Deutsches Institut für Normung e.V., 2017, S. 96 - 99).

- Überprüfungen der Informationssicherheit
    - Unabhängige Überprüfung der Informationssicherheit

      Da es für die Dienstleistungskunden praktisch unmöglich ist den Public Cloud Provider in Audits direkt zu überprüfen, sollte der Public Cloud Provider schon vor dem Beginn der Zusammenarbeit, für die gesamte Dauer der Laufzeit ,eine von einer unabhängigen Stelle ausgestellte Bestätigung vorweisen, dass der Provider Maßnahmen zur Sicherstellung von Informationssicherheit und Verfahren zur gesetzeskonformen Umsetzung von der Bearbeitung von personenbezogener Daten umgesetzt hat (DIN Deutsches Institut für Normung e.V., 2017, S. 99 - 100).

7. Entwurf eines Frameworks zur Überprüfung der DSGVO konformen Umsetzung in Public Cloud Lösungen

In diesem Framework sollte die Auswahl des Public Cloud Providers und die notwendigen Maßnahmen (vertraglich, organisatorisch und technisch) für die Umsetzung abgedeckt sein. Die Checklisten werden offene und geschlossene Fragen beinhalten. Die genauen Inhalte dieser Checklisten werden in Folge der Interviews spezifiziert und erstellt. Des Weiteren müssen auch Verknüpfungen zu bestehenden Normen und Leitfäden bezüglich IT-Sicherheitsmanagement implementiert werden.

Es muss für ein Framework zur Überprüfung der DSGVO konformen Umsetzung in Public Cloud Lösungen einerseits auf die Arten der IT-Lösungen in der Public Cloud Rücksicht (wie zum Beispiel Storage, Network, Server, Backup) genommen werden und andererseits auf die organisatorischen Anpassungen und die vertraglich notwendigen Inhalte bezüglich der Cloud Anbieter. Ein weiterer Aspekt, der beachtet werden muss, ist wie in Kapitel 5.2 Modelle von Cloud Lösungen beschrieben, das Modell der Cloud Lösung (IaaS, PaaS und SaaS).

Wie in der Studie von KPMG und Bitkom Research beschrieben, nutzen 47 Prozent der Unternehmen technische Services wie Datenspeicher oder Rechenleistung (Infrastructure as a Services) in Public Cloud Umgebungen (bitkom research GmbH, 2017). Da die Versicherungskernprozesse zu meist mit eigens entwickelten Applikationen betrieben werden und die zu verwendeten Services im Bereich IaaS anzusiedeln sind, werden die zu erarbeiteten Maßnahmen und Checklisten speziell für diese Model entworfen, beziehungsweise beschrieben.

Wichtig ist zu diesem Framework anzumerken, dass rein die in Zusammenhang mit Public Cloud Lösungen relevanten Aspekte abgedeckt werden. Die Aspekte zur grundsätzliche IT-Sicherheit werden durch die Standard Modelle der ISO 27001 & 27002 oder den BSI IT-Grundschutz abgebildet.

7.1 Grobentwurf Checkliste zur Auswahl des Public Cloud Providers

In dieser Checkliste sollen vor allem Themen abgehandelt werden, die sich auf die Auswahl eines möglichen Providers beziehen. In diesem Bereich sollte es möglich sein, eine Wertung der Provider zu erstellen. Ausschlaggebend wären aus Sicht des Autors, die Referenzen der schon umgesetzten Lösungen. Es kann davon ausgegangen werden, dass wenn renommierte große Firmen Lösungen bei diesem Provider umgesetzt haben, dieser diese Lösungen in dementsprechender Qualität zu liefern im Stande ist. Allerdings sollte auch ein Augenmerk darauf gelegt werden welche Services von diesen Unternehmen genutzt werden.

Neben dieser Bewertung sollten noch folgende Punkte erfragt beziehungsweise bewertet werden.

- Welche Modelle bietet der Provider an?
- Welche Referenzen gibt es für diese Modelle?
- Gibt es Zertifizierungen, beziehungsweise Überprüfungen von Dritten zu den Services, die bezogen werden sollen? Als Beispiel könnten die in Kapitel 6.3 angeführten Leitfäden, beziehungsweise Normen herangezogen werden.
- Recht, beziehungsweise Gerichtstand kann vereinbart werden, beziehungsweise entspricht den Anforderungen.
- Ermittlungsbefugnisse und Offenbarungspflichten entsprechen den geforderten Anforderungen.
- Lokationen der Datenspeicherung, beziehungsweise Verarbeitung sind vereinbar oder entsprechen den geforderten Anforderungen.
- Geschäftsbedingungen, Regelungen zur Nutzung und Weitergabe von Daten sind vorhanden und entsprechen den geforderten Anforderungen.
- Gibt es auf dem aktuellen Stand der Technik befindliche Verschlüsselungsverfahren für Datenspeicherung und -übertragung?
- Gibt es eine den Stand der Technik entsprechende Berechtigungsvergabe und Authentifizierungsregeln (zum Beispiel Passwort Mindestvoraussetzungen)?

- Gibt es Regelungen bezüglich jeglicher Änderungen des Services (Changemanagement)?
- Gibt es Regeln bezüglich Beendigung, beziehungsweise Auflösung der Zusammenarbeit?
- Gibt es beziehungsweise können Regeln zur Datenrückgabe und Löschung vereinbart werden?

7.2 Grobentwurf Checkliste zu den vertraglichen Inhalten

Diese Checkliste wird sich vor allem auf die Inhalte, wie sie in Kapitel 6.3 vertragliche Maßnahmen bezogen auf den Public Cloud Provider beschrieben sind beziehen.

Einige Fragen, beziehungsweise Hinweise werden sich allgemein auf die Vertragsinhalte beziehen und andere speziell auf die Art der Public Cloud Modells (IaaS, PaaS, SaaS). Wie in Kapitel 7 Entwurf eines Frameworks zur Überprüfung der DSGVO konformen Umsetzung in Public Cloud Lösungen angeführt, werden in dieser Arbeit in den Maßnahmen und Checklisten nur die IaaS relevanten Themen eingearbeitet.

7.3 Grobentwurf Checkliste zu den notwendigen organisatorischen Maßnahmen (Prozesse)

Bei dieser Checkliste sollten alle Änderungen und Maßnahmen abgeprüft werden, die sich einerseits für die Implementierung von notwendigen Einführungen von Prozessen und Verantwortlichkeiten drehen.

Dabei wären zum Beispiel die Rechte und Pflichten durch die DSGVO wie in Kapitel 3.2.8 Rechte der betroffenen Person erwähnt und andererseits auch die notwendigen Kontrollprozesse, ob diese auch regelmäßig überprüft und verbessert werden.

Ein Beispiel wäre das Verarbeitungsregister, siehe Kapitel 3.2.6., wo überprüft werden muss, ob es eingeführt wurde und aber auch ob es sich am aktuellen Stand befindet. Grund dafür sind technische und organisatorische Änderungen, die ständig in einem Unternehmen vorkommen.

Es sollte in dieser Checkliste ebenfalls einen allgemeinen Teil geben und einen speziell auf die Art der Public Cloud Modells (IaaS, PaaS, SaaS) und wie in Kapitel 7 Entwurf eines Frameworks zur Überprüfung der DSGVO konformen Umsetzung in Public Cloud Lösungen angeführt in den Maßnahmen und Checklisten ebenfalls nur die IaaS relevanten Themen eingearbeitet.

7.4 Grobentwurf Checkliste für notwendige technische Maßnahmen

Der Inhalt dieser Checkliste wird sich auf den Schwerpunkt technische Umsetzung von Maßnahmen beziehen. Es soll überprüft werden, ob alle notwendigen Maßnahmen dem technischen aktuellen Stand entsprechen und den notwendigen Schutz bieten. Auch in diesem Bereich wird es notwendig sein zu überprüfen, ob die Kontrollprozesse zur regelmäßigen Überprüfung durchgeführt werden.

Ein Beispiel wäre die Verschlüsselung der Datenübertragung. Ist diese am aktuellen Stand der Technik? Überprüfbar wäre dies zum Beispiel, über das österreichische Informationssicherheitshandbuchs, beziehungsweise der Ausgaben der technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik in Deutschland.

Auch in dieser Checkliste wird es einen allgemeinen und einen speziellen Teil, bezogen auf das Modell, geben.

8. Methode

In diesem Kapitel wird erläutert mit welcher Methode, das aus dem theoretischen Teil der Arbeit geformte Framework, überprüft und fertiggestellt wird.
Der Aufbau des Frameworks wird Spezialisten aus dem Bereich IT-Security und Datenschutz vorgestellt und danach mit einem erarbeiteten Leitfaden gestützten Interview auf Vollständigkeit und Relevanz abgefragt. Dazu werden als erstes Informationen bezüglich der Erfahrung, der Inhalte und wichtigsten Punkte zu Datenschutzgrundverordnung, IT Security und Public Cloud abgefragt. Das Framework wird als letzter Punkt in diesen Interviews vorgestellt. Es sollen dadurch vor allem fehlende Aspekte gefunden und möglicherweise nicht notwendige Teile entfernt werden.

Folgende Inhalte sollen von den Experten aus dem Bereich IT-Security, Datenschutz und Public Cloud abgefragt werden.

- Wissen und Erfahrung zu Datenschutzgrundverordnung und daraus entstehende Maßnahmen
    - Umsetzung der DSGVO in Unternehmen
    - Erfahrung und Kernpunkte in der Evaluierung der Daten
    - Erfahrung und Kernpunkte in der Evaluierung des Schutzbedarfs der Daten
    - Erfahrung und Kernpunkte in der Erstellung Verarbeitungsregister
- Wissen und Erfahrung zu IT Sicherheit und daraus entstehende Maßnahmen
    - Integrität, Verfügbarkeit und Vertraulichkeit von Daten
    - Datenspeicherung, -sicherung, -wiederherstellung
    - Datenübertragung
    - Netzwerksicherheit
    - Zugriffschutz, Berechtigungskonzept
    - Notwendige weitere Maßnahmen bezüglich DSGVO

- Wissen und Erfahrung zu Public Cloud und daraus entstehende Maßnahmen
    - Allgemeiner Informationsstand zu Public Cloud
    - Datenschutz in der Public Cloud
    - Zugriffssicherheit in der Public Cloud
    - Integrität, Verfügbarkeit und Vertraulichkeit der Daten in der Public Cloud
    - Standort
    - Vertragsinhalte

9. Experten Interviews

Die Experteninterviews werden in inhaltlich schematischer Form transkribiert (Dresing & Pehl, 2018, S. 20 - 22). Das bedeutet, dass diese wörtlich transkribiert werden allerdings nicht lautsprachlich. Die Dialektsprache wird so gut wie möglich ins Hochdeutsche übersetzt und es werden diverse Satzbrüche, Stottern und Wortdoppelung ausgelassen. Nicht verständliche Aussagen werden mit (?) gekennzeichnet und die Zeilen werden nummeriert. Interviewer wird mit A gekennzeichnet und Interviewter mit B. Diese Transkripte werden als Anhang an diese Arbeit angefügt.

In den folgenden Kapiteln werden die Ergebnisse der Analyse der Interviews in Bezug auf den Theorieteil der Arbeit zusammengefasst.

9.1 Interviewpartner

Interview 1: Heinrich Riedl LL.B.(WU) war der Interviewpartner im Bereich Recht, Datenschutz und Versicherungsprozesse. Er hat an der Wirtschaftsuniversität Wien Wirtschaftsrecht studiert und ist in der Allianz Elementar Versicherung in der Organisation und Planung tätig. Er war maßgeblich im Projekt zur Umsetzung der organisatorischen Maßnahmen zur Datenschutzgrundverordnung im Jahre 2018 beteiligt.

Interview 2: Stefan Biehl, M.Sc. ist Information Security Officer in der Allianz Technology GmbH. Er hat an der FH St. Pölten den Master in IT-Security abgelegt und ist seitdem im Bereich Security im Unternehmen tätig. Er ist im Moment maßgeblich an der Entwicklung einer zukünftigen Cloud Lösung beziehungsweise Plattform der Versicherungsapplikation aus der Sicht IT-Security beteiligt.

Interview 3: FH-Prof. Dipl.-Ing. Herfried Geyer ist FH Dozent an der FH St.Pölten und Stellvertretender Studiengangsleiter IT Security (BA). Weiters ist er als freiberuflicher Mitarbeiter der CIS - Certification & Information Security Services GmbH als Consultant und Auditor tätig.

Interview 4: Mag. Thomas Schober ist Information Security Officer in der Allianz Elementar Versicherung und der Allianz Technology GmbH. Er begleitete einerseits die Umsetzung der Datenschutzgrundverordnung und aber auch die Projektierung eines Prototypen zur Umsetzung einer Versicherungslösung in der Cloud.

9.2 Ergebnis Interview

In diesem Abschnitt werden die Ergebnisse der Textanalyse aus dem Transkript nach Thema gruppiert und den dazugehörenden notwendigen Maßnahmen zugeordnet.

9.2.1 Datenschutzgrundverordnung und Umsetzung

In Österreich gab es schon ein recht strenges Datenschutzgesetz, daher waren die meisten Anforderungen in den großen Unternehmen auch schon umgesetzt und es war dadurch nur eine Art GAP Analyse notwendig. Ein Beispiel wäre das Recht auf Löschung, das auch schon in der DSG2000 vorhanden war (B2 Z21-24). Dieses Recht hatte hohes mediales Interesse hervorgerufen, allerdings dem entgegen gibt es auch die rechtlichen Aufbewahrungsfristen, welche grundsätzlich erfüllt sein müssen(B2 Z55-63).

Die GAP Analyse ergab im Versicherungsunternehmen von Hr. Riedl, dass eine Art Inventur der vorhandenen und verarbeiteten Daten vorgenommen wurde. Es wurde überprüft und aufgenommen, welche Daten von welchen Abteilungen verarbeitet werden und ob dies auch wirklich notwendig ist (B2 Z74-113; B4 Z16-27).

Ein wesentlicher Unterschied zur DSGO 2000 ist, dass das Verarbeitungsregister früher bei der Datenschutzbehörde geführt wurde und nun diese Pflicht an die Unternehmer übertragen wurde (B2 Z31-35).

Der Schwerpunkt liegt bei allen Interviewten im Bereich der Rechte der Betroffenen. Diese gab es zwar schon in der DSG2000, allerdings meistens nicht in diesem Detail (B1 Z33-36; B2 Z124-144; B3 Z13-36).

Aus Sicht der Interviewten, ist einer der ausschlaggebendsten Punkte der DSGVO, warum Unternehmen diese termingerecht umsetzen mussten, der sehr hohe Strafrahmen, der für viele Betriebe Existenz bedrohend ist.

Haben früher Firmen Datenschutz immer im nur unter dem Aspekt von wesentlichen geschäftskritischen Unternehmensdaten gesehen, ist nun mit der DSGVO auch der Schutz von personenbezogenen Daten von Mitarbeiter und Kunden, durch diesen Strafrahmen in den Fokus gelangt (B1 Z13-18; B2 Z63-68).

Aus technischer Sicht wurden von den Interviewpartnern auch auf die drei Prinzipien Integrität, Vertraulichkeit und Verfügbarkeit verwiesen. Diese sollen einerseits durch organisatorische und aber auch, durch technische Maßnahmen erfüllt werden (B1 Z103-153; B3 Z102-166). Es wurden als Beispiele folgende Inhalte angeführt:

- Integrität: Maßnahmen die Datenveränderung am Transport verhindern, Check auf Richtigkeit der Daten, Logging (B1 Z534-546; B3 Z109-121)
- Verfügbarkeit: Bandbreiten der Anbindungen, Datensicherungen, Wiederherstellpläne, Notfallpläne (B1 Z546-561; B3 Z121-136)
- Vertraulichkeit: Zugriffschutz durch Berechtigungs- beziehungsweise Rollenkonzepte (Need to Now, Last Privilege), Logging (B1 Z162-169; B3 Z136-166)

Ein besonderes Augenmerk sollte auch auf der Überprüfung der umgesetzten Prozesse und technischen Maßnahmen liegen. Es sollten regelmäßige Überprüfungen dieser durchgeführt werden, um die Wirksamkeit, Aktualität und Notwendigkeit festzustellen und wenn notwendig sind Änderungen durchzuführen (B1 Z85-101; B3 Z603-615; B4 Z119-126&Z199-212).

Grundsätzlich wurde der Einsatz von Public Cloud Diensten in den Versicherungsprozessen, bei Einhaltung der Stand der Technik, als möglich gehalten (B1 Z933-936; B2 Z303-312; B3 Z667-668).

Es wurde erweiternd angeführt, dass:

- durch die Einbeziehung eines Public Cloud Providers möglicherweise die Verfügbarkeit erhöht wird und teilweise einige Aufgaben besser und professioneller durchgeführt werden würden (B1 Z660-680).

- Kleinere und mittlere Unternehmen haben sogar kaum Möglichkeiten, solche Plattformen für sich selbst wirtschaftlich umzusetzen und auf den aktuellen Stand zu halten (B1 Z660-680).

- Zusätzlich wurde noch angeführt, dass es bei den regelmäßigen Penetration Tests im Cloud Umfeld wesentlich weniger Findings gibt, als in eigenen Infrastruktur Lösungen (B1 Z680-682; B3 Z386-401; B4 Z458-469).

Allgemein wurde von den Interviewten auch hervorgehoben, dass ein gewisses Maß an Vertrauen zu den Public Cloud Provider aufgebaut werden muss, da es nicht möglich ist jegliches Risiko über Maßnahmen und Verträge abzusichern (B2 Z386-395; B4 Z481-484).

In den nächsten Unterkapitel werden nun die notwendigen Maßnahmen aus Sicht des Interviewpartners:

9.2.2 Auswahl Public Cloud

Zur Auswahl von Public Cloud Providern wurden folgende Informationen von den Interviewten hervorgehoben:

- Welche Services bieten diese an? (B1 Z443; B3 Z470-476).
- Nach welchen Zertifikaten sind diese zertifiziert? (B1 Z449&607-622; B3 Z378-321&475-483; B4 Z297-299)
- Einsicht in die Security Protokolle nehmen. (B1 Z473-479)

9.2.3 vertragliche Maßnahmen

Zusammengefasst aus dem Interview können folgende vertragliche Maßnahmen hervorgehoben werden.

- Überprüfungsrechte zu Datenschutz und IT-Sicherheit sichern (B1 Z716 -717; B2 Z354-358).
- Einhaltung gewisser Normen wie z.B. ISO 27001 und ISO 27018 (B1 Z607-622; B2 Z372-382; B3 Z566-573).
- Verwendung von Technik die den Stand der Technik entspricht (B1 Z217-238; B2 Z333-341&383-387).
- Einhaltung der Verpflichtungen aus Datenschutzgrundverordnung (B2 Z336-339).
- Grundsätzliche Vertragsinhalte, wo es schon viele Vorlagen gibt, wie zum Beispiel von der Wirtschaftskammer Österreich. Diese wurden in Kapitel 6.3 genauer beschrieben und als Beispiel kann die Leistungsbeschreibung, Rechtsprechung, Offenbarungsverpflichtung genannt werden (B2 Z343-348).
- Verfügbarkeit der Lösung beziehungsweise des Services (B3 Z520-521&585).
- Reaktionszeiten, Antwortzeiten auf Vorfälle beziehungsweise Anfragen festlegen (B3 Z131-133&521-523&584).
- Meldewege und Prozesse für Datenschutzverletzungen und IT-Sicherheitsvorfälle regeln (B2 Z221-230).
- Exit Strategie und Umgang mit Daten regeln (B3 Z240-252&547-549&584;

9.2.4 organisatorische Maßnahmen

Zusammengefasst aus den Interviews können folgende organisatorische Maßnahmen hervorgehoben werden.

- Einführung der Rolle Datenschutzbeauftragter. Alle bestehenden und verschärften Prozesse in Bezug auf Datenschutz sollten so geändert werden, dass der Datenschutzbeauftragte eingebunden wird (B2 158-166).
- Einführen eines Verarbeitungsregisters und regelmäßige Kontrolle der Aktualität. (B1 Z102-127; B2 Z31-42; B4 Z16-21&199-212).
- In den Bereichen der Rechte des Kunden (Informationsrecht, Auskunftsrecht, Recht auf Richtigstellung, Recht auf Löschung und Wiederspruchrecht) müssen die entsprechenden Prozesse und deren regelmäßige Überprüfung aufgesetzt beziehungsweise angepasst werden (B2 Z180-193; B3 Z12-50)
- Das Recht auf Datenübertragung soll mittels einer technischen IT Lösung sichergestellt werden. Hier wurde angemerkt, dass es seit der Einführung im Mai 2018 keine einzige Anfrage dazu gab (B2 Z144-153).
- Für die Informationspflicht bei Datenschutzverletzung müssen eigene Prozesse, geschaffen und über den Datenschutzbeauftragten geführt werden. Dadurch wird sichergestellt, dass einerseits nur wirkliche Datenschutzverletzungen und andererseits die vorgegebenen Fristen eingehalten werden (B2 Z221-245).
- Awareness Bildung und Schulungen aller Mitarbeiter zur Klarstellung, was sind Datenschutzverletzungen und welche Vorfälle können dazu führen und müssen wann und wie gemeldet werden (B2 Z218-270).
- Kontrollprozesse um die Datenverwendung und die Berechtigungen der Verarbeiter und aber auch der Notwendigkeit der Verarbeitung regelmäßig zu kontrollieren (B1 Z85-101; B2 Z; B4 Z194-212).

- Regelmäßige Durchführung von IT-Security Tests. Als Beispiel können hier Penetration-Tests genannt werden (B3 Z415-422; B4 Z453-455).

9.2.5 technische Maßnahmen

Nach Meinung von Interviewter sollte beachten werden, dass alle technischen Vorgaben, die ein Gesetzgeber ausspricht, immer nur eine Basis darstellen und diese sehr oft nur einer Mindestanforderung entspricht (B3 Z623-627). Der Stand der Technik sollte immer eingehalten sein, zur Überprüfung wurden diverse gepflegte Dokumentationen, wie die des BSI und aber auch das österreichische IT-Sicherheitshandbuch erwähnt (B1 Z17-238; B3 Z176-180)

Zusammengefasst aus den Interviews können folgende technische Maßnahmen hervorgehoben werden.

- Einführen eines Berechtigungskonzeptes rollenbasierend unter Berücksichtigung des Verarbeitungsregisters (B3 Z138-142&Z303-315; B4 Z176-188).
- Absicherung der Datenübertragung durch Verschlüsselung. Als Beispiel eine End to End Verschlüsselung wie VPN Übertragung. (B1 Z164; B3 Z253-264&275; B4 Z141-143).
- Absicherung der Daten bei Speicherung durch Verschlüsselung (B1 Z164&Z534; B3 Z149-152; B4 Z52&305-316).
- Netzwerksicherheit mittels klar definierten Entry Point und abgeschotteten Netzwerk, um Unbefugten keinen Zugriff auf Daten und Applikationen zu ermöglichen (B1 Z255-260; B3 Z274-296).
- Strengere Authentifizierungsmethoden für Administratoren wie zum Beispiel 2-Faktoren Authentifizierung (B3 Z330-337; B4 Z186-188).
- Logging aller Zugriffe und Tätigkeiten mit revisionssicherer Speicherung (B1 Z369-380&542-543; B4 Z179-183).
- Datensicherung und Wiederanlaufprozedur herstellen (B1 Z554-560)

10. Fertigstellung des Frameworks unter Berücksichtigung der Information aus den Experteninterviews

Auf Grund der Unterschiede der Checklisten, wie schon in Kapitel 7 erwähnt, sollte eine Gliederung in die Basisanforderungen und in die besonderen Anforderungen in Beziehung auf die implementierte Form des Services, wie in Kapitel 5.2 beschrieben, durchgeführt werden. Wie in den Interviews erwähnt, sind die notwendigen Maßnahmen für die einzelnen Implementierungsarten, aufbauend aufeinander. Daher wird, wie im Kapitel 7 beschrieben, die Ausarbeitung auf die Implementierungsform IaaS beschränkt. Die Checklisten werden nur für Basis und IaaS Inhalte entworfen.

In den nächsten Kapiteln werden nun diese Checklisten in Form von Abbildungen dargestellt. In den Abbildungen werden folgende Inhalte dargestellt,

- in Abbildung 13 erfolgt die Darstellung der Checkliste zur Auswahl des Public Cloud Providers,
- in Abbildung 14 die Checkliste zu den vertraglichen Maßnahmen,
- in Abbildung 15 und Abbildung 16 die organisatorischen Maßnahmen und
- in Abbildung 17 die technischen Maßnahmen.

10.1 Checkliste zur Auswahl des Public Cloud Providers

Nr.	Checkliste zur Auswahl von Public Cloud Provider	Anforderung	Information	Bewertung OK/ NOK
A1.1	Hat der Public Cloudanbieter Global anerkannte Zertifizierungungen in Bezug auf IT-Sicherheit?	z.B. ISO 27001		
A2.1	Hat der Public Cloudanbieter Global anerkannte Zertifizierungungen in Bezug auf DSGVO?	z.B. ISO27018		
A3.1	Welches Recht beziehungsweise welcher Gerichtsstand wird angewandt und ist dieser mit	z.B. Europäisches Recht, österreichisches Recht		
A4.1	Hat der Cloudanbeiter fremdstaatliche Offenbarungspflichten und Ermittlungsbefugnisse zu erfüllen und sind diese mit den eigenen	z.B. USA auf amerikanische Firmen		
A5.1	An welchen Lokationen werden die Daten abgespeichert beziehungsweise verarbeitet?	Mögliche Einschränkung wie in DSGVO beschrieben		
A6.1	Gibt es in den Geschäftsbedingungen Regelungen zur Nutzung und Weitergabe von Daten an Dritte?	Abklärung mit Rechtsabteilung notwendig		
A7.1	Werden Verschlüsselungsverfahren zur Datenübertragung vom Public Cloud Anbieter verwendet und welche Technologie?	unbedingte Notwendigkeit		
A8.1	Werden die Daten in der Public Cloud verschlüsselt gespeichert und mit welchen	unbedingte Notwendigkeit		
A9.1	Ist es notwendig spezielle Software Produkte zu Nutzung der Public Cloud zu installieren?			
A10.1	Wie ist die Berechtigungsvergabe in der Public Cloud organisiert?	z.B. Kann der Nutzer selbst Berechtigungen vergeben?		
A11.1	Welche Mindestanforderungen an Kennwörter sind vom Public Cloud Provider gefordert?	Password Policy		
A12.1	Gibt es eine Regelung zum Umgang mit Benutzernamen und Kennwörtern?			
A13.1	Gibt es eine Regelung zur Information bei jeglicher Änderungen des Cloud Dienstes?			
A14.1	Gibt es Kündigungsfristen und Vereinbarung zur Auflösung beziehungsweise Beendigung des			
A15.1	Welche Vereinbarungen zur Datenrückgabe und Datenlöschung können mit dem Public Cloud Anbieter vereinbart werden beziehungsweise werden vom Anbieter angeboten?			
A16.1	Welche Modelle bietet der Provider an?	IaaS, PaaSund oder SaaS		
A17.1	Welche Referenzen gibt es für diese Modelle?	Vergleichbare Unternehmen bzw. Services		

Abbildung 13 Checkliste zur Auswahl von Public Cloud Provider

10.2 Checkliste zu vertraglichen Inhalten

Nr.	Checkliste vertraglich festzulegende Inhalte	Anforderung	Information	Bewertung OK/NOK
V1.1	Systembeschreibung beziehungsweise Vertragsgegenstand mit den Mindestinhalten vereinbaren!	Art und Umfang der erbrachten Cloud-Dienste gemäß SLA		
V1.2		Grundsätze, Verfahren und Maßnahmen zur Erbringung des Cloud Dienstes und Kontrollen		
V1.3		Beschreibung der Infrastruktur		
V1.4		Nutzungsvoraussetzungen		
V1.5		Umgang mit bedeutsamen Vorkommnissen die nicht den Regelbetrieb entsprechen.		
V1.6		Rollen und Zuständigkeitendes Cloud Providers und des Kunden (z.B. Mitwirkungsspflichten)		
V1.7	Verwendung Stand der Technik sichern			
V2.1	Vertragslaufzeit			
V3.1	Vergütung	Festlegen der Art der Vergütung und der Modalität (z.B. nach benutzter Ressourcen)		
V4.1	Regelung Haftung			
V5.1	Regelung Datenschutz	Vorgabe an Einhaltung der DSGVO des Providers und deren Mitarbeiter		
V6.1	Gewährleistung für Sach- und Rechtsmängel			
V7.1	Notwendige Zertifizierung oder Bestätigung von unabhängigen Dritten festlegen	Es soll vertraglich die Überprüfung von unabhängigen Dritten nach internationalen Standards vereinbart weren.		
V8.1	Umgang mit Unterauftragnehmern und externen Dritten vertraglich vereinbaren.	z.B. Informationspflicht bei Einbeziehung Dritter in die Dienstleistungserfüllung und mögliche Vertragskündigung)		
V9.1	Das Recht auf Prüfung und Kontrolle zusichern im Bezug auf:	Sicherheitsrichtlinien und Arbeitsanweisungen		
V9.2		Datenschutz		
V9.3		Risiko Behandlung (Identifizieren, Analyse, Berurteilung und Behandlung)		
V9.4		Physische Sicherheit (Zutritt, Umwelt, Stromversorgung)		
V9.5		Datensicherung und Wiederherstellung (Überwachung & regelmäßigen Tests)		
V10.1	Geschäftsbedingungen und Gerichtsbarkeit in notwendiger Form festlegen!	Festlegen der gesetzlich vorgeschrieben Gerichtsbarkeiten und den Geschäftsbedingungen		
V11.1	Lokation der Datenspeicherung und Verarbeitung festlegen.	Festlegen der gesetzlich vorgeschrieben möglichen Lokationen		
V12.1	Gesetzlich notwendige Offenbarungspflichten und Ermittlungsbefugnisse vertraglich festlegen.	Klar dokumentierte Pflichten und Befugnisse des Cloudproviders ersichtlich.		
V13.1	Gesetzlich notwendige Informationspflichten vertraglich festlegen.	z.B. Finanzmarktaufsicht, Medlung von Sicherheitsvorfällen		
V14.1	Benutzerverwaltung und Personensicherheit festlegen	Von wem und wie werden die Benutzerverwaltung durchgeführt?		
V14.2		Wie wird die Personensicherheit gewährleistet?		
V15.1	Vertragsbeendigung vereinbaren	Vorrausetzungen, Ablauf, Rechte und Pflichten festlegen		
V16.1	Datenrückgabe und Löschung in der Public Cloud mit dem Anbieter vereinbaren.	Wie werden Daten übergeben beziehungsweise gelöscht.		

Abbildung 14 Checkliste vertraglich festzulegenden Inhalten

10.3 Checkliste zu notwendigen organisatorischen Maßnahmen (Prozesse)

Nr.	durchzuführende organisatorische Maßnahmen	Anforderung	Information	Bewertung OK/NOK
O1	**Einführung & Betrieb**			
O1.1.1	Einführung Rolle Datenschutzbeauftragter	Rolle ist benannt und Aufgaben und Verantwortungen beschrieben.		
O1.1.2	Verfahrensverzeichnis mit Einbeziehung des Public Cloud Providers erstellen	Einbeziehen der Tätigkeiten in Bezug der Datenverarbeitung des Public Cloud Providers		
O1.2.1	Einführung bzw. Überprüfung von Rollenkonzepten für Zugriff auf Daten	z.B. Need to Now Prinzip		
O1.3.1	Einführung von Regelungen für die Zustimmung zu den	Verarbeitungsrechten		
O1.3.2		Nutzungsrechten		
O1.3.3		Übermittlungsrechten		
O1.4.1	Verpflichtungen der Mitarbeiter auf Einhaltung des Datenschutzes & IT-Sicherheit	Schulungen und Überprüfungen		
O1.5.1	Einrichten bzw. Anpassungen der Prozessabläufe der Bewahrung der Betroffenenrechte und Grundsätze mit Einbeziehung des Public Cloud Providers	Informationspflicht: Übermittlung der Informationen die bei der Erhebung übermittelt werden müssen. (z.B. Verantwortlicher, Datenschutzverantwortlicher, Zweck, Rechte,..)		
O1.5.2		Auskunftsrecht: Möglichkeit jederzeit Auskunft über die Bearbeitung der persönlichen Daten einer Person möglich.		
O1.5.3		Einwilligungspflicht: Prozess zur Einholung der Einwilligung zur Verarbeitung der personenbezogenen Daten.		
O1.5.4		Berichtigungsrecht: Prozess zur Richtigstellung von Daten auf Anforderung des Betroffenen		
O1.5.5		Recht auf Löschung: Prozess zur Löschung von Daten wenn Aufbehaltung rechtlich nicht vorgeschrieben.		
O1.5.6		Recht auf Einschränkung der Verarbeitung: Möglichkeit auf Anforderung der Betroffenen, die Verarbeitung nur für bestimmte Arten der Verarbeitung einzuschränken		
O1.5.7		Recht auf Wiederspruch der Verarbeitungeinwilligung		
O1.6.1	Public Cloud in das interne ISMS einbinden			
O1.7.1	ISMS Kontrollsystem mit dem Public Cloud Provider erweitern	Regelmäßige Überprüfung der Sichertsnachweise bzw. Zertifizierungen		
O1.7.2		Leistungsfähigkeit des Anbieters regelmäßig überprüfen		
O1.7.3		regelmäßige Überprüfung der Einhaltung der Informationspflicht des Public Cloud Providers		

Abbildung 15 Checkliste durchzuführender organisatorischer Maßnahmen Teil 1

Nr.	durchzuführende organisatorische Maßnahmen	Anforderung	Information	Bewertung OK/NOK
O1.8.1	Kontrolle für Datensicherung und Wiederherstellung	Überwachung der Durchführung		
O1.8.2		Überwachung der Aufbewahrung		
O1.8.3		Überwachung und Prüfung der Wiederherstellung		
O1.9.1	Prozess zur Handhabung von Informationssicherheitsvorfällen mit dem Cloud Provider etablieren	Meldung, Mitarbeit zur Behebung		
O1.10.1	Public Cloud Provider in die Notfallorganisation mit eingliedern	Public Cloud Provider muss in den Notfallplan mit eingebunden werden.		
O1.11.1	Einführen regelmäßiger Audits zur Überprüfung aller Maßnahmen & IT Sercurity Tests			
O1.12.1	Eintritts- und Austrittsprozesse von Mitarbeitern bezüglich Zugriff auf Systeme und Ressourcen	Prozesse sind eingeführt und auch mit Public Cloud Provider abgestimmt.		
O2	**Beenden**			
O2.1.1	Überprüfung und Kontrolle der Datenrückgabe beziehungsweise Löschung !			

Abbildung 16 Checkliste durchzuführender organisatorischer Maßnahmen Teil 2

10.4 Checkliste zu notwendigen technischen Maßnahmen

Nr.	durchzuführende technische Maßnahmen	Anforderung	Information	Bewertung OK/NOK
T1.1	Datenübertragung in die Public Cloud abgesichert	Verschlüsselt nach aktuellen Stand der Technik siehe zum Beispiel BSI Mindeststandards		
T2.1	Verschlüsselung der Datenspeicherung,-sicherung und -wiederherstellung	Verschlüsselt nach aktuellen Stand der Technik siehe zum Beispiel BSI Mindeststandards		
T3.1	Netzwerksicherheit mit Stand der Technik herstellen	(z.B. Firewall, Netzwerksegmentierung, 802.1X)		
T4.1	Zugriffschutz	sichere Authentifizierung (mind. 2 Faktoren)		
T4.2		Rollenkonzept&Benutzerrechte (z.B. Funktionstrennung)		
T4.3		Zugriffsrechte von priviligierten Usern auf Notwendigkeit einschränken (Betreibssystem, Applikation, Daten) und Berechtigung (Lesen, Ändern)		
T5.1	Protokollierung aller Zugriffe und Änderungen	Autorisierung		
T5.2		Dokumentation		
T5.3		Sicherstellen, das es nicht möglich ist Protokollierungen zu verändern		
T6.1	Datensicherung und Wiederanlaufprozedur	Sicherstellen das Daten gesichert und wiederherstellbar sind.		
T7.1	Anonymisierung von Daten			
T8.1	Trennung von Umgebungen	Trennung Entwicklung-, Test-, Produktivumgebung		

Abbildung 17 Checkliste durchzuführende technische Maßnahmen

11. Zusammenfassung und Ergebnis

Um die Implementierung der Versicherungskernprozesse wie in Kapitel 2 beschrieben umzusetzen, sind wie am Anfang der Arbeit schon angenommen, bestimmte Maßnahmen notwendig, beziehungsweise zu beachten. Diese Maßnahmen können in die Bereiche wie in Kapitel 6 beschrieben gegliedert werden.

In den nächsten Kapiteln folgen nun die aus den Interviews und der Analyse der Prozesse und Datenschutzgrundverordnung notwendigen Maßnahmen. Es wird darin auch ein Querbezug auf die erarbeitete Checkliste dargestellt. Dies erfolgt entweder im Text beziehungsweise direkt bei der Maßnahme in Klammer dargestellt.

11.1 Notwendige Vertragsinhalte

Es hat sich aus der Analyse im Theorieteil und den Interviews ergeben, dass die in Kapitel 6.3 beschrieben Inhalte unbedingt beinhaltet, beziehungsweise geregelt werden sollten. Dies wurde auch durch die Informationen aus den Interviews, wie in Kapitel 9.2.3 ersichtlich, bestätigt. Damit können auch die Fragen in der Checkliste zu den vertraglichen Inhalten zufriedenstellend beantwortet werden.

Ergänzend noch eine kurze Auflistung der notwendigen Inhalte die:

- Leistungsbeschreibung (V1.x)
- Rechtliche Inhalte
    - Gerichtsstand (V10.1)
    - Ermittlungsbefugnisse (V13.1)
    - Offenbarungspflichten (V12.1)
    - Lokationen der Speicherung beziehungsweise Verarbeitung nach rechtlichen Vorgaben (V11.1)
    - Datenschutz (V5.1)
    - Gewährleistung für Sach- und Rechtsmängel festlegen (V6.1)
    - Vertragslaufzeit (V2.1)
    - Haftung (V4.1)

- Vergütung (V3.1)
- Umgang mit Unterauftragnehmern und externen Dritten (V8.1)
- Vorgaben auf Überprüfung Dritter beziehungsweise Zertifizierungen (V7.1)
- Recht auf Überprüfung von Datenschutz und IT-Sicherheit (V9.x)
- Vorschreibung der Verwendung von Technik, die Stand der Technik ist (V1.7)
- SLA in Bezug auf Verfügbarkeit, Reaktionszeiten und Antwortzeiten (V1.1)
- Benutzerverwaltung und Personensicherheit regeln. (V14.x)
- Vertragsbeendigung und Rückgabe und Löschung in der Public Cloud vereinbaren. (V15.1 und V16.1)
- Sicherheitsvorgaben (V9.x)
    - Vereinbarung bezüglich Anwendung von Kryptographie bei Datenübertragung
    - Vereinbarung bezüglich Anwendung von Kryptographie bei Datenspeicherung
    - Vereinbarung bezüglich Anwendung von Authentifizierungsverfahren
- Prozessvorgaben
    - Regelungen im Umgang mit Änderungen (V1.5)
    - Regelungen bezüglich Beendigung beziehungsweise Auflösung der Zusammenarbeit.(V15.1)
    - Regelung zur Datenrückgabe und Löschung (V16.1)
    - Regelungen zur Nutzung und Weitergabe von Daten sind vorhanden und entsprechen den Anforderungen. (V8.1)
    - Regelung des Meldeprozesses bei Datenschutzverletzungen (V5.1)
- Geschäftsbedingungen (V10.1)
- Finanzielle Regelung beziehungsweise Entgelt (V3.1)

11.2 Notwendige organisatorische Maßnahmen

Die notwendigen organisatorischen Maßnahmen wurden im Kapitel 6.2 beschrieben und wurden in den Interviews auch bestätigt. Es wurde vor allem auf die nachfolgend beschriebenen Punkte hingewiesen.

Es ist nicht nur notwendig, die organisatorischen Maßnahmen wie in Kapitel 6.2 einzuführen, sondern auch, wie aus den Interviews hervor geht und im Kapitel 9.2.4 angeführt, die Kontrollprozesse dieser umzusetzen. Grund dafür sind die ständigen Veränderungen in Applikationen und von Ressourcen, die diese Kontrolle notwendig machen. Als Beispiel kann die Kontrolle, die im Interview mit Mag. Thomas Schober (B4 Z199-212) angeführt wurde, genommen werden.

Es handelt sich um die Kontrolle, ob Zugriffsberechtigungen noch aktuell sind, da sich durch Abteilungswechsel oder Verantwortlichkeitswechsel immer wieder zu Veränderungen der notwendigen Berechtigungen führt.

Dies muss beachtet werden, um die in Kapitel 6.2 unter personelle Maßnahmen beschriebenen Richtlinien einzuhalten. Diese sind wiederum notwendig, um die im Kapitel 3.2.3 beschriebenen Prinzipien einzuhalten.

Weiters sind besonders im Umgang mit Public Cloud Providern die sicherheitsrelevanten Meldeprozesse zu erwähnen. Es muss unbedingt, wie im Kapitel 6.4.10 beschrieben, die Handhabung von Sicherheitsvorfällen umgesetzt werden.

Hier kurz zusammengefasst, die organisatorischen Maßnahmen, die sich aus der Analyse der Interviews und aus dem theoretischen Teil der Arbeit ergebenen, die sowohl im Unternehmen, aber auch als Anforderungen an den Cloud Provider umgesetzt gehören:

- Personelle Maßnahmen diese werden in der Checkliste im Bereich O1.1 bis O1.4 abgefragt:
    - Regelung der Verarbeitungs-, Nutzungs- und Übermittlungsrechte
    - Einschränkungen für Lese-, Schreib- und Änderungsrechte
    - Berechtigung und Rollenzuweisung nach Erforderlichkeitsprinzip
    - Vertreterregelungen
    - Verpflichtung der Mitarbeiter auf Einhaltung des Datenschutzes
    - Schulungen zu DSGVO und IT-Sicherheit

- Organisatorische Maßnahmen
    - Einführung der Rolle des Datenschutzbeauftragten (O1.1.1)
    - Einführung, beziehungsweise Anpassung des Verarbeitungsregisters (O1.1.2)
    - Einführung Prozesse zur Regelung der Zustimmung zu den
        - Verarbeitungsrechten (O1.3.1)
        - Nutzungsrechten (O1.3.2)
        - Übermittlungsrechten (O1.3.3)
    - Anpassungen der Prozessabläufe für die Bewahrung der Betroffenenrechte und Grundsätze. Vor allem für die Verpflichtungen des Daten Verarbeiters und die Rechte des Betroffenen wie in Kapitel 3.2.8. beschrieben.
        - Informationspflicht (O1.5.1)
        - Auskunftsrecht (O1.5.2)
        - Einwilligungspflicht (O1.5.3)
        - Berichtigungsrecht (O1.5.4)
        - Recht auf Löschung „Recht auf Vergessen werden“ (O1.5.5)
        - Recht auf Einschränkung der Verarbeitung (O1.5.6)
        - Recht auf Wiederspruch (O1.5.7)
    - Prozesse zur regelmäßigen Überprüfung der Aktualität der umgesetzten Prozessabläufe wie in der Zusammenfassung der Interviews in Kapitel 0 beschrieben. (O1.11.1)
    - Awareness Bildung und Schulungen aller Mitarbeiter (O1.4.1)
    - Anpassungen bezüglich interner Unternehmensorganisation
        - Eintritts- und Austrittsprozesse von Mitarbeitern (Zugriff) (O1.12.1)
        - Aufbau Notfallorganisation und Einbeziehung des Cloud Providers (O1.10.1)
    - Regelmäßige Durchführung von IT-Security Tests (O1.11.1).

11.3 Notwendige technische Maßnahmen

Bei den technischen Maßnahmen sind besonders die Anwendung von kryptographischer Verfahren zur Übertragung, Speicherung und Sicherung von Daten hervorzuheben. Dies ist notwendig, um die Vorgaben zur Kryptographie, wie im Kapitel 0 beschriebenen, der ISO 27018 zu erfüllen. Diese sichert wiederum die Integrität der Daten wie Kapitel 3.2.6 beschrieben. Hier ist aus Sicht des Autors auch die Anwendung von IT-Security Services der Public Cloud Anbieter zulässig. Allerdings hat als Beispiel das Unternehmen des vierten Interviewpartners, zur aus seiner Sicht absoluten Absicherung, das Key Management in der eigenen Umgebung umgesetzt (B4 Z239-240).

Um die Verfügbarkeit der Daten sicherzustellen, wie in Kapitel 6.1 dargestellt, müssen Datensicherungen und die Wiederherstellbarkeit sichergestellt werden.

Hier nun eine Aufstellung der notwendigen technischen Maßnahmen die aus den Informationen der Interviews Kapitel 9.2.5 und den theoretischen Teil in Kapitel 6.1 und 6.4.5 bis 6.4.9 erarbeitet wurden:

- Einführen eines Berechtigungskonzeptes rollenbasierend unter Berücksichtigung des Verarbeitungsregisters (T4.3)
- Absicherung der Datenübertragung durch Verschlüsselung (T1.1)
- Absicherung der Daten bei Speicherung durch Verschlüsselung(T2.1)
- Netzwerksicherheit mittels klar definierten Entry Point und abgeschotteten Netzwerk, um Unbefugten keinen Zugriff auf Daten und Applikationen zu ermöglichen (T3.1)
- Strengere Authentifizierungsmethoden für Administratoren wie zum Beispiel 2-Faktoren Authentifizierung (T4.1)
- Trennung von Entwicklungs-, Test-, und Produktivumgebungen (T7.1)
- Anonymisieren von Daten (T8.1)
- Logging aller Zugriffe und Tätigkeiten mit revisionssicherer Speicherung (T5.x)
- Datensicherung und Wiederanlaufprozedur herstellen (T6.1)

12. Antwort auf die Forschungsfrage

Durch die, in der Analyse ausgearbeiteten Maßnahmen, kann die Forschungsfrage „Unter welchen technischen und organisatorischen Voraussetzungen kann eine Public Cloud Lösung, unter Einhaltung der Anforderungen, die sich auf Grund der Datenschutzgrundverordnung (DSGVO) und dem Datenschutzgesetz (DSG) ergeben, für die Kernprozesse der Versicherungsbranche eingesetzt werden?“ folgendermaßen beantwortet werden.

Die Antwort auf die Forschungsfrage ist, dass es möglich ist, mit den in Kapitel 6 und Kapitel 11 beschriebenen Maßnahmen, die Kernprozesse der Versicherung in Public Cloud Umgebungen, unter Einhaltung der Datenschutzgrundverordnung, umzusetzen.

Es ist allerdings, trotz aller Maßnahmen und Kontrollmechanismen notwendig, ein gewisses Vertrauensverhältnis zum Public Cloud Provider aufzubauen. Es wird nicht möglich sein, alle Gefahren- beziehungsweise Risikoquellen selbst zu überprüfen, zu kontrollieren, beziehungsweise zu beseitigen. Daher wird es notwendig sein, gut vereinbarte Arbeitsweisen zur Information und Beseitigung von Gefahrenquellen beziehungsweise Risikoquellen zu vereinbaren.

13. Ausblick auf die zukünftige Entwicklung

Die Nutzung von Cloud Services wird aus Gründen der Flexibilität und der Kosten noch wesentlich stärker in die IT-Landschaften von Unternehmen und auch der Versicherungsbranche Einzug halten. Wie im Cloud Monitor 2018 ersichtlich ist von 2014 auf 2015 ein Sprung der Unternehmen die Public Cloud Services einsetzen beziehungsweise den Einsatz planen von 24% auf 58% gestiegen und die Datensicherheit wird zunehmend als positiv bewertet. (KPMG, 2019, S. 7).

Aus diesem Grund lässt sich erwarten, dass die Lösungen für die Versicherungskernprozesse immer weiter verstärkt in Cloud Lösungen umgesetzt werden. Durch diese Entwicklung wäre es möglich, dass diese zentralen Applikationen von Versicherungen immer mehr auf einzelne Services aufgetrennt werden und dadurch die Nutzung von Public Lösungen verstärkt werden. Eine weitere mögliche Entwicklung ist, dass die großen Versicherungen mit ihren IT Töchtern, beziehungsweise Abteilungen, ihre Applikationen für den Versicherungsmarkt öffnen und diese am Markt als Gesamtlösungen anbieten. Dafür wäre natürlich eine Cloud Lösung eine sehr interessante Möglichkeit, auch kleinere Versicherung damit anzusprechen.

Eine wichtige Entwicklung damit sich Cloud Lösungen bei Versicherungsunternehmen etablieren, ist sicherlich das Vertrauen in die IT-Sicherheit und den Datenschutz der Cloud Lösungen. Nur wenn dieses Vertrauen erarbeitet wird, werden sich Cloud Lösungen in diesem Bereich und anderen Bereichen auch durchsetzen (KPMG, 2019, S. 33 - 34).

Als mögliche Weiterentwicklung dieser Arbeit wäre es interessant, die Ausarbeitung der Checklisten einerseits auf die verschiedenen Modelle (IaaS, PaaS, SaaS) zu erweitern und andererseits ein jährliches Review und Anpassung an die Weiterentwicklung der Vorgaben beziehungsweise rechtlichen Anforderungen vorzunehmen.

14. Literaturverzeichnis

Allenspach, M., 2015. *www.alexandria.unisg.ch.* [Online]
Online: https://www.alexandria.unisg.ch/127408/1/20110428-Kernprozesse_online.pdf
[Abruf am 31 03 2019].

Amazon Web Service, 2017. *https://docs.aws.amazon.com.* [Online]
Online:http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
[Abruf am 31 03 2019].

Amazon Web Services Inc., 2018. *https://aws.amazon.com.* [Online]
Online: https://aws.amazon.com/de/products/security/?nc2=h_m1
[Abruf am 31 03 2019].

Amazon Web Services, Inc, 2018. *https://aws.amazon.com.* [Online]
Online: https://aws.amazon.com/de/products/
[Abruf am 31 03 2019].

A-SIT, 2016. *https://www.sicherheitshandbuch.gv.at.* [Online]
Online: https://www.sicherheitshandbuch.gv.at/downloads/Cloud.pdf
[Abruf am 17 04 2018].

Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2008. *Rechtliche Grundlagen.* Wien: Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV).

Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018. *KFZ-Versicherung.* Wien: Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV).

Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018. *Krankenversicherung.* Wien: Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV).

Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018. *Lebensversicherung.* Wien: Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV).

Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV), 2018. *Sachversicherung.* Wien: Bildungsakademie der Österreichischen Versicherungswirtschaft (BÖV).

BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2014. *https://www.bitkom.org.* [Online]
Online:https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Vertragsgestaltung-Cloud-Computing/BITKOM-Checkliste-Cloud-Computing-Vertraege.pdf
[Abruf am 31 03 2019].

bitkom research GmbH, 2017. *www.bitkom.org.* [Online]
Online:https://www.bitkom.org/Presse/Presseinformation/Nutzung-von-Cloud-Computing-in-Unternehmen-boomt.html
[Abruf am 12 03 2019].

Brainloop, 2017. *https://www.brainloop.com.* [Online]
Online:https://www.brainloop.com/hubfs/01%20PDF_neu/Brainloop-WP-041-0417-Datenschutz%20und%20Cloud%20Computing-DE-1117.pdf?t=1531913001945&utm_source=hs_automation&utm_medium=email&utm_content=59462456&_hsenc=p2ANqtz--HrWZAs4t-e7NihQaUsDfJyR94V3ZTfNhDy4Lr1u5_UF
[Abruf am 05 07 2018].

Bundesamt für Sicherheit in der Informationstechnik – BSI, 2019. *https://www.bsi.bund.de.* [Online]
Online:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf?__blob=publicationFile&v=3
[Abruf am 17 12 2018].

Cloud Security Alliance, 2017. *https://cloudsecurityalliance.org.* [Online]
Online: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/
[Abruf am 05 12 2018].

Cloud Security Alliance, 2019. *https://cloudsecurityalliance.org.* [Online]
Online: https://cloudsecurityalliance.org/about/
[Abruf am 05 02 2019].

DIN Deutsches Institut für Normung e. V, 2014. *DIN ISO/IEC 27002,* Berlin: DIN Deutsches Institut für Normung e. V.

DIN Deutsches Institut für Normung e.V., 2017. *DIN ISO/IEC 27018.* Berlin(Berlin): Beuth Verlag GmbH.

Dresing, T. & Pehl, T., 2018. *Praxisbuch Interview,Transkription & Analyse. Anleitungen und Regelsysteme für qualitativ Forschende.* 8. Auflage Hrsg. Marburg: Eigenverlag.

EUR-Lex, 2016. *eur-lex.europa.eu.* [Online]
Online: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE
[Abruf am 17 04 2018].

Hammer, K., 2017. *Sicherheit während der Cloud-Kommunikation,* Wiener Neustadt: Fernfh.

Karlstetter, F. & Luber, S., 2017. *https://www.cloudcomputing-insider.de.* [Online]
Online: https://www.cloudcomputing-insider.de/was-ist-eine-public-cloud-a-633184/
[Abruf am 31 03 2019].

KPMG, 2019. *www.kpmg.de.* [Online]
Online: https://hub.kpmg.de/cloud-monitor-2018
[Abruf am 16 03 2019].

Luippold, T. L., Imholz, M. & Wiederin, E., 2008. *https://www.bcg.com.* [Online]
Online: https://www.bcg.com/documents/file15193.pdf
[Abruf am 31 03 2019].

Mell, P. & Grance, T., 2011. *The NIST definition of cloud computing.* [Online]
Online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[Abruf am 31 03 2019].

Microsoft Corporation , 2018. *https://azure.microsoft.com/.* [Online]
Online: https://azure.microsoft.com/de-de/overview/trusted-cloud/

Österreichische Datenschutzbehörde (DSB), 2018. *https://www.dsb.gv.at.* [Online]
Online: https://www.dsb.gv.at/gesetze-in-osterreich
[Abruf am 31 03 2019].

Parlament, E., 2016. *https://eur-lex.europa.eu.* [Online]
Online: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE

Red Hat, 2018. *https://www.redhat.com.* [Online]
Online: https://www.redhat.com/de/topics/cloud-computing/what-is-public-cloud
[Abruf am 31 03 2019].

Schradin, H. R. & Malik, A., 2008. *http://hdl.handle.net/10419/59193.* [Online]
Online: http://hdl.handle.net/10419/59193
[Abruf am 31 03 2019].

Schweinoch, M. & Störtkuhl, T., 2015. *https://www.computerwoche.de.* [Online]
Online: https://www.computerwoche.de/a/ratgeber-it-sicherheit,2363872,2
[Abruf am 31 03 2019].

Synergy Research Group, 2018. *https://www.srgresearch.com.* [Online]
Online: https://www.srgresearch.com/articles/aws-leading-public-cloud-market-all-major-regions
[Abruf am 31 03 2019].

Vogt, S. & Werner, M., 2014. *www.th-koeln.de.* [Online]
Online: https://www.th-koeln.de/mam/bilder/hochschule/fakultaeten/f01/skript_interviewsqualinhaltsanalyse-fertig-05-08-2014.pdf
[Abruf am 11 07 2018].

von Diemar, U. et al., 2011. *http://m.jonesday.com.* [Online]
Online: http://m.jonesday.com/files/Publication/b08c0e38-5bf3-4400-bc75-7f8ad5148a38/Presentation/PublicationAttachment/7a43dd04-ff6f-4783-940c-82f862e194cb/CloudComputing_Versicherungswirtschaft.pdf
[Abruf am 17 04 2018].

Wagner, F., 2018. *https://wirtschaftslexikon.gabler.de.* [Online]
Online: https://wirtschaftslexikon.gabler.de/definition/sachversicherungen-44926/version-268229
[Abruf am 31 03 2019].

Weidmann, M., Renner, T. & Rex, S., 2010. *https://wiki.iao.fraunhofer.de.* [Online]
Online: https://wiki.iao.fraunhofer.de/images/studien/cloud-computing-in-der-versicherungsbranche.pdf
[Abruf am 31 03 2019].

Zepke, G., 2016. *Lust auf qualitative Forschung.* Wien: Texte zur systemischen Organisationsforschung.

15. Abbildungsverzeichnis

A. Interview Leitfaden

Leitfaden Interviews

- **Vorstellung & Begrüßung**
  - Kurvorstellung Autor inkl. Info, dass Master-Studium an der FernFH
  - Motivation für die Arbeit
  - Kurzvorstellung der Arbeit
  - Interview dauert ca. 1h und das Interview wird aufgezeichnet
- Wissen und Erfahrung zu **Datenschutzgrundverordnung** und daraus entstehende Maßnahmen
  - Umsetzung der DSGVO in Unternehmen bzw. in ihrem Unternehmen
  - Was sind die Schwerpunkte der DSGVO für Unternehmen (z.B. Maßnahmen)?
  - Erfahrung in der Evaluierung der Daten
  - Erfahrung in der Evaluierung des Schutzbedarfs der Daten
  - Erfahrung in der Erstellung Verarbeitungsregister
- Wissen und Erfahrung zu **IT Sicherheit** und daraus entstehende Maßnahmen
  - Integrität, Verfügbarkeit und Vertraulichkeit von Daten
  - Was bedeutet Stand der Technik und wie kann es überprüft werden?
  - Datenspeicherung, -sicherung, -wiederherstellung
  - Datenübertragung
  - Netzwerksicherheit
  - Zugriffschutz, Berechtigungskonzept
  - Notwendige weitere Maßnahmen bezüglich DSGVO

- Wissen und Erfahrung zu **Public Cloud** und daraus entstehende Maßnahmen
    - Allgemeine Einschätzung von Public Cloud Providern
    - Auswahl der Public Cloud
    - Datenschutz in der Public Cloud
    - Zugriffssicherheit in der Public Cloud
    - Integrität, Verfügbarkeit und Vertraulichkeit der Daten in der Public Cloud
    - Standort
    - Vertragsinhalte
- Vorstellung der geplanten Checkliste
    - Erklärung Aufbau und Inhalt
    - Feedback
- Abschluss und Danke!

B. Interview Transkripte

B1. Transkript Interview Herfried Geyer

Das Interview wurde am 22.2.2019 um 10:00 Uhr in Wien 14. Linzerstrasse 211 geführt.

A: Wie wir eh schon besprochen haben, habe ich dir den Umfang der Arbeit schon erklärt. Ich würde jetzt gerne die einzelnen Punkte die ich, die Themen in der Arbeit sind Datenschutzgrundverordnung, um IT-Sicherheit im Allgemeinen und aber auch in Bezug, hauptsächlich in Bezug auf Public Cloud und genauso in dieser Reihenfolge würde ich gerne ein bisschen eine Information haben die mir dann Informationen oder Input ergeben zu der Checkliste bzw. am Schluss nachher die Checkliste allgemein durchgehen sage ich mal, den Aufwand und dein Feedback dazu einholen. Also ich würde jetzt einmal bei der Datenschutzgrundverordnung beginnen wo ich sage, vielleicht einmal allgemein ein Thema aus deiner Erfahrung heraus, wie ist es in, sage ich mal, in Unternehmen in Österreich? Ist die wirklich auch sehr ernst genommen worden? Ist auch sehr viel umgesetzt worden davon oder wird das eher, ja?

B: (?) gegeben ist hat es eigentlich eine strategische Bedeutung für die Unternehmen bekommen, das hat auch zur Folge gehabt, dass es auch bis zur Geschäftsleitung hochgekommen ist, aufgrund der möglichen oder potenziellen Strafrahmens durchaus eine unternehmenskritische Situation eintreten könnte. Nämlich nicht nur aufgrund von strafrechtlichen, sondern auch aufgrund zivilrechtlicher Ansprüche die sich ergeben könnten. Die meisten Organisationen haben natürlich sehr, sehr viel gemacht, wobei wo ich mir nicht sicher bin ob das alles was sie gemacht haben auch im Zweifel Bestand haben wird, es hängt ja davon ab von der Jurisdiktion in der Zeit. Beispiel in Österreich die Post ist da schon jetzt (?) in der Situation belangt zu werden und Untersuchungen über sich ergehen zu lassen und so lange keine Strafandrohung da ist, alleine die Untersuchungen von den Behörden sind schon sehr aufwendig und lästig, das will man sicher vermeiden. Das heißt, viele haben sich sehr gut vorbereitet indem sie entsprechende Dokumentationen aufgelegt haben, die auch schlüssig sind und von den Hausjuristen, ob das im Haus

oder aus dem Haus, außer Haus ist, überprüfen haben lassen und das Hackerl darunter haben, ja das ist entsprechend DSGVO soweit zulässig und sinnvoll für die Unternehmensbranche und Größe.

A: Mir würde weiter interessieren, was sind die Knackpunkte bei der Umsetzung sage ich mal von Maßnahmen damit man die DSGVO einhält, sage ich jetzt mal, was sind da so die Eckpfeiler drinnen was der Knackpunkt sein kann.

B: Naja viele haben das Problem, dass sie halt Verfahren und Prozessen sehr stark automatisiert oder automationsunterstützt abwickeln und das Ansprüche gekommen sind die möglicherweise der alten DSG 2000 so ausgeprägt noch nicht gestanden sind, zum Beispiel die Löschpflicht. Das heißt, wir haben Situationen wo die IT, da sind wir bei den technischen von den organisatorischen Maßnahmen wo die IT einfach nicht gewusst hat, wie kriege ich das aus einer Archivlösung raus, nämlich einen einzelnen Datensatz von einem einzelnen Kunden möglicherweise, wie kriege ich das aus einer Datensicherung heraus. Da hat es eine große Unsicherheit gegeben und da haben auch teilweise also die Produkthersteller spät oder zu spät reagiert. Da ist man vielfach jetzt noch in Umsetzung und muss die technischen Lösungen durch organisatorische Lösungen irgendwie kompensieren. Also das war eigentlich ein Teil. Ein zweiter Teil, der nur aufgepoppt ist, wenn das ein größeres Unternehmen ist, die Zuordnung, die Verantwortung für die TOM´s. Wer ist jetzt über den gesamten Verarbeitungsprozess und da gibt es ja verschiedenste oder viele, je nachdem wie viel in dem Verfahrensverzeichnis angeführt sind, wer ist für welche ausführende Tätigkeit verantwortlich? (?) nicht so lange aus diesen Workflows die jetzt zusätzlich durch die DSGVO einzubringen sind, maschinell abgebildet? Zum Beispiel ein Ticket-System. Also auch das war ein großer Aufwand, das war teilweise eine Ummodellierung von organisatorischen Maßnahmen, die aber durchaus massiven technischen Einfluss auch haben.

A: Was ich nun weiter Fragen würde, was sind aus deiner Sicht die Hauptpunkte im Bereich der Evaluierung der Daten, wie komme ich, was sind die wichtigsten Punkte was man durchführen sollte, sage ich mal, dass man überhaupt bemerkt wann bearbeite ich wirklich solche Daten oder wo bearbeite ich solche Daten, gibt es da eine Herangehensweise aus deiner Sicht die sich etabliert hat.

B: Also ich sage mal, ganz dumm, die die es wirklich ernst genommen haben das

Ding und das sind sehr viele, haben sich am Markt entsprechende Partner gesucht. Weil durch die DSGVO hat sich ja in der Juristerei aber gerade auch bei den Beraterunternehmen aus der Wirtschaftsprüferbranche so eine Goldgräberstimmung ergeben und die haben teilweise schon recht gute Modell wie man da herangeht. Das heißt, die analysieren die ganzen Businessprozesse nochmal durch und ordnen dann zu im jeweiligen Schritt dieses Businessprozesses welche Art von Daten personenbezogen oder besondere Kategorie personenbezogen abgewickelt wird. Die schauen natürlich jetzt nicht rein über welche technischen Verfahren, das abgewickelt wird oder wo die geografisch auch liegen. Das liegt dann wieder bei der IT bzw. beim CIO.

A: Und ich sage jetzt mal, nach deiner Erfahrung (?) was für einen Schutzbedarf gewisse Daten haben, die Herangehensweise vielleicht auch die Knackpunkte wie komme ich drauf was für einen Bedarf so ein Schutz, was für eine Stufe es hat. Mit was für einer (?) kann ich da ran gehen.

B: Es gibt, also wir haben relativ früh begonnen im deutschsprachigen Raum, das waren einige deutsche Bundesländer, die haben in ihrer, wie soll ich sagen, in ihrem Rechtsumfeld sehr, sehr gute Werke auch geliefert und das haben einige auch in Österreich, aber wie gesagt deutschsprachigen Raum haben das aufgegriffen, es gibt zum Beispiel von Bayern oder von Schleswig-Holstein tatsächlich auch Listen über technische, organisatorische Maßnahmen die fast universell anwendbar sind und die durchaus auch aufzeigen für besondere Kategorien dieser oder jener Art wäre gerade was Stand der Technik betrifft dieses oder jenes nötig. Es wurde errichtet irgendwann so um 2017 herum, wird jetzt aber nur aktualisiert. Also Stand der Technik ändert sich ja von Jahr zu Jahr (?) hängt von der Technik ab, da muss dann das Unternehmen eben selber dafür sorgen, dass der jeweilige aktuelle Stand der Technik nach dieser Initialzündung Umsetzung DSGVO eingehalten wird. Also das glaube ich, ist ein wesentlicher Prozess den viele Unternehmen tatsächlich noch nicht verstanden haben, habe ich so auch noch selten wo gesehen in Unternehmen, dass die tatsächlich jetzt versuchen überall dort, aus ihren Verfahrensverzeichnissen möglicherweise auch heraus, nachzuvollziehen ob man eh nicht nur, ich weiß nicht, am 1.5.2018 was auch immer, datenschutzkonform war, was die TOM´s betrifft, sondern auch beispielsweise am 23.7.2020 das sein wird. Wer

sich darum kümmert ist in einigen Unternehmen so nicht durchgesetzt. (?)
A: Ich höre daraus, dass es zum Beispiel für so ein Framework oder Checkliste ganz wichtig ist, dass auch bei den organisatorischen Maßnahmen diese Review Prozess, dass der abgefragt ist, ist dieser Review Prozess, dass ich die Daten kontrolliere ob ich diese noch verarbeite, wie ich diese verarbeite, wie ich diese speichere, wie ich den Schutzbedarf erhebe. Dieser Prozess für diese ganzen Sachen halt einfach eingeführt wird, dass da jährlich, halbjährlich immer reviewed wird ob er noch aktuell ist und das Verfahren dafür noch immer Stand der Technik ist. Ein ganz wichtiger Punkt, den überprüfe, dass es dieser Prozess ist und dass er auch gelebt wird und kontrolliert wird.
B: So wie du das gesagt hast kann ich eigentlich nichts mehr hinzufügen.
A: Okay. Ja, ich habe dann noch bei der Datenschutzgrundverordnung ist ja gefordert ein Verarbeitungsregister zu führen das ich feststelle, wann, wer, was verarbeitet und wer für diesen Schritt verantwortlich ist usw.
B: Vor allem mit dem Zweck verknüpft!
A: Was sind da Erfahrungen wie es da bei den Firmen da ausschaut, wie ernst ist der falsche Ausdruck, aber wie genau sie es umgesetzt haben das Register?
B: Eigentlich alle die ich kenne die sich mit dem beschäftigt haben, haben das sehr, sehr gut umgesetzt. Vor allem auch deshalb, weil das teilweise aus einem Bereich gekommen ist der jetzt, ich sage es mal, weit entfernt von IT ist. Weil das ist wirklich, dass das aus einer Rechtsabteilung gekommen ist, dass das aus einem Datenschutzumfeld gekommen ist, dass das teilweise aus einem nicht nur Zusammenarbeit mit Governance, Complaince und GDC gemacht worden ist, dass man da externe Partner miteinbezogen hat. Das hat oder es gibt Lösungen am Markt das selbst in eine Cloud auszulagern, zum Beispiel die IT vom Land Oberösterreich bietet an, man kann dort entsprechend so was führen gegen Einwurf kleinerer Münzen oder größerer, je nachdem und hat damit eigentlich ein hohes Maß auch an Rechtssicherheit abgedeckt , denn wenn man das dort sauber und richtig befüllt ist im österreichischen Rechtskontext zumindest einmal sichergestellt, dass ich nicht fahrlässig oder grob fahrlässig bin. Was dieses Befüllen betrifft, was die Vollständigkeit betrifft, was die Seriosität von diesem Verfahrensverzeichnis betrifft. Und viele sind eigentlich rein gegangen und haben sehr ausführlich das

berichtet oder dokumentiert, einfach deshalb, weil sie auch gesagt haben, dass dies erste sein wird falls ein Vorfall passiert was von uns verlangt wird und da hat man schnell reagieren können Richtung der Behörde. Sondern nicht erst dann, wenn wir den Anruf kriegen, sondern wirklich dann, ich hole das dann schon an (?) einfach weiterschicken können.

A: Also aus meiner Ausarbeitung heraus, eigentlich ist dieses Verarbeitungsregister das wichtigste oder der Start zu allen Maßnahmen, die dahinter irgendwie treffen muss.

B: Ja genau!

A: Ja. Okay. Gut. Das war es einmal im Großen und Ganzen über die Datenschutzgrundverordnung.

A: So, der zweite Schwerpunkt der Arbeit ist natürlich dazu die allgemeine IT-Sicherheit, in dem Bereich IT-Systeme mit Kundendatenverarbeitung verwendet, was für Rahmen gibt es, was uns klar ist, Integrität, Verfügbarkeit, Vertraulichkeit von den Daten, ich habe Themen dabei wie Daten speichern, Daten sichern, Daten wiederherstellen, Datenübertragung, Netzwerksicherheit, Zugriffsschutz, Berechtigungskonzept, wie gesagt, diese Punkte sind also die Schlagwörter dazu was ich in dem Bereich genauer betrachte müsste und ich hätte ganz einfach von dir so ein bisschen erklärt zum Beispiel Integrität, Verfügbarkeit, Vertraulichkeit in dem Bereich was sind da so die Maßnahmen bzw. auf was muss man besonders, was für Sachen gibt es deines Erachtens passieren viele Fehler, dass das nicht eingehalten wird . (Telefon läutet)

B: Also die Maßnahmen an sich sind absolut nichts neues oder Spezielles für die Datenschutzgrundverordnung. Es ist einfach so, wenn ein Unternehmen zum Beispiel Forschungs- und Entwicklungsdaten hat, die sehr wertvoll sind etwa für die Pharmaindustrie oder entsprechend Bankdaten, diese Maßnahmen sind existent, das Wesentliche ist, aber die Berechtigungsverwaltungen wo jeder in diesem gesamten Ablauf Berechtigungsvergabe, Änderung, Entzug, weiß was zu tun ist, von der organisatorischen bis über die technische Ebene hinweg. Damit habe ich eigentlich schon fast alle drei Anforderungspunkte von dem CIA-Triple recht gut im Griff. Was ich mit der Verfügbarkeit habe und das ist eigentlich auch ganz klar, ist eine Datensicherung entsprechend einer Business Impact-Analyse für das jeweilige

Service. Und wenn wir schon bei dem Begriff Business Impact-Analyse sind, im Rahmen eben der Datenschutzgrundverordnung und auch anderer rechtlicher oder vertraglicher Ansprüche, sollte ich bei der gleich mit evaluieren wie groß mein Integritätsanspruch dort ist und wie groß mein Vertraulichkeitsanspruch dort ist und das ergibt sich eben wieder aus dem bereits vorher erwähnten Verfahrensverzeichnis heraus wo ich dann sehe, ich habe normale unter Anführungszeichen personenbezogene Daten und ich habe welche besonderer Kategorie. Die technischen Möglichkeiten die es gibt die sind klar auf der Hand, also die funktionieren was zum Beispiel auch die Vertraulichkeit betrifft, das ist Verschlüsselung, das ist digitale Signatur was die Kommunikation betrifft, die Authentifizierung betrifft, das ist das ganze Logfile-Management, möglicherweise auch über CM Werkzeuge oder Loganalyse-Analysewerkzeuge, über Sandboxing die dafür sorgen, dass man eben sieht auch ob möglicherweise eine Malwarefikation stattgefunden hat, dass man das auch nachvollziehen kann, also all diese Maßnahmen technischer Natur sind gegeben, das Einzige was halt auffällt dabei ist, dass es bislang, also vor DSGVO keinen Kopf darüber gemacht hat ob man das auch für personenbezogene Daten jetzt braucht, da ist es eigentlich immer nur um im Wesentlichen Geschäftsdaten gegangen und wie gesagt, da schließt sich jetzt eben der Kreis wieder zur ersten Frage, ja es ist ein strategischer Risiko geworden und darum denkt man sich jetzt eben auch dort hinein und investiert eben dort in diese Art Maßnahmen

A: Du meinst also, das man früher nur auf die eigenen Business-Sicht gearbeitet hat, das man IT-Sicherheit macht, dass man sein eigenes Wissen nicht stehlen kann und nicht wer verwenden der sie nicht verwenden soll und mittlerweile ist der Gedanke durch die DSGVO gekommen, dass ich eigentlich die Daten von meinem Kunden schützen muss, dass der nicht irgendwie jetzt verletzt, bzw. das mit den Daten nicht etwas gemacht wird das nicht mein Geschäftszweig entspricht.

B: Genau und zwar nicht aus einer moralischen Überhöhung jetzt heraus, weil man plötzlich auf die Idee kommt, Jössas Gesetze sind ja sehr wichtig aus moralischer Sicht, sondern einfach weil das Strafausmaß rein fällt mit in eine Jahresbilanz Überlegung, in der Planung für die nächsten zwei, drei Jahre wie ich meinen Profit entsprechen vornehmen und planen und welches Risiko habe ich drin? Das ist

einfach so wie wir es vorher eben aufgemacht hat in der Risikoanalyse für das Gesamtunternehmen, nicht nur die Informationssicherheit, habe ich gewisse Faktoren. Zum Beispiel ein Notfallmanagement, das ich betreibe präventiv um festzustellen, wenn ein Stockwerk ausgebrannt ist kann ich so oder so lang ausfallen bis es geschäftsrelevant wird für mich ist. Und genau durch diese Datenschutzgrundverordnung, durch vor allem dieses Strafausmaß ist diese Überlegung halt jetzt auch hier mit reingekommen, dass ich auch in der eigentlich technischen oder IT-Risikoanalyse diese Aspekte mit betrachten muss als relevant. Und das war eigentlich der (?)

A: (?) man kann es ein bisschen auch zusammenfassen in diese Richtung, dass man sagt, es hat früher schon ein Datenschutzgesetz gegeben

B: es war einen jeden Wurst!

A: das hat keine Zähne gehabt, deswegen war es kein Risiko für Unternehmen, wenn man sich ehrlich ist und deswegen war es egal und das neue Gesetz hat ein bisschen Verschärfungen von dem Datenschutz selbst aber der Hauptfokus ist das Risiko durch eine Strafe geschäftskritisch geschädigt zu werden. Das ist einfach der Knackpunkt.

B: Das ist so wie wenn du ein 70er Täfelchen auf der Landstraße hast auf der große und du bist immer 110 gefahren und es war wurscht, weil wenn sie dich erwischen zahlst du 40 Euro und jetzt zahlst du aber 40.000 Euro. Und du weißt auch, die stehen, weil das echt Kohle bringt. Und so hat sich das halt abgeändert und du fährst du 100% 65.

A: Okay. Dann hätte ich noch kurz wenn ich fragen darf noch vielleicht in Richtung technischer Natur geht, wenn man früher Stand der Technik gesagt hat, ich habe vorher eh schon gesagt Datenspeicher, Sicherung und Wiederherstellung ist klar, daher Datenspeicherung wird wahrscheinlich eine Verschlüsselung der Daten sein, gibt es da, was ist da aus deiner Erfahrung der technische Stand momentan womit man verschlüsselt oder wie hoch der Verschlüsselungsgrad ist oder so der jetzige Stand und der wird sich ein paar Jahre noch halten, dass man sagt, das sollte das Mindestmaß sein, dass man Daten sichert.

B: Da gibt es einerseits natürlich das Werk in Österreich das IT-Sicherheit oder das österreichische Informationssicherheitshandbuch so heißt es jetzt, das ist aber

immer schon ein bisschen überwutzelt, also das ist durchaus nicht am Stand, ich würde sagen nicht unbedingt am Stand der Technik, wobei es für Sachverständige die das letztendlich ja feststellen bei einem Verfahren ob Stand der Technik eingesetzt ist oder nicht, der Richter weiß ja das nicht, der braucht einen Sachverständigen, die werden schwer dagegen argumentieren können wenn vom Innenministerium beauftragt bei der A-SIT dieses Informationssicherheitshandbuch aufliegt und da steht halt AES 256 und das haben wir eingesetzt bei unserem Produkt. Was an dem Ganzen oder was da besser performt ist wiederum das eine oder andere Werk vom deutschen BSI, die haben genau zu dem Thema auch gerade Verschlüsselung oder Kryptoverfahren 2018 ein neues Werk rausgebracht und es ist vorgesehen das tatsächlich auch, ich will nicht sagen jährlich, aber so wenn sich größere Schritte in der Entwicklung ergeben, das abzutreten. Das heißt, da hat man eine sehr, sehr gute Quelle und das ist auch das was die meisten Berater dann heranziehen in ihren Empfehlungen. Das ist auch das was man heranziehen sollte wenn man eine Produktauswahl jetzt etwa trifft. Das heißt, man hat eine Datenbank, irgendeine Lösung ohne ein Produkt zu nennen und der Hersteller dieser Datenbank bietet an, selbstverständlich haben wir immanent die Möglichkeit zu verschlüsseln die Daten, die Informationen vielleicht sogar rollenabhängig, da sollte man sich bitte schon anschauen wie, wie qualitativ gut und aktuell diese Verschlüsselungsmethodik ist.

A: Das heißt, wenn es zum Beispiel Richtung Checkliste und Framework geht (?) wäre es natürlich sinnvoll da jetzt nicht unbedingt hinzuschreiben wie du gesagt hast AES 256 sollte es sein, sondern man sollte hinschreiben entspricht die angewandte Verschlüsselungsmethode dem aktuellen, zum Beispiel der aktuellen Ausgabe der BSI zum Thema Verschlüsselung.

B: Ist richtig und der sehr gute Punkt wäre dann natürlich, wenn in so einem Dokument wo das für das Unternehmen festgelegt ist, noch eine Metainformation dabeisteht, dass man auch diese Aussage wo das zu finden ist, halbjährlich oder jährlich überprüft. Das heißt, dass auch das aktuell ist und nicht nur das Dokument.

A: Das heißt (?)

B: Nicht, dass der arme Mitarbeiter, der nicht nachschauen will auf einen Broken Link hinkommt.

A: Gut. Das war Verschlüsselung, ich denke mir Netzwerksicherheit wird (?)
B: Wir haben, Entschuldige wenn ich dich da unterbreche, aber zu dem Thema haben wir Security by Design als Begriff mit drinnen, das betrifft jetzt natürlich nicht nur die IT-Architektur aber auch, das heißt, wenn ich wirklich jetzt besondere Kategorien habe, müsste ich schon schauen und das ist halt der Stand der Technik weil es sehr günstig machbar ist, dass ich nicht über physische aber virtuelle Lösung entsprechend eine saubere Netzwerksegmentierung, eine saubere Netzwerktrennung habe damit ich alleine nicht nur über das Berechtigungskonzept in einem flachen Netzwerk eine Sicherheitsschicht einziehe, sondern tatsächlich auch physisch oder virtuell über die netzwerktechnische Ecke.
A: Gut. Dann der nächste Punkt wäre von mir Zugriffsschutz und Berechtigungskonzept, wobei ich jetzt einmal den ersten Fokus auf Zugriffsschutz. Also aus meiner Sicht, wenn ich jetzt Sage Zugriffsschutz ist, das heißt, jeder soll zugreifen können der die Daten zu verarbeiten hat und dazu gehören eben auch Identifizierungsmechanismen dazu. Meines Wissensstandes ist das Mindestmaß, das es dafür gibt ist eine Zwei-Faktoren-Authentifizierung, das man verwenden sollte, wenn ich von extern irgendwo einsteigen muss dazu oder kann.
B: Auch das ist wieder wie gesagt zu überlegen wer diese Vorgaben entsprechend empfiehlt, ich würde es einmal als Empfehlung sehen und ob man das als Unternehmen einsetzen will. Zwei-Faktor-Authentifizierung von außen rein über entsprechende Lösungen wie etwa PIN oder TAN auf einem Smartphone ist heute in jedem Fall Stand der Technik. Also wenn er das nicht macht und es passiert tatsächlich was aufgrund eines Angriffsvektors ist man unten durch. Was bei dem Ganzen aber noch dazu kommt, es geht nicht nur um die Empfehlungen zum Beispiel vom BSI oder von wem auch immer, sondern es geht wirklich auch darum, dass man das überprüfen lässt durch entsprechend geschulte Unternehmen. Das heißt, ich kann schon einmal mich drauf verlassen was der Hersteller sagt, ja wir haben das jetzt so oder so eingerichtet und es spielen in der Regel da eine größere Menge an Personen damit, die Leute aus dem Haus, die administrativ tätigen, die Produkthersteller, die Lieferanten, das Wartungspersonal und man kann jetzt nicht davon ausgehen, dass nicht jemand einen Fehler macht, das ist menschlich. Das heißt, um wirklich hier auch sicher zu sein, dass man keine Lücken hat in seiner

technischen Absicherung wären wir eigentlich verpflichtet so hin und wieder vielleicht jährlich oder halbjährlich, je nachdem wie kritisch man das einstuft, externe Spezialisten einzuladen wirklich einmal eine Attacke auf einen Inhouse-Rechner zu machen mit den normalen User Credentials eine Attacke zu starten und mit administrativen Accounts, eine Attacke zu starten, vielleicht aufs WLAN wenn das entsprechend hier irgendwo etwa mit personenbezogenen Daten kritischer Natur möglicherweise in einem Zusammenhang steht.

A: Gut. Berechtigungskonzepte haben wir im Prinzip eh schon im Skript, eigentlich geht es einfach darum, dass man im Unternehmen Rollenkonzepte wer den Zugriff auf Daten hat und dass die eben mit vier Augenprinzip vergeben wird, dass alles protokolliert und geloggt wird, glaube ich, das ist der wichtigste Punkt.

B: Ja ein Punkt kommt eben noch dazu, es steht schon auch in der Datenschutzgrundverordnung wirtschaftlich angemessen, das heißt, ich kann nicht auf personenbezogener Ebene die Berechtigungen bis ins letzte Detail auf jede einzelne Applikation oder auf jede einzelne Datenbank oder sonst wo runterbrechen, das heißt, ich brauche eine sehr, sehr schlaue Lösung, so wie du sagst mit Profil oder Gruppen oder was auch immer wo ich dann die User eben zuordne. Das sollte halt so eng wie möglich zu geschneidert sein, auch die jeweilige Tätigkeit, ist in manchen Branchen ganz gut möglich, in anderen zum Beispiel Krankenhausumfeld halt sehr schwierig da hat man den Leitstand die durchaus auch unter Umständen auf personenbezogene Daten selbstverständlich zugreifen müssen, das kann sein das die Leitstandskraft und das können 15 oder 20 sein nicht immer wieder aus und einloggen. Aber wie gesagt, das ist auch wieder wirtschaftlich angemessen der Branche und dem Verfahren entsprechend situativ angemessen muss das eben eingerichtet werden.

A: Ich sehe das zum Beispiel bei Versicherungen (?), als Beispiel genannt (?) im Schadensberater, ich habe einen der die Verträge anlegt, ich habe einen der die Verträge prüft usw. usf. Der die Anforderungen prüft der wird alle Daten ins letzte Detail wissen müssen, weil er zum Beispiel die Gesundheitsgeschichte überprüfen muss zum Beispiel bei Lebensversicherungen oder so, das heißt, der wird einen sehr hohen Zugriff auf Daten haben müssen. Der der die Polizze ausstellt, der wird wahrscheinlich relativ wenig Information haben müssen, der wird den Namen, die

Adresse und was für eine Art von Versicherung der und die Zahl was er verrechnet kriegt in seinen eigenen Daten die er selber hat, die braucht er eigentlich nicht sehen können, die sind für ihn uninteressant weil der stellt nur die Polizze aus, der prüft nicht. Als Beispiel. Da könnte man aus meinen Gefühl her aus technische Maßnahme die Daten anonymisieren die Bewertung Ich hätte zwar die Krankheitsgeschichte und alles, aber ich habe keine Person dazu und einen Faktor zu machen, das die Berechtigung so (?) dass man keinen Zusammenhang, das sind so Lösungen und ich glaube, im Versicherungsbereich könnte man das sehr gut die einzelnen Schritte einer Versicherung (?) oder was weiß ich (?) ein Schadensgutachter oder Schadensberater wird wieder alles wissen müssen und sehen müssen.

B: Was halt da dazu kommt was durchaus in Richtung der DSVG oder der Umlegung des österreichischen Gesetzesentwurfs eine Diskussion war, war eben diese indirekte Zuordenbarkeit. Das heißt, auch wenn ich jetzt einmal den Personenbezug rausnehme, muss ich darauf achten, dass ich nicht über Geschlecht, Wohnort, KFZ-Farbe oder was auch immer blöd gesagt, doch irgendwie einmal das so einschränken kann, dass ich es vielleicht auf zwei, drei Personen einmal einschränke und dann nur durch blöd nachfragen irgendwie drauf komme wer das wieder ist.

A: Als Beispiel genannt, dass ich es richtig verstehe, ist wenn jemand in der Müllergasse wohnt und ein blaues Auto hat und ich nehme den Namen Kurt Maier weg. Wenn ich jetzt nachher schaue, wer von den drei ist es. Das ist das Thema, dass es nachvollziehbar ist.

B: Und das kann durchaus schwierig werden, weil die Zahlen habe ich ja nicht ob das jetzt wirklich nur drei sind oder nicht.

A: Den wirtschaftlichen Aufwand habe ich ja in der Erstellung das beim Auseinanderdividieren sicherzustellen, dass ist schwierig. Viel günstiger den Personenkreis einzuschränken und lieber nicht standardisiert zu machen, sondern einfach zu sagen ich habe die Daten und setze da die Maßnahmen der der sie braucht verarbeiten kann und er aber auch vereinbart hat, dass er Stillschweigen halten muss.

B: Das ist genau das Beispiel, das du erwähnst jetzt ja auch das mit der Post momentan eben passiert. Die Post hat ja aufgrund gewisser Datenerhebungen wer

welche politische Einstellung hat und hat das den politischen Parteien weiter verkauft und das fällt ihnen jetzt am Kopf weil diese Zuordnung diese personenbezogene die sie eigentlich rausgenommen haben, die lässt sich über andere Faktoren sehr gut darstellen.

A: Okay. (?) den nächsten Punkt (?) was du als IT-Sicherheit siehst, vielleicht noch weitere Maßnahmen die wir bisher noch nicht besprochen haben bezüglich der Umsetzung von DSGVO, aus IT-Security Sicht gibt es da irgendwelche wesentlichen Themen die ich vielleicht noch nicht erwähnt habe.

B: Das erste wesentliche Thema, das hier sehr stark im Kern von deiner Arbeit betrifft ist, wer betreibt, wer betreibt was? Ich sage mal so, wissen wir überhaupt ob wir uns mit unseren Lösungen in einer Cloud befinden oder ob wir alles selber im Griff haben. Wissen wir wann wir smarte mobile Geräte beim Kunden einsetzen ob diese smarten mobilen Geräte tatsächlich die Daten so privat halten wie wir ausgehen davon oder ob die die sowieso in die Google Cloud oder in Dropbox oder in One Cloud oder sonst irgendwo hinschicken ohne, dass wir das Wissen, das wären Aspekte. Der zweite und finde ich auch sehr wesentliche Aspekt, der oft vergessen wird, es ist nie die alleine oder einzig technische Lösung, es ist immer ein Konvolut an technischen Lösungen, die das Ganze sicher macht. Das heißt, wenn wir von einer Berechtigungsverwaltung sprechen etwa und wir sehen, wir haben da eine Gruppe von vielleicht 30 oder 40 Personen in einem Rollenkonzept oder in einem Profil oder in einer Gruppe drinnen und eigentlich müssten die oder könnte man die schon noch weiter unterteilen, das ist aber technisch, wirtschaftlich nicht möglich, muss ich das Ganze über den zweiten Mechanismen Logging nachvollziehen können ob da möglicherweise eine, ja Betrug, Malversifikation oder Fehlhandlung nennen wir es einfach mal so, passiert ist. Und dann über den Personenbezug auf die Leute zugehen und sagen, liebe Leute, wir kriegen das mit, wenn ihr da was macht EGIS ist so ein Fall zum Beispiel, wir kriegen das mit und das ist mit Sanktionen verbunden. Und wir loggen oder wir tracken das jeden Tag und schauen uns das an und wenn uns irgendwas auffällt was nur irgendwie unplausibel ausschaut aufgrund eurer Tätigkeit, müssen wir das hinterfragen. Also nennen wir es Berechtigungskonzept alleine ist es, sondern auch Auswertung der Log-Daten und vorher natürlich die saubere Strukturierung und dann natürlich auch die

Konsequenzen zu tragen um etwa auf die Personen zuzugehen. Es ist ja eine Sammlung

A: Das heißt wenn ich das richtig verstehe, es sind viele technische Lösungen die ich aber in Überbegriff

B: Kontext

A: dass jedes einzeln eigentlich wenig bis nur ein Teil bringt

B: Genau (?)

A: die komplette Sicherheit nur alles im Ganzen wirklich die Sicherheit gewährleistet.

B: Richtig, genau und das ist aber auch nichts Datenschutzgrundverordnungsspezifisches. Das ist so, ja genau, wenn ich vertrauliche, streng vertrauliche Daten habe im Unternehmenskontext, meine Bilanz Zahlen oder was auch immer, dann muss ich das dort genauso machen.

A: Okay. Ja. Mit dem wäre ich eigentlich schon beim dritten Punkt jetzt, nämlich die DSGVO und die IT-Sicherheit und das jetzt ganz spezifisch bezogen auf Public Cloud Lösungen bezogen. Allgemein deine Meinung oder deine Erfahrung von, ich nehme jetzt mal die großen Public Cloud-Anbieter her, also ich rede von Amazon, (?) Microsoft, von Google, diese (?) ich glaube, das sind die Hauptprovider, an die man sich hält. Wie ist deine Erfahrung wie die mit IT-Sicherheit und Datenschutz umgehen oder was deine Erfahrung ist, was bedeutet das für diese Firmen? Oder sind die immer am letzten Stand kann man sich an diesen ein Beispiel nehmen was das angeht?

B: Ja, ich darf vielleicht noch kurz ausholen. Du nennst ja immer den Begriff Public Cloud, du hast auch gesagt vorhin, du hast dir die 27018 schon ein bisschen angeschaut, da sind ja Verweise drinnen unter anderem auch in die 17788 und 17789, also ISO 17788 und 89. Da ist relativ klar definiert auch was Cloud ist und was Public, hybrid und Private Cloud ist. Wann wir jetzt von Cloud reden und da bitte jetzt um dein Ja oder Nein, nehme ich an du meinst Application as a Service, nicht Infrastructure as a Service oder was weiß ich

A: Nein, eigentlich, also eigentlich von der Arbeit her wäre es so angedacht gewesen, schon alle drei Arten, also Infrastructure as a Service, Plattform as a Service und Software as a Service zu erwähnen. Ich glaube, dass ich wenn ich alle drei bearbeiten

soll und auch in den Checklisten (?) werden würde und das (?). Bei uns in der Firma ist das Hauptthema eigentlich Infrastructure as a Service und ich würde bei den Checklisten aller Wahrscheinlichkeit nach sage ich jetzt mal, mich auf die Infrastructure as a Service (?) Plattform as a Service fokussieren in erster Linie einmal. Wobei ich sagen muss, wird sich herausstellen ob ich vielleicht das dritte Thema auch noch angehe. Also ich denke, was du meinst ist, dass man bei Infrastructure as a Service ganz andere Sachen wichtig sind als bei Software as a Service. Da bin ich selbstverantwortlich was für Daten wo, wie sind sie verschlüsselt (?) Software as a Service ist halt eine Software und da muss ich mich verlassen können, dass der Cloud Provider oder der Anbieter, die Daten, die ich dort eingebe (?) sicher dorthin übertragen, werden dort sicher (?) abgespeichert, werden verschlüsselt, niemand anderer kann zugreifen usw. usf.

B: Ja, das ist der Punkt.

A: Deswegen würde ich mal sagen, aus meiner Sicht ist die Anforderung von Software as a Service ist sehr hoch bei einem Cloud Provider und in Richtung Infrastructure as a Service werden die Verantwortungen und die notwendigen Maßnahmen immer kleiner. Vielleicht, dass wir grundsätzlich vielleicht sogar schon Richtung Software as a Service einmal denken, wenn wir darüber reden, ich glaube, auch der Software as a Service-Anbieter, der Cloud Provider, meine Meinung, bitte dich um Bestätigung wenn du es auch so siehst, hat das was an Verantwortung für Infrastructure as a Service hat, die hat er bei Software as a Service genauso und die Anforderungen steigen einfach immer je mehr, je mehr Tätigkeiten Richtung dem Cloud Provider fallen.

B: Ist richtig ja.

A: Habe ich die Überlegung ob wir uns einmal großen Brocken sich mal anschaut und den mal durchgeht und da ganz einfach mal anfängt, sage ich jetzt mal so.

B: Ja, mein Vorschlag wäre, dass wir das umgekehrt mal angehen.

A: Also umgekehrt! Ok.

B: Also Infrastructure as a Service, das war sogar so, dass ich damals vom Thomas Schober beauftragt, ich glaube, vor drei Jahren war das, wo ich so eine Untersuchung gemacht habe wegen E-Shelter. E-Shelter war einmal so die Idee, dass man das in Frankfurt glaube ich auslagert und der Thomas wollte einfach

wissen, wie sicher sind die dort, was bieten die an und das war hauptsächlich eine Netzrecherche, also wir waren nicht vor Ort dort, sondern eine Netzrecherche, wir haben uns eben angeschaut auch wie sind die Bewertungen der Mitarbeiter in den Jobbörsen, wie schaut das Bild aus von Google Earth und Google Maps, was befindet sich in der Nachbarschaft und das Ganze, es war nicht notwendig, dass man hinfährt, man kann sich das wirklich in einer Online-Recherche sehr, sehr gut feststellen, auch über die Zertifikate die dargestellt sind usw. Das heißt, so wie du richtig gesagt hast, Infrastructure as a Service zum Beispiel kann ich mir sehr gut ein Bild machen wie gut oder schlecht die dort arbeiten. Ich kann mir, ich habe das in Österreich jetzt gemacht, da gibt es auch einen E-Shelter-Außenstandort, es gibt auch die Interaction in der Schuttlewarestrasse da kann ich auch hingehen, die haben kein Problem damit, dass ich sage, okay, ich bin die Firma XY, ich überlege mir hier einen Infrastructure as a Service Partner zu suchen, einen Termin auszumachen und ihr zeigt mir das einfach. Die Herren sagen, nein gerne, machen wir den Termin, gehen wir dann Mittagessen, das sind unsere Zertifikate und machen einen Walkthrough, wir zeigen ihnen wie die Leute bei uns eingebucht werden, wie sie ausgebucht werden, welche Protokolle wir führen, welchen 24 Stundendienst wir haben, welche (?) Anlagen wir haben, also Heizung, Klima, Lüftung, Brandmeldung, Brandschutz, all das lässt sich sehr gut begreifen. Und so wie du richtig sagst, da muss man davon ausgehen, dass das alle auf ein gewisses Mindestmaß hinuntergebrochen auch haben. Das nächste was jetzt dazu kommt bei Plattform as a Service zum Beispiel ist eben, dass die eine Betriebssystembasis anbieten wo natürlich auch noch mit den entsprechenden Spezialisten relativ gut feststellbar ist wie gut oder schlecht die dort arbeiten. Weil die Plattforms die wir haben da gibt es nur ein paar, sage ich jetzt einmal vereinfacht am Markt die halt verwendet werden, das ist irgendwas Linux-basiertes oder Unix-basiertes oder was Microsoft-basiertes, das ist alles keine Zauberei, das kann man sich vorstellen lassen und da kann man sich dann auch nachweisen lassen, dass der Plattform as a Service-Partner auch technische Checks dort fährt. Und das ist ganz klassisch, wo wir uns jetzt hinbewegen ist fast schon ein bisschen weg von der 27001 Richtung ISO20000. Ich lasse mir nicht nur Kapazitätsprotokolle oder was schicken, sondern ich lasse mir wirklich auch Security-Protokolle schicken, ich habe zwar selber zum Beispiel

Radar Services im Haus im Einsatz, so was Ähnliches (?)systeme oder was auch immer, wie man das nennen will, zusammen mit einem SOC, kann man von denen verlangen das ist Stand der Technik, die bieten das auch selbstverständlich und da kann man auch reinschauen oder hinschauen ob das bei Plattform as a Service so funktioniert oder nicht.

A: Das ist zum Beispiel AWS gibt es diesen Security-Bericht zum Download, was wo betroffen war, was für ein Vorfall es war

B: Und was man dann noch, also was ich persönlich dann noch machen würde, wenn ich unternehmensverantwortlich wäre, ich würde hergehen mit diesem Modell wie du auch gesagt hast, mit diesem monatlichen, wöchentlichen oder was auch immer Sicherheitsbericht, ich würde in ein unabhängiges Rechtsbüro gehen und mir dort bestätigen lassen, dass ich datenschutzgrundverordnungsmäßig mit dem als Grundlage darauf aufbauend gut arbeiten kann. Also, dass mir da keiner irgendwas anhängt. Und wenn ich das als Zettel auch noch irgendwo liegen habe, diese Bestätigung, dann habe ich es. Dann würde ich sagen, mehr brauche ich nicht. Was ich schon tun muss ist natürlich auch im Web so ein bisschen mit schnuppern nennen wir es jetzt einmal, bei dem jeweiligen Provider den man hat, du hast ja AWS und ein paar andere aufgezählt, ob da irgendwelche Probleme aufgetaucht sind, die einschlägigen Seiten, dass man sich anschaut von (?) oder (?) oder BSI in Deutschland oder von Sans, bei AWS hat es einen großen Vorfall gegeben, dass man erstens seine Seite oder seine Sicht dort auch anschaut ob man da betroffen ist und dass man dann zweitens auch zu diesem Partner geht und sagt, was ist euch da passiert? Warum ist euch da was passiert? Und wie arbeitet ihr jetzt dagegen an? Das ist das eine. Klassisch ist natürlich dann bei Plattform as a Service, dass man weiß, dass dort, ich nenne es einmal Rootrechte oder privilegierten Accounts bei Partner liegen, dass dort Menschen arbeiten die man nicht selber gescreent hat, die nicht durch das eigene Assessment-Verfahren durchgelaufen sind. Das heißt, wenn ich jetzt eine Applikation oder Datenbanken drauf aufsetze, das heißt, das mache ich ja selber, muss ich dafür sorgen, dass selbst wenn der alle Berechtigungen auf seiner Plattform hat, nicht an die personenbezogenen Daten kommt.

A: Muss er das wirklich, also muss oder sollte ich dafür sorgen, dass der auf diese Daten nicht kommt oder reicht es für mich, aufgrund deiner Erfahrung her, dass dir

der Public Cloud Provider bestätigen kann, dass zum Beispiel der Mitarbeiter von ihm (?) überprüft worden ist und er die Anwendungsverpflichtungserklärungen unterschrieben hat und (?) reicht das oder muss ich das wirklich technisch verändern?

B: Du hast deine Antwort eigentlich vorher schon selber gegeben indem du gesagt hast, ja wir müssen schauen von der Berechtigung her, du hast ein paar so Rollen in der Versicherung genannt, also den Makler der das überprüft, welchen Sinn hätte es jetzt, dass bei euch zum Beispiel intern der Datenbank Admin auf alle Daten Zugriff hat? Warum braucht der das? Die braucht er nicht. Und der Betriebssystem-Admin schon gar nicht. So wenn das jetzt technisch weltweit, wenn es keine Lösung gibt, keine wirtschaftlich vernünftige Lösung das zu verhindern, müsste man wahrscheinlich sagen, ja da muss ich es in Kauf nehmen und dann muss ich mit diesen Dingen irgendwie auskommen, wenn es wirklich wirtschaftlich so vernünftig ist, dass ich das dann in die Cloud auslagere. Und da muss aber möglicherweise schon auch wieder ein Schadensfall DSGVO gegen rechnen. Das ich nicht nur sagen, naja dann kann es mir aber trotzdem passieren.

A: Müsste ich eine Risk-Analyse machen wieder, was bedeutet das für mein Business, wenn der (?) und was kostet oder was sind wirtschaftliche Kosten, dass ich das umsetze, dass er nicht (?)

B: Genau, das ist der Punkt. Also was passiert, wenn der wirklich, USB-Stick blöd gesagt, reinsteckt, zieht mir 10.000 Kundendaten ab und vermarktet die irgendwie Richtung Russland und das kommt halt rauf und das lässt sich schlüssig zurückverweisen, dass das eigentlich unser, nämlicher meiner und der von meinem Partner, der Fehler war. Und das betrachte ich in der Risikobetrachtung wo sich dann herausstellt, okay, trotz aller Widrigkeiten, es ist trotzdem noch günstiger wenn ich es so mache mit meinem Outsourcing-Partner, werde ich sagen, ja ich mache es, aber wie gesagt, immer wirklich dann und es gibt heute die Lösungen, dass ich sage, okay, ich kann Datenbanken sauber verschlüsseln und entsprechend ein Berechtigungskonzept dazu stellen, dass der, der die Plattform administriert keine Chance hat in diese Datenbank irgendwie rein zu kommen

A: Sondern nur der der aus der Applikation kommt sieht die Daten. So wie bei uns, ich weiß das wir unsere Plattform mit Guardium verschlüsselt haben und der

Schlüssel nicht bei uns liegt, sondern irgendwo bei einem Notar und ich kann nur über die Applikation die Daten lesen und über die Applikation ist sichergestellt, dass nur der Zugriff hat, der das Rollenkonzept hat und die Berechtigung hat.

B: Genau und nachweisbar ist es damit auch in der Protokollierung

A: In der Protokollierung kann man genau schauen wer hat was gemacht.

B: Zusätzlich darf man bitte nicht vergessen, weil wir immer Vertraulichkeit jetzt, dass ja die Datenschutzgrundverordnung auch Datenverfügbarkeit und Integrität vorsieht. Die Integrität habe ich mit dem auch relativ gut abgedeckt, die Verfügbarkeit nicht. Das heißt, wenn der Admin dort sagt, hey, heute habe ich einen schlechten Tag, ich fahr denen das Zeug runter und der fährt die Plattform herunter alles virtuell relativ schön gemacht, dann seid ihr weg. Dafür müsst ihr natürlich auch sorgen.

A: Das ist natürlich das, nachher die technische Umsetzung, dementsprechend die System gebackuped haben,

B: Genau

A: das ich ein BCM eingerichtet habe, dass ich Wiederanlaufprozedur festgeschrieben habe usw. Also was ist businesskritisch bei uns, wenn wir 2 Stunden das System nicht haben oder einen halben Tag das System nicht haben das muss man analysieren wie lange das ist und das muss in der (?) geplant due Kennzahl , entfernen und Stopp Also ja genau, ich kann sofort anfangen wieder zu Starten und ich verlier laut Business Analyse oder Business Impact oder Risk Analyse verliere darf maximal nur 20Minuten der Datenverarbeitung

B: oder einen Tag oder was

A: das wäre unter Verfügbarkeit zu sehen. Oder, dass ich das System redundant ausgelegt haben muss und ja, dass wenn irgendwo ein Fehler passiert oder irgendwas, dass der abgedreht werden kann und weitergearbeitet werden kann.

B: Aber da ist natürlich auch wieder die Frage, wir reden ja jetzt noch über Allianz und du wahrscheinlich auch, eine der größten Versicherungen weltweit, die hat vielleicht sogar irgendeine Handhabe gegen Google oder gegen Microsoft oder was auch immer. Wenn das jetzt eine Hagel-Versicherung ist in der (?)strasse mit den 120 Mitarbeitern und die würden das machen, ja wie wollen die ein Rechtsverfahren gegen Google oder Amazon anstreben? Die kratzt das nicht einmal.

A: Da kommen wir dann auf ein Thema was ich da (?) Vertragsinhalte (?) usw. diese Thematiken wo ich sage, wo ich bei meiner Ausarbeitung fällt in den Bereich schon (?), dass ebenso wie du sagst, dass man gegen die großen Cloud-Anbieter die zwar die sind mit einer der ausgereiftesten Techniken und auch wahrscheinlich die Prozesse in sich selbst sehr gut sein müssen, denn sonst würden sie nicht die größten sein, sage ich jetzt einmal so, aber wie du sagst, ein Kleiner der dort ein Service bezieht kann nicht viel Flexibilität von so einem Unternehmen erwarten. Und da komme ich jetzt wieder nämlich zu den Vertragsinhalten nachher hin wo ich glaube, oder vielleicht, dass du es mir noch bestätigst auch, dass es da ganz wichtig ist zu schauen wie sind die überprüft, was für Zertifikate habe ich, dass ich feststellen kann, wie arbeiten die intern wie passt das zu meinem System dazu, dass die das haben, kann ich mir sicher sein, dass so dort gearbeitet worden ist.

B: Es sind noch wesentliche Inputs in die Organisationseigenrisikoanalyse. Man kann sagen welche Handhabe habe ich da? Was mache ich auch mit der Handhabe, wenn vielleicht ein halbes Jahr später dann tatsächlich eine finanzielle Kompensation kommt für einen Schaden, der aufgetreten ist, ich bin aber innerhalb von drei Monaten weg vom Markt, wenn mir das passiert ist, also all das und BCM und Risikomanagement soll drinnen sein.

A: Ich habe in meiner Arbeit dazu auch ausgearbeitet, dass ich, es gibt einige Leitfäden dazu was diese Zertifikate oder Überprüfungen oder Bestätigungen oder wie man sie auch nennen will. Ich habe drinnen beschrieben drei Normen oder Frameworks, das eine ist dieser BSI-Anforderungskatalog, Cloud Computing C5 von der BSI aber ich glaube, das ist ein recht gutes Sammelsurium, (?) was dein, (?) doch ein bisschen sehr, nach Deutschland ein bisschen ausgelegt, weil ja von einer deutschen Organisation ist oder (?). Dann habe ich noch die CSA die Cloud Security Allianz (?), das ist einfach nur ein recht verbreitetes und (?)

B: Das europäische

A: europäische und als nächsten Punkt habe ich die ISO-Normen genommen wobei da aufbauend auf 27001, 27002 die Maßnahmen, die 27018 Zusatzanforderung wobei 17 ja auch Cloud-Thematik allgemein (?) usw. und die 27018 besonderes Augenmerk auf die Datenschutz, also auf die, also allgemein Datenverarbeitung in der Cloud. Und ich habe jetzt für mich in der Arbeit jetzt angenommen, habe gesagt, ich will

die 27018 besonders in Auge nehmen und analysieren, weil ich glaube diese Punkte aus der Datenschutzsicht dargestellt sind oder auch die Maßnahmen teilweise sehr gut ausgearbeitet sind und festgestellt natürlich, dass Amazon, Google, Microsoft all auch nach dieser Norm zertifiziert sind.

B: Ja da muss du aufpassen was das der Scope ist. Das ist Amazon ist zertifiziert, es sicher nicht Gesamtamazon, du musst schauen ob genaue die Services, die ihr nutzt die Versicherung da nutzt, entsprechend (?). Noch etwas zu deinen Aufzählungen von unterschiedlichen Standards, also de facto Standards, denn echter Standard oder echte Norm ist wirklich nur die ISO, international anerkannt, du hast es eh richtig gesagt, das eine ist halt Deutschland, das BSI ist ein super Grundsatz oder Grundlagenwerk, wenn man eine ISO27001 plus 27018 umsetzen will, da gibt es auch eine Zertifizierung dafür. Das mit dem European Star ist so eine Geschichte, auch da kann man durchaus das CIS mit der Österreich Ansprechpartner (?) und verhandelt, ist meines Wissens nach, vielleicht täusche ich mich aber, meines Wissens nach nicht wirklich gut dabei. Es ist mehr oder weniger (?) akkreditierte oder international akkreditierte Lösung so wie es bei den ISO-Normen ist wo wirklich die nationalen Normungsinstitute und die nationalen Akkreditierungsgesetzgebunden dafür sorgen, dass man wenn man in einem Land zertifiziert ist auch in anderen Ländern diese Zertifizierung anzuerkennen ist. Also das ist ein wesentlicher Aspekt da dabei.

A: Das heißt, du würdest von deiner Sicht her, empfehlen (?) wen könnte ich nehmen? Sagen, was für Services würde ich denn beziehen wollen? Und dann aber schauen, dass diese Services bei diesen Unternehmen eine ISO-Zertifizierung haben, weil die weitverbreitetste, anerkannteste und wie du gesagt hast, einzige echte Norm dieser Themen sind

B: Genau, wenn die nun einen Zettel haben und da steht drauf, die bekannte Beraterfirma was weiß ich, ich sage jetzt einfach mal EOY hat festgestellt, dass man nach diesem BSI-Papier oder nach European Star konform arbeitet, ist das auch wertvoll. Das will ich gar nicht in Abrede stellen, es macht aber wie es in Österreich eigentlich ist, freie Beweiswürdigung zum Beispiel, das schätze ich schon so ein, dass die Sachverständigen und auch die Richter und (?), dass das anerkannt wird, dass die sagen, ja wir haben uns das angetan oder die haben sich dem entsprechend

unterzogen, das hilft natürlich. Gerade weil wir auch gesagt haben wir starten bei Infrastruktur Dienstleister, da gibt es ja die TI(?)42 die so Infrastruktur sich anschaut, da gibt es jetzt auch eine EN-Version dazu, die fällt mir jetzt gerade nicht ein wie die heißt, die wird auch von der CIS angeboten (?) das heißt, in der Regel, soweit ich weiß, (?) E-Sheelter haben auch diese Zertifizierungen für ihre Infrastruktur wo wirklich auch geschaut wird, dass die lokale Gesetzgebung aber auch international Stand der Technik der Verkabelungs-Sicherheit, Offshore - Sicherheit wenn alles mit eingehalten wird, da gibt es mehrere Stufen, da gibt es auch von der Bitcom, von der deutschen, die ist auch da sehr wertvoll, entsprechendes Stufenkonzept. Also man findet da durchaus eine größere Sammlung an sehr wertvollen Unterlagen und de facto normativen Geschichten. Was ich vielleicht noch mit erwähnen möchte, weil du es schon angesprochen hast, wenn man ein internes Kontrollsystem hat das zum Beispiel von einem Wirtschaftsprüfer gefordert ist und ich nehme in meinem IKS derartige Prüfpunkte mit auf und behandle die seriös, da muss ich auch extra dazu sagen, und ich habe eine ISAE3402-Zertifizierung hat das auch einen zusätzlichen Wert. Es ist halt auch wieder kein Zertifikat nach einer Norm oder Akkreditierungsgesetz aber, die Wirtschaftsprüfer unterliegen, die wissen die gesetzlichen Richtlinien, die wissen Seriosität, das heißt, auch das würde ich jetzt nicht von der Hand weisen.

A: Also Bitcom habe ich zum Beispiel auch bei den vertraglichen Themen hier hergenommen, weil die eine gute Aufstellung haben was so in einem Vertrag drinnen steht, aber ich komme da jetzt zum nächsten Thema, wir haben jetzt oder sagen wir so, für dich wenn du das Unternehmen (?) die Cloud gehen willst mit deinem System, wäre es für dich ein Thema (?) Allianz ist, würde man jetzt natürlich auf die großen Betreiber zugehen.

B: Ja, vor noch 10 Jahren hätte ich gesagt, never ever in die Cloud. Du darfst auch nicht vergessen, wenn wir jetzt ein Unternehmen hätten sofort im Kopf, Jössas ich muss mir jetzt einen IT-Abteilung erst aufbauen. Hier ist ja anders, die haben einen IT-Betreiber im Haus, dem man mehr oder weniger vertraut was die Erfahrungen der Vergangenheit (?) und da wägt man dann dagegen ab und das ist oft (?) eine Diskussion was ist heute sicherer, selber betreiben oder ein Cloud-Dienstleister wie du sagst, einer von den großen. Und die Meinung wendet sich jetzt schon massiv

Richtung Cloud-Dienstleister. Also man sagt Amazon betreibt sich ja selber, Microsoft betreibt sich selber, bei Microsoft, bei Amazon, wir haben ja Role Models, wir haben (?), wirklich große internationale Unternehmen die (?) lassen die abseits der Datenschutzgrundverordnung ja auch einen hohen Vertraulichkeits-, Verfügbarkeits- und Integritätsanspruch haben und die würden, (?) gut und gerne vermuten, das ist legitim, dort nicht sein, wenn es da nicht diese Vertrauensbasis gäbe, das heißt, ich brauche keine Betriebsfeuerwehr mehr aufbauen wo 15 Straßen weiter das städtische Wiener Feuerwehr ist und ich weiß, das sind Profis und geschult, machen ihre Übungen, die trinken nichts in der Dienstzeit, die machen das sauber. Mache ich nicht. Aber ist so und wir wechseln heute alleine schon durch diese Komplexität oder durch die zusehends stärker werdende Komplexität der IT-Welt. Ist das für Einzelunternehmen zusehends schwieriger solche Plattformlösungen Plattformapplaince, für sich selber schlau und sicher aufzusetzen. Sichtbar man dann immer, wenn man die Pentester in kleineren oder größeren Unternehmen schickt, die finden dort immer was. Während hingegen bei den großen, professionellen Unternehmen ist das sehr, sehr schwierig was zu finden.
A: Jetzt haben wir über Infrastructur und Plattform gesprochen und jetzt kommt noch im Prinzip die Software as a Service. Ausschlaggebend in der Public Cloud, da ist ja die Software selbst betrieben von (?) ich nutze ja eigentlich nur (?) eine Applikation (?) wo ich ja auch nicht wirklich überprüfen kann (?) ist das wirklich (?) kennst du überhaupt ein Verfahren oder auch Normen oder (?) die es gibt, dass man feststellen kann als Außenstehender, diese Software ist konform, die erfüllt diese Notwendigkeiten?
B: Ja wo nutzen wir es? Zum Beispiel Office 365. Das ist eigentlich, also viele Unternehmen nutzen das mittlerweile ja für, Schriftverkehr, teilweise für SharePoint unter Umständen usw. Ich denke schon, dass sie sich über die bestehenden Risiken diesbezüglich bewusst ist, dass man die aber einfach auch aufgrund der Marktsituation oder der Alternativlosigkeit fast nicht mehr anders wählen kann. Natürlich kann ich mir ein System anschaffen, mit dem ich lokal das alles betreibe, das ist aber heute eigentlich nicht mehr die Art wie man arbeitet.
A: Ich denke jetzt einmal zum Beispiel im Fokus wie ich vorher schon gesagt habe, auf die Versicherungsträger. Ich sage jetzt es gibt eine Firma die

Schadensregulierungen in der Cloud anbietet. Also die bieten mir ein Tool und wollen meine Schäden (?) und dass ich sage, was muss ich beachten wenn ich sage, ich will so einen Cloud-Provider, ich will das nutzen, wie könnte ich feststellen, aus deiner Sicht, dass diese Applikation dem entspricht, sage ich mal, dass diese Anforderungen von mir an Datensicherheit, dass die Datenschutzgrundverordnung eingehalten wird und diese Sachen? Ich weiß das muss oder soll, Rollenkonzept, Benutzerkonzept und so weiter, muss entweder seine Daten (?) Daten inhaltlich, sondern dass ich (?) Logging, es ist alles wahrscheinlich gleich wie man es selbst betreibt, aber ich kann es ja nicht überprüfen bei dem selber. Im Haus könnte ich es überprüfen selbst.

B: Da kommt es einmal drauf an, wer hat diese Software oder diese Applikation hergestellt? Bin das ich selber und ich übergebe das und schule dort Leute ein, die nicht in meinem Konzern sind dann habe ich eigentlich recht gute Möglichkeit das mit zu tracken, weil ich die Stärken und Schwächen meiner Lösung kenne. Ist es aber, so wie zum Beispiel bei SAP oder eine Cloudlösung, dann habe ich aber keine Ahnung was da dahinter passiert. Dann muss ich mich mehr oder weniger wirklich drauf verlassen, dass die Angaben des Herstellers oder des Dienstleisters stimmen und dass der Dienstleister aber auch das wiederum eine möglichst Vier-Augen oder Sechs-Augen-Prinzip überprüfen lässt, dass der auch nicht sagt ja meine Entwickler oder externe Entwickler, die das entwickeln für den, denen vertraue ich, sondern dass der auch wieder sagt, so wie er es selber entwickelt, okay, bevor wir (?) bevor wir einen Change machen oder bevor wir das überhaupt lancieren, haben wir ein oder zwei externe Untersuchungen noch brauche, über alle möglichen Testverfahren hinweg, dass das wirklich auch sicher ist und das macht (?) nachweislich.

A: Gibt es da Standards?

B: Es gibt zum Beispiel diesen Microsoft-Software-Development-Lifecycle. Das ist fast ein de facto Standard, der ist halt auch recht umfassend, der ist natürlich nicht nur für Microsoft brauchbar, sondern für alles Mögliche andere auch. Da gibt es auch noch ein paar andere Werke, die ich jetzt aus meiner Fachhochschultätigkeit herauskenne, also die wirklich so den ganzen Software-Entwicklungs-Lifecycle abdecken kann damit, das sind auch wieder so Art de facto normative Werkzeuge. Was es noch gibt, weil du vorhin auch wieder hingewiesen hast, meines Wissens

nach ist die 27034 das eine ist Netzwerksicherheit, das andere ist Applikationsentwicklung, die auch aus mehreren Teilen besteht, eins, zwei, drei, vier oder fünf, glaube ich, zumindest sind die alle publiziert, das kann ich wieder als Größe heranziehen. Wird nicht so nicht so stark wie eine 27018 von der ich mich ja zertifizieren lassen kann sogar in Verbindung mit einer 27001. Ich kann 27018 und 27034 zertifizieren lassen, aber trotzdem, wenn ich hergehe und sage, ja ich lege da das als Schwerpunkt (?). Und ich kann entsprechend auch nach diversen, sage ich, Projektvorgehensmodellen, ich kann Prince 2 oder IPA Art und Weise Software entwickeln, ich kann vor allem über die ISO9001 ein sehr, sehr gutes Qualitätsframework über Softwareentwicklung von der ersten Designphase weg im ersten Schritt bis zum Abschluss hinten nach das sauber machen. Über ISO20000 die über den Betrieb herkommen ich übernehme nichts in meinem Betrieb wo ich nicht 100% weiß, dass (?), dass ich nicht (?). Also wie gesagt, da gibt es wieder so ein Paket an unterschiedlichen Maßnahmen die abgefragt den Provider (?)

A: Das war jetzt die Entwicklung und die Inbetriebnahme. Die Applikation selbst prüfe ich wahrscheinlich genauso mit 27018 ob es Mandantentrennung gibt oder so

B: Ja (?)

A: Also die Funktion dieser Applikation, dass das getrennt ist, dass keiner auf die Daten zugreifen kann usw. das ist ja im Prinzip genau das gleiche wie bei einer Plattform (?) das sind die Grundvoraussetzungen, die lege ich halt auch in die Applikation (?).

B: Es ist so, dass zum Beispiel so große Unternehmen wie SAP zu ihren Produkten auch Sicherheitshandbücher anbieten wo beschrieben ist welche Features diese Lösung hat. Vielleicht noch einmal, eine gewisse Vertrauensbasis muss gegeben sein. Ich weiß halt, wenn ich mir zum Beispiel jetzt einen Audi oder einen Mercedes oder BMV oder einen VW kaufe, was ich mir einbauen lasse. Vielleicht defekte Software aber vielleicht auch wirklich ein qualitativ gutes und wertiges Auto. Wenn ich mir einen Dacia oder einen Lada oder einen Renault oder was kaufe, habe ich vielleicht die wirtschaftlich vernünftigste Lösung, aber ich werde das Auto vielleicht nicht 15 Jahre rostfrei fahren können. Weiß ich jetzt nicht

A: Wahrscheinlich wäge ich ab und gehe das Risiko ein.

B: Ja genau, richtig, ja genau (?)

A: ich geh das Risiko ein um 30% weniger zu Zahlen und augenscheinlich für die gleiche Funktion hat, weil es fährt, gleiche Funktion, aber voraussichtlich ist es so, dass es halt nur (?) bis 10 Jahre vernünftig zu fahren ist und beim VW 15 Jahre vernünftig fahren kann.

B: Was wir noch dazu haben, ich habe meine Aufpreis Liste und beim Dacia kann ich mir möglicherweise nicht irgendwie so einen Front Assistent dazu kaufen weil sie ihn nicht anbieten und da kann es sein, dass ich aus meinem Sicherheitsbedürfnis weil ich meine Familie damit transportiere oder weil ich auch die Fußgänger irgendwie verantwortlich denke, dass ich mir sage, nein das Auto kaufe ich mir nicht, ich kaufe mir dann doch irgendein ein bisschen Richtung Premium gehendes das mir das mit anbietet und zahle halt entsprechend mehr. Genauso ist es da halt auch.

A: Super. Ein kurzes Thema hätte ich noch, kurz nicht, ein Thema hätte ich noch und zwar die Checkliste selbst. Also meine Überlegung in diese Richtung war ganz einfach mehrere Checklisten. Wo ich sage, ich baue das so auf, dass ich einmal eine mache für die Auswahl des Anbieters, dann eines wo ich sage was den Vertrag betrifft möglicherweise auch da, also in jedem Bereich glaube ich, gibt es eine Basis-Anforderung für diese Checklisten und dann möglicherweise Infrastructur, Plattform, Software als Zusatzanforderung sind so aufgebaut, so würde ich das gerne aufbauen, also einmal die Auswahl, der Aufbau, Prozesse und organisatorische Notwendigkeiten, dass ich dich die Abfrage, also gibt es das, habe ich so was usw. ja, nein und dann auch technische Maßnahmen. Also diese vier Checklisten, ob das eine eigene Excel ist oder nicht ist egal, aber diese vier Checklisten würde ich gerne erstellen mit (?) aber zum Beispiel wenn man jetzt als Beispiel hernimmt die Auswahl, also bei den vertraglichen Inhalten da gibt es von, zum Beispiel von der Firma Bitcoin eine sehr gute Unterlage dazu und diese Inhalte wenn ich es jetzt finde, habe ich schon ausgearbeitet was ich meine was notwendig ist in den Vertrag zu stellen. Ich nehme mal an, (?) ziemlich klare Angelegenheit aus meiner Sicht, ja genau, (?) ganz wichtig ist genaue Servicebeschreibungen (?), das sind eh ganz klare Sachen, hast du aus deiner Erfahrung vielleicht Themen also die vergisst man sehr oft oder meistens (?) usw. das ist alles okay, aber gerade bei Public Cloud-Providern wo du sagst aus deiner Sicht, das sind essentielle Dinge Themen die unbedingt

vertraglich festgesetzt werden müssen.
B: Nein, eigentlich man muss sich überlegen, wenn man in eine Public Cloud geht, (?) wenn man rein geht, man muss wirklich, also ich fange nochmal anders an. Es gibt ja zum Beispiel in Österreich Public Clouds, die Huemerhost zum Beispiel oder die Firma Huemer IT, die bildet ja auch Cloud-Lösungen (?) Application as a Service oder Software as a Service, sondern Plattform as a Service, mit denen kann ich sehr gut verhandeln auch. Also mit denen, das ist nicht McDonalds, das ist Wirtshaus. Ich gehe hin und sage, ja ich hätte gern das Schnitzel, bitte statt den Petersilerdäpfel kommt Reis und statt dem gemischten Salat einen grünen Salat. Bei Microsoft, bei den großen (?) ja (?) genau, da hast du die AGBs und du musst halt diese 200 Seiten deiner Rechtsabteilung geben zum Durchlesen, was die damit machen weißt du eh nicht. Ich bin einmal vor der Situation gestanden als Privater vor 4 Jahren oder 5 Jahren war das wo ein Unternehmen gekommen ist und gesagt hat, Herr Geyer arbeiten schon lange zusammen, wir sind vor einem Problem, wir IT, unsere Mitarbeiterinnen und Mitarbeiter wollen skypen. Wir müssten quasi Skype als Tool, da war es noch nicht Teil von Microsoft, wir müssen Sykpe jetzt wirklich als (?) von der Sicherheitssicht her, können wir das oder können wir das nicht? Ich habe dann überlegt, was soll ich sagen? Weil ich es nicht gewusst habe ob Skype sicher ist oder nicht. Ich habe nur diese, weißt eh in den Hurra-Medien hörst du ja sofort, Skype ganz furchtbar und der Rechner gehört nicht mehr dir, sondern Skype und ich bin hergegangen und habe gesagt, liebe Leute, schaut euch an, Skype wenn ihr verwendet bietet im Web sehr, sehr gute AGBs, nehmt die, geht die zu eurer Rechtsabteilung, lasst euch dort diese AGBs durch arbeiten und wenn euch eine Rechtsabteilung sagt, das ist okay was da drin steht, das können wir verantworten, dann kann die IT nicht sagen das verweigern wird. Das hat keine Woche gedauert hat die Rechtsabteilung hat gesagt nie und nimmer. Weil da ist dringestanden, die gesamte Kommunikation wird von uns aufgezeichnet und wir dürfen die auswerten zum Beispiel. Die ganzen Accounts, Skype-Accounts gehören uns, das geht nicht. Und genau das ist es wo ich sage, da wird viel zu wenig wert draufgelegt weil die Leute oder die Organisationen viel zu viel Angst haben, dass sie auf was stoßen was ihren Cloud(?) möglicherweise stoppen könnte (?). Nichtsdestotrotz ein verantwortliches Unternehmen oder ein verantwortungsvolles Unternehmen muss

das durchgehen und auch wenn es mühsam ist und wenn es lang ist.
A: Ich habe im Prinzip so ein bisschen so die Grundvoraussetzungen wie Vertragslaufzeit, Vergütung (?) Haftung, Datenschutz, Vertraulichkeit und (?) Einschaltung von Subunternehmen, das muss geregelt sein (?) und Exit Management, Gerichtsstand, Rechtswahl, Vertragsart eh klar, aber das steht eh wie du sagst in den AGBs und da ist (?) ist es wichtig, dass man halt einfach wirklich (?) von der Rechtsabteilung prüfen lässt (?) akzeptieren oder kann man das nicht akzeptieren. Weil einzelne Punkte verhandeln wird bei einem Amazon nicht möglich sein, wobei Amazon wahrscheinlich grundsätzlich schon einmal gewisse Angebote auch hat drinnen wie (?) diese Services und (?)
B: Ja genau
A: Und somit ist da sehr viel (?) Vertrag erstellen (?) das sind die Mindestanforderungen die, also AGBs oder Vertrag hergeben müssen oder nicht wenn ich AWS, Microsoft oder Google hernehme und (?) bieten ein bestimmtes, ich sage jetzt einmal, der Gerichtsstand (?) gesetzlich nicht weil ich Versicherer bin und die Finanzmarktaufsicht oder so irgendwie (?) und (?) ist der Gerichtsstand ist Amerika zum Beispiel kann ich den nehmen oder möglicherweise nicht nehmen weil die Finanzaufsicht als österreichisches Unternehmen auf einer österreichischen Versicherung muss ich den Gerichtsstand Österreich gesetzlich vorgegeben. Darum sage ich, das ist zu überprüfen (?), dass ich sage das ist möglich oder nicht!
B: Genau, auch da kann wieder so Role Models (?) Versicherung (?) auf der Plattform arbeiten und die sind zufrieden und glücklich und haben noch kein Problem mit irgendwelchen Kunden oder Rechtsträgern, Beteiligten (?) kann man durchaus sagen, okay, da sind wir die Dritten, warum sollte das jetzt gerade bei uns nicht gehen? Also das ist durchaus auch legitim, wenn was passiert zu sagen, ja wir sind den anderen gefolgt und sind schon davon ausgegangen, wir haben es selber untersucht, aber was noch dazu kommt es ist ein Zusammenspiel unterschiedlichster Organisationseinheiten. Du hast jetzt viele Dinge aufgezählt die von mir wiederum aus einem Supply Management, aus IT (?). Du hast ein paar Punkte aufgezählt, die aus dem 27002 Kapitel 15 ist es, Supply Management drinnen steht. Das heißt, wenn ich so was mache, ich kann das nicht alleine entscheiden, ich brauche eine Rechtsabteilung oder ich brauche externe

Rechtsberater die sich im Vertragswesen gut auskennen, die die unterschiedlichsten Rechtsordnungen wie die Datenschutzgrundverordnung etwa auch kennen, meine Branche und mein Unternehmen kennen, ich brauche dann aber auch entsprechend möglicherweise Personen (?) also von der Personalabteilung die sagen, okay, warum, (?) dürfen die Frage stellen, warum haben wir so strenge Onboarding-Richtlinien wenn wir dann einen Teil vom Betrieb wohin geben wo wir keine Ahnung haben wie dort Leute aufgenommen werden und vielleicht Leasing Personal da drinnen arbeitet je nachdem ob die gerade einen höheren Bedarf oder weniger Bedarf haben, ob das ein Hire and Fire Unternehmen ist. Also diese Fragen muss man sich gefallen lassen und auch da wieder ist ein checklistenbasiertes System recht gut.

A: Das heißt zum Beispiel als (?) Checkliste, ich sage grundsätzlich, das sind meine Mindestanforderungen im Vertrag, (?) gibt es Rechtsvorschriften für deine Rechtsform

B: Zum Beispiel

A: Wenn ja, bietet (?), dass ich das verwenden kann auch? Das wäre zum Beispiel ein so ein Aufbau von so einer Checkliste oder Frage in dem Sinn, (?) Österreich sage ich jetzt einmal, bietet (?), wenn ja, kann er das erfüllen? Ja, nein. Wenn nicht, fällt er raus.

B: Genau. Eigentlich wenn man auf deine Checkliste eingeht was ich da überlegen würde wäre, dass ich einmal ein Feld habe wie mache ich es jetzt? Von der Security her, wie gut bin ich zum Beispiel beim Onboarding (?) Personal. (?) vertrauenswürdig das Personal in der Softwareentwicklung in Test oder auch im Betrieb. Wie gut habe ich das im Haus jetzt im Griff? So, dann die nächste Spalte, wie gut werde ich das im Griff haben, wenn ich das auslagere? Und da habe ich dabei, wer kann mir diese Fragen beantworten? Vielleicht HR, vielleicht eins Rechts(?), vielleicht das externe Unternehmen, vielleicht alle miteinander und da habe ich aber auch in der Spalte die Möglichkeit drinnen anzukreuzen, ich kann es nicht feststellen. Das muss ich offenlassen. Und am Ende des Tages wie es so schön heißt, schaue ich mir die Gegenüberstellung an von oben bis unten und kann wieder eine Risikoabschätzung machen lassen von den entsprechenden Entscheidungsträgern, denn um die geht es ja letztendlich, gehen wir raus oder gehen wir nicht raus? Das heißt, was du machst und das finde ich mit der checklistenbasierten Version sehr, sehr gut. Ich kann

Entscheidungsträgern und das ist ja das Herz des Risikomanagements oder (?) ich kann Entscheidungsträgern was vorlegen worauf sie entscheiden können

A: Eine Entscheidungsbasis kann ich ihnen geben.

B: Genau. Und nämlich eine Qualifizierte. Du hast überall dort wo du sagst wir haben da ein Qualitätsrating, wenn ich jetzt hernehme von 2, also es ist etabliert, aber wir überprüfen es nicht. Beim Outsourcing Partner sind wir auf einen 4, weil das wissen wir, das ist super (?) und da haben wir die Unterlagen und die Nachweise gesehen (?) vorhanden, passt, Häkchen, also überall dort wo verbessere kann ich schon mal ein Häkchen machen. Überall dort wo ich mich verschlechtere, was passieren kann muss ich, muss ich eintragen ehrlich und dann kann ja der Entscheidungsträger sagen, okay, durch diese Vorteile ersparen uns so oder so viel, nehme ich das und das und das Risiko in Kauf. (?) du weißt genau, wenn du interviewen musst und wer deine Partner sind, das kann durchaus sein, dass die eine oder andere Frage mehreren Parteien stellst und du bekommst ein Summenergebnis und das Zweite ist halt dann, ja manche Dinge kann ich gegenüberstellen, manche weiß ich nur wie ich selber bin, aber nicht das kann ich nicht feststellen oder nicht qualifiziert feststellen wie ich da draußen (?).

A: Sehr gut. (?). Ich glaube, organisatorische Maßnahmen haben wir eh schon angesprochen gehabt in diese Richtung von der Checkliste her ist für mich ganz einfach zu sehen die meisten Dinge sind einfach, dass ich Prozesse, diese Prozesse was für die DSGVO für Richtlinien ausgibt, dass die erfüllt werden müssen, dass ich einfach, erstens einmal, dass ich sie durchführen kann und das ist meistens irgendwie eine technische Anweisung, dass das technisch möglich wird, da wird das meistens Technik notwendig, aber wie ich vorher schon einmal erwähnt habe, ganz wichtig die Prozesse, dass ich immer wieder überprüfe ist das aktuell? Wie wird das durchgeführt, muss ich was ändern, dass ich es weiter durchführen kann? Diese regelmäßigen Prozesse, die Überprüfungsprozesse für diese Sachen, kann ich Informationspflicht geben, kann (?), kann ich das (?)recht erfüllen, kann ich das Recht auf Löschung erfüllen, kann ich (?) auf (?) usw., dass das auch immer wieder regelmäßig überprüft wird, das ist ein Riesenpunkt das diese (?)

B: Das sind die Features, die auch möglicherweise der Outsourcing-Partner mitliefern muss und möglicherweise sogar besser kann als du selber, weil er halt

professioneller ist da drinnen. Aber vielleicht noch, eine Sache, die mir gerade einfällt, erwähnen könnte, (?) Begriff Datenschutzmanagementsystem. Ich glaube, ich habe es dir eh schon mal irgendwann in der Vergangenheit gesagt, da gibt es eine Norm dazu, das ist die BS, British Standard 10 012 oder 13 ich weiß nicht, eine der zwei Zahlen (?) kannst du locker nach googlen, die beschreibt eigentlich nichts anderes als so ein 27001, aber sehr, sehr stark spezifisch auf die Datenschutzgrundverordnungsanforderung ans Managementsystem. Also das ist echt was Empfehlenswertes, ich glaube nämlich auch, dass die als ISO oder EN schön langsam irgendwann einmal aufpoppen wird. ja genau, dass die (?) in Zukunft. Ja genau, schau dir das einmal an du wirst keine Überraschungen erleben, aber du kannst es zumindest erwähnen in deinem Werk. Das ist das eine. Und sonst wie gesagt, es ist die Datenschutzgrundverordnung definitiv kein Show Stopper dafür um in die Cloud zu gehen. Das absolut nicht. Es ist wirklich so, dass man dann sagen kann, ja eigentlich wäre wir dadurch besser und reifer und du bastelst ja an dem Auto nicht herum (?) ein paar kleine Sachen vielleicht oder gar nicht (?), sondern du gibst es dem Profi. Und genauso ist das dort eben auch zu sehen.

A: Gut. Dann danke ich dir für das Gespräch. (?)

B2. Transkript Interview Heinrich Riedl

Das Interview wurde am 4.3.2019 um 16:30 Uhr in Wien 14. Linzerstrasse 211 geführt.

A: Dann starten wir jetzt einmal das Interview. Also danke für das Interview. Du bist ja, du hast das Projekt bei uns gemacht, bei der Allianz für Datenschutzgrundverordnung einführen, aus diesem Grund würde ich gerne mit dir ein bisschen allgemein über dein Wissen, deine Erfahrung von der Datenschutzgrundverordnung und die daraus entstandenen Maßnahmen die zu treffen sind aus deiner Meinung, was die wichtigsten sind und daraus irgendwie mal im ersten Schritt einmal, dass du vielleicht ein bisschen erzählst und Information gibst von der Umsetzung der Datenschutzgrundverordnung im Unternehmen wie das abgelaufen ist und was da die Schwerpunkte auch waren?
B: Ja also das ist korrekt, ich war da Projektleiter zur Datenschutzgrundverordnung, zur Umsetzung, speziell jetzt für Österreich, also innerhalb des Konzerns. Da wir ein weltweiter Konzern sind wurde ein weltweites Projekt sozusagen aufgerufen, APP Allianz Privacy Removal Program. Das heißt, wir waren hier sehr zentral gesteuert von unserer Mutter, natürlich mit den speziellen österreichischen zusätzlichen Anforderungen aufgrund nationaler datenschutzrechtlicher Regelungen. Ich denke, der Ansatz war bezüglich Datenschutzgrundverordnung bei vielen Unternehmen, ich will jetzt nicht sagen ident, aber zumindest sehr gleich. Ich habe mir mal angeschaut welche Bereiche betrifft die Datenschutzgrundverordnung eigentlich, also was regelt die Datenschutzgrundverordnung, eben einmal die Rechte der Betroffenen, ganz allgemein wie man mit Daten umzugehen hat. Wir haben hier in Österreich die doch ein bisschen spezielle Lage, weil wir durch das Datenschutzgesetz vom Jahr 2000 schon im Vergleich zu vielen anderen Ländern ein sehr strenges Datenschutzgesetz hatten und wir im Prinzip begonnen haben mit einer Gap-Analyse, Datenschutzgrundverordnung, Datenschutzgesetz 2000, was ist neu? Hätten wir unter Umständen Gaps, weil einfach ein gewisser Bereich neu oder strenger geregelt wird als schon im Datenschutzgesetz. Bestes Beispiel ist dieses Löschungsrecht was

ja vor allem ein mediales Thema war, speziell jetzt in Österreich war das kein neues Thema, das mussten wir auch schon unter dem Datenschutzgesetz. Ganz allgemein zum Projekt, wir haben hier begonnen, also es waren im Summa zehn große Themen, unter anderem wurde zum Beispiel bezüglich Datenverarbeitungsregister hier, war die Situation vor der Datenschutzgrundverordnung so, dass das die Datenschutzbehörde sozusagen in Österreich verwaltet hat, das heißt wir als Unternehmen mussten ein melden welche Datenverarbeitungen haben wir in einem Unternehmen, das wurde ja auf die Unternehmen sozusagen umgemünzt, dafür sind wir jetzt verantwortlich und einer der wichtigsten Schritte zu Beginn dieser, ich sage es mal, Gap-Analyse war sozusagen eine große Inventur, einmal schauen welche Abteilung im Unternehmen arbeitet mit welchen Daten, wo speichert diese Abteilung diese Daten, also in welchen Systemen, wie lange wird es aufbewahrt und dann entsprechend zu schauen ob Löschkonzept vorhanden sind, ob die angepasst werden müssen oder ob man sozusagen das so lassen kann wie es bereits war. Das war einmal so der große Beginn. Auch sehr von der Gruppe getrieben, auch eine Art Readiness Assessment Questionaire wo die Datenschutzgrundverordnung mehr oder weniger mit Fragen zusammengefasst war ob wir gewisse Bereiche so schon erfüllen oder nicht und dann mit entsprechendem Actionplan, wenn dem nicht so war diese Gaps sozusagen zu beheben sind. Begonnen haben wir schon und da weiß ich, da waren wir wirklich sehr früh dran, zweieinhalb Jahre vor Inkrafttreten der Datenschutzgrundverordnung. Das war mal so ein grober Überblick.

A: Gut, das war die Umsetzung wie wir gestartet sind und wie wir das gemacht haben die Umsetzung. Jetzt vielleicht die Info von dir die ich noch gern hätte ist, was sind deiner Meinung nach den Schwerpunkten bei der Umsetzung der DSGVO allgemein für Unternehmen? Was sind wirklich die Knackpunkte für diese Umsetzung? Also das ist unbedingt notwendig oder das sind Themen, die wirklich schwierig sind bzw. unbedingt erfüllt werden müssen.

B: Natürlich vor allem das mediale Thema dieses Daten löschen. Also das ist natürlich ein großer Punkt, weil das für sehr viel Verwirrung gesorgt hat. Wenn man sich die Medien davor angeschaut hat die dann kommuniziert haben, wenn jetzt ein Vertrag wegfällt muss das Unternehmen diese Daten löschen, stimmt so nicht. Also wir haben genauso die nationalen Aufbewahrungsfristen, UGB, BAO, die auch ab

25. Mai 2018 gelten, genauso wie es am 24. Mai 2018 gegolten hat. Das war hauptsächlich ein mediales Thema. Wenn dann diese Fristen natürlich auch abgelaufen sind, dann musste man auch schon vor der DSGVO natürlich die Daten löschen. Was natürlich noch viel schlimmer war medial waren die potenziellen Strafen die schon vorher von einer Verwaltungsstrafe jetzt speziell in Österreich bei Verstößen gegen das Datenschutzgesetz von maximal 25.000 Euro, ab 25. Mai 2018 aufgrund der Datenschutzgrundverordnung bemisst es sich dann nach dem Konzernumsatz bzw. nach dem Umsatz des Unternehmens bis zu 4% dieses Umsatzes u das geht dann schon unter Umständen in die Millionen. Wenn man sich viele Klein- und Mittelbetriebe anschaut, die haben niemals Daten gelöscht, die haben das auf den Festplatten irgendwo liegen, zum Beispiel auch hier war unser Ansatz, unser System wo wir die Kundendaten verwalten haben wir uns wirklich alle Designs angeschaut mit den hinterlegten Aufbewahrungsfristen, passt das mit der DSGVO überein, also löschen wir, löschen wir nicht? Genauso wie natürlich in allen anderen Systemen. Also im Prinzip haben wir eine große Inventur gemacht, die Informationen waren natürlich alle vorhanden, wir haben das Ganze zentralisiert, eben aufgrund dieses Projektteams schöne Übersichten gemacht welche Abteilung arbeitet mit welchen Daten, fallen die überhaupt in die Datenschutzgrundverordnung weil es gibt ja viele Unternehmen, viele Bereiche, viele Abteilungen die schon mit anonymisierten Daten arbeiten weil es nur noch irgendwelche Zahlen sind, aber keine Namen und keine Daten die unter die DSGVO fallen, ist das überhaupt relevant wenn ich jetzt an die IT denke mit voll anonymisierten Testdatenbanken die nicht unter die DSGVO bezüglich des Löschens fallen, natürlich IT-Security, ein anderes Thema, aber jetzt bleiben wir beim Bereich löschen, da haben wir dieses Thema nicht. Eine Rieseninventur welche Abteilung arbeitet mit welcher Software und mit welchen Daten und wo speichert sie es, wo schickt sie sie hin, ist es nur innerhalb vom Unternehmen oder unter Umständen auch in ein anderes Land? Also wirklich eine komplette Inventur. Wir haben auch zum Beispiel Datenflussdiagramm erstellt, ein komplettes, wie hängt unter Umständen Software miteinander zusammen wenn ich jetzt denke SAP, Data Warehouse etc. und welche Fachbereiche greifen hier auf welche Datentöpfe im Hintergrund zu und das hilft einem dann natürlich enorm zu sehen um welchen

Datentopf müssen wir uns eigentlich kümmern, was macht die Software eigentlich mit diesen Daten.

A: Das heißt, kann man sagen, es sind grundsätzlich einmal die Daten erhoben worden

B: Genau

A: Und dann wer arbeitet mit diesen Daten wo drin

B: Also wirklich speziell runter auf die einzelnen Abteilungen, wirklich welche Abteilung arbeitet mit welchen Daten, müssen wir dort uns das eigentlich näher anschauen weil das Daten sind die unter die Datenschutzgrundverordnung fallen und dann eben was macht diese Abteilung mit diesen Daten?

A: Das heißt, es wird auch überprüft ob diese Abteilung überhaupt mit diesen Daten zu arbeiten hat, ob das überhaupt notwendig ist

B: Natürlich entsprechend, im Zuge dessen natürlich auch dem Need-To-Know-Prinzip, wir haben uns einmal angeschaut, ist das überhaupt notwendig? Wir haben zum Beispiel (?) Software wie SAP haben wir auch eine große Aufstellung gemacht wer im Unternehmen hat eigentlich Zugriff zu dieser Software? Und in welchem Ausmaß hat der Administratorenrechte, hat irgendwelche speziellen Berechtigungen für die Software und dann auch gleichzeitig in groß angelegten Aktionen an alle Vorgesetzten geschrieben, braucht der das überhaupt? Also wirklich jedes Recht überprüft, genauso wie in unserem Kundenverwaltungssystem, haben wir uns das genau angeschaut welcher Mitarbeiter das Organisationsmodell sozusagen im Hintergrund, passt das? Entspricht das dem Need-To-Know-Prinzip?

A: Wir haben vorher schon einmal gesprochen, also was mich nur interessieren würde, ist es allgemein in der DSGVO nicht nur das Löschen, sondern allgemein was sind so die Schwerpunkte der DSGVO? Also als Beispiel zu nennen, dass es gewisse, also es gibt gewisse Rechte der Betroffenen zum Beispiel oder dann gibt es weiß ich nicht, technische Maßnahmen die getroffen werden müssen oder so, so in diese Richtung einmal nur kurz überblicksmäßig von dir vielleicht, was glaubst du, sind diese zentralen Schwerpunkte in der DSGVO die betrachtet werden müssen?

B: Natürlich für unsere Kunden am wichtigsten sind natürlich wie schon angesprochen die Rechte der Betroffenen sozusagen. Das heißt, welche Rechte haben unsere Kunden aufgrund der Datenschutzgrundverordnung und da war für uns der

wichtigste Punkt welches dieser, es sind im Prinzip 6 Rechte der Betroffenen, ist eigentlich neu unter der DSGVO hier in Österreich? Und im Endeffekt ist das nur ein einziges, also wenn man es zusammenfasst, die Rechte der Betroffenen sind einerseits Informations- und Auskunftsrechte, das heiß, da müssen wir zu Beginn einmal dem Kunden sagen warum nehmen wir seine Daten auf, Informationspflichten und was machen wir damit? So, Auskunftsrecht ist dann schon wenn wir schon einen Vertrag mit dem Kunden hätten, darf man jeder Zeit nach Artikel 15 der Datenschutzgrundverordnung von uns wieder so ähnlich wie die Informationspflichten verlangen, dass wir ihm sagen welche Daten haben wir von ihm, welchen möglichen Dritten haben wir seine Daten weitergegeben wenn ich jetzt an einen Schaden zum Beispiel denke, an eine Werkstätte etc. was machen wir mit seinen Daten? An wen haben wir sie weitergegeben? Wie lange speichern wir sie etc.? Das war beides nicht neu, das gab es auch vorher schon unter dem Datenschutzgesetz 2000. Dann natürlich das Recht auf Richtigstellung und Löschung. Wie gesagt, Richtigstellung wenn der Kunde jetzt, weiß ich nicht, heiratet und er hat einen neuen Namen und dass wir dann den aktuellen Namen anführen, sage ich jetzt einmal, ist nicht so das große Thema. Das Recht auf Löschung, wie gesagt, ich mache es jetzt nur ganz kurz wie gesagt, ist auch nicht neu in Österreich, das Widerspruchsrecht hat es vorher auch schon gegeben, Widerspruchsrecht wenn der Kunde keine direkte Werbung zum Beispiel haben wollte in Österreich auch mit der Robinson-Liste zum Beispiel verankert, das einzig wirklich neue Recht jetzt für uns gesehen war das Recht auf Datenübertragbarkeit, das heißt, dass wir die vom Kunden zur Verfügung gestellten personenbezogenen Daten in einem maschinenlesbaren Format von einem Anbieter A zum Anbieter B übermitteln, das war das einzig wirklich Neue und das haben wir zum Beispiel mit einer Lösung in der IT sichergestellt, ich darf aber verraten, wir haben heute den 4. März 2019, also bald ein Jahr Datenschutzgrundverordnung, bis jetzt gab es keinen einzigen Kunden der das wollte. Also es hat bei uns noch niemand angerufen und gesagt, liebe Firma A, bitte schickt meine Daten an die Firma B. Das war eigentlich das einzige was wirklich komplett neu war und so sind wir auch an die Sache herangegangen. Ganz allgemein zu den Rechten der Betroffenen, nichtsdestotrotz wir wussten ja nicht was hier auf uns zukommt, wie viele Kunden rufen am 26., 27. Mai 2018 bei uns an und

sagen eben, ich habe gestern mein Auto abgemeldet, bitte löscht heute meine Daten. Wir haben natürlich auch eine entsprechende eh so wie eigentlich alle großen Unternehmen eine eigene Email-Adresse eingerichtet, wir haben natürlich einen Datenschutzbeauftragten, war ja auch ein großes Thema, das hatten wir aber auch in der Allianz schon zuvor, das ist auch nicht neu und wir haben uns dafür entschieden, dass wir all diese Themen zentralisiert, also die jetzt speziell diese Rechte der Betroffenen betrifft, zentralisiert von unserem Datenschutzbeauftragten bearbeiten lassen. Ein kompetenter juristischer Mitarbeiter der auch Teil des Projektes war, der das Unternehmen kennt, der weiß eben auch in welchem, welche Abteilung arbeitet mit welchen Daten, sich in unseren Systemen auskennt damit er eben seine Arbeit auch entsprechend ausführen kann.

A: Was mich noch interessieren würde aus Sicht der Datenschutzgrundverordnung auch, haben wir eigene Prozesse einführen müssen, die es vorher nicht gegeben hat dafür? Als Beispiel vielleicht von mir genannt, dass ich einen regelmäßigen Review der Datenverwendung zum Beispiel oder vielleicht auch

B: Naja, es gab, also ja und nein. Sagen wir so, wir haben das Ganze jetzt sozusagen in eine gewisse Richtung zum Datenschutzbeauftragten gelenkt. Aber wenn ich jetzt an gewisse Systeme denke, gab es auch vorher schon monatliche Listen, die ausgeschickt wurden an zum Beispiel an die O&P wer hat eigentlich diese Recht, nur natürlich das Scope wie man mit diesen Daten umgeht hat sich ein bisschen geändert. Vorher hat man natürlich auch darauf geschaut wer hat welche Rechte und warum. Auch vorher musste man schon eine entsprechende Anforderung stellen, wenn man eine spezielle Software haben musste, also hier waren wir schon zu 99,99% datenschutzgrundverordnungskonform. Was wir halt jetzt gemacht haben, ist, dass der Datenschutzbeauftragte hier natürlich überall involviert war. Bezüglich Prozesse, es war auch vorher schon so, dass sämtliche Anfragen zu Daten löschen, Auskunftsrecht was in dieser Form ja auch unter dem Datenschutzgesetz schon gegeben hat, vielleicht jetzt nicht so detailliert, aber es gab das Auskunftsrecht vorher schon. Es war immer auch jetzt im Kundenservice, dass das in der Rechtsabteilung bearbeitet wurde. Wir haben das im Prinzip nur umgelenkt, wir haben bestehende Prozesse zum Datenschutzbeauftragten umgelenkt. Aber es gab es vorher auch schon. Wir haben natürlich eine Arbeitsanleitung geschrieben,

wir haben Awareness geschafft, wir sind sogar rausgefahren in die Bundesländer auf Landesdirektorleitungen, haben das Ganze vorgestellt und die Awareness einfach verstärkt und, also ich möchte jetzt nicht sagen, dass wir Prozesse komplett neu aufgesetzt haben, sondern wir haben bestehende Prozesse adaptiert und ich glaube, das ist schon, wie gesagt, weil wir in Österreich mit dem Datenschutzgesetz schont teilweise sehr nahe an der Datenschutzgrundverordnung dran waren. Aber natürlich, wir haben jetzt auch speziell für das Kundenservice haben wir eine Arbeitsanleitung sehr wohl geschrieben wie sie damit umzugehen haben, wenn jetzt ein Kunde, eben weil das damals auch so ein mediales Thema war, wie haben sie damit umzugehen, was haben sie damit zu tun, aber kompletter neuer Prozess wüsste ich jetzt nicht was wir neu aufgesetzt haben. Wie gesagt, also den Datenschutzbeauftragten hätten wir vorher nicht haben müssen, in der AIB aber jetzt speziell auf die AEV gesehen nicht, hatten wir schon, da mussten wir den nur organisatorisch neu eingliedern. Warum? Weil der Datenschutzbeauftragte unter der DSGVO sozusagen weisungsbeigestellt sein muss und dem höchsten Management berichten muss und bis dahin war es der Bereichsleiter Recht und somit in einer Hierarchie, da haben wir jetzt zum Beispiel eben den als Stabsstelle direkt berichtend an den Vorstand, weiß jetzt nicht ob man da sagen kann einen Prozess neu aufgesetzt zu haben.

A: Aber das heißt im Prinzip auch, dass durch dieses Verarbeitungsregister gibt es ja für jegliche Verarbeitung die wir haben drinnen, ja auch einen Verantwortlichen für diesen Verarbeitungsschritt und ist für den eine gewisse Verantwortung auch aufgetaucht in der Firma sage ich mal, oder hat der rechtliche Verantwortung dafür auch für diesen Schritt übernommen nachher oder ist das?

B: Nein, man kann die Haftung vom Unternehmen der Datenschutzgrundverordnung nicht auf einzelne Mitarbeiter runterbrechen. (?)

A: Gut, ja. Also einmal ich glaube, Datenschutzgrundverordnung haben wir, hätte ich jetzt für mich einmal recht gut aus meiner Sicht einmal erklärt, hast du vielleicht noch Sachen, die du dazu bringen willst die wichtig sind?

B: Was natürlich noch ganz wichtig ist, ist was ich vorher schon angesprochen habe, dieses ganze Thema bezüglich Awareness schaffen. Es gab natürlich schon vor der Datenschutzgrundverordnung, ich will nicht sagen Arbeitsanleitungen, aber

natürlich gewisse Richtlinien wie im Falle des Falles Databreach-Management sage ich als Stichwort, Incident-Management umzugehen ist. Dieser ganze Prozess hier ist nämlich schon etwas neu unter der Datenschutzgrundverordnung und zwar müssen natürlich gewisse Datenschutzverstöße jetzt innerhalb von 72 Stunden an die Datenschutzbehörde gemeldet werden. Aber nicht jeder Verstoß, sondern gewisse Verstöße nämlich dann, wenn es möglicherweise zur Beeinträchtigung der persönlichen Rechte oder wenn es um personenbezogene Daten von unseren Kunden geht. Beispiel wenn jetzt eine Datei entwendet wird wo vollanonymisierte Daten drauf waren, dann interessiert das die Datenschutzbehörde nicht, sind das tatsächlich Kundendaten dann müssen wir diesen Databreach, diesen Datenverlust binnen 72 Stunden an die Datenschutzbehörde melden. Hier haben wir natürlich wie gesagt vorher auch schon Mechanismen gehabt mit einer eigenen Email-Adresse wohin solche Fälle zu melden sind, aber auch hier haben wir nochmal große Awareness geschaffen, hier haben hier, das ist auch ein Teil vom Protecture and Resilience haben wir das hier eingebettet, wir haben für verschiedene Szenarien gewisse Krisenteams die zusammentreffen und hier haben wir auch jetzt zum Beispiel den Datenschutzbeauftragten überall mit eingebunden der das dann entsprechend mit beurteilen kann. Und ganz wichtig, wir haben vor Inkrafttreten der Datenschutzgrundverordnung diesen Prozess nochmal überarbeitet und ganz wichtig nochmal mit einer kurzen Information an alle Mitarbeiter der Allianz, also egal ob Außendienstmitarbeiter, GD-Mitarbeiter, AKS-Mitarbeiter, Vertriebsmitarbeiter, wer auch immer, nochmal in Erinnerung gerufen, auch was sie zu melden haben. Also mit Beispielen. Verlust eines Laptops, das ist ja eigentlich als Databreach zu sehen und dann natürlich auch noch einmal was er dann tun soll und warum er das tun soll. Und das funktioniert ganz gut, das war so ein großer Punkt

A: Das heißt, ich kann mich erinnern, glaube ich, dass so ein E-Learningthema gegeben wo Mitarbeiter ganz einfach mitgelernt haben, wenn das passiert, was würdest du dann tun? Was ist richtig, was ist falsch? Usw.

B: Unabhängig von dieser, ich sage mal Incident, Databreach-Management-Prozess gab es für alle Mitarbeiter der Allianz ein Training, das war eine knappe Stunde wo wir wirklich anhand, also das ist ein gruppenweites Tool wo ein jeder Mitarbeiter

verpflichtend ein Training absolvieren musste mit im Prinzip allen relevanten Kapiteln der Datenschutzgrundverordnung, also von was ist die Datenschutzgrundverordnung, welche Daten regelt die Datenschutzgrundverordnung, was sind eben diese Rechte der Betroffenen, also unserer Kunden bis hin zum Databreach-Management? Was ist der Datenschutzbeauftragte? Was macht der Datenschutzbeauftragte? Was ist neu? Die Privacy by Design, Privacy by Default, all das wurde mit Fragen, die der Mitarbeiter beantworten musste sozusagen verpflichtend von einem jeden Mitarbeiter durchgeführt. Hat eine knappe Stunde gedauert und auch hier war es egal ob das jetzt ein Kundencenter-Mitarbeiter, von unserem Kundenservice ein Mitarbeiter, auch unsere Vorstände haben das machen müssen, also wirklich ein jeder Mitarbeiter hat das gemacht damit er weiß was ist Datenschutzgrundverordnung eigentlich, warum müssen wir uns damit beschäftigen. War verpflichtend, wurde vom Datenschutzbeauftragten auch sozusagen überwacht, wurde reported wer was gemacht hat und wer nicht und das waren mehrere Module, aber damit ist die Sache noch nicht erledigt, da gibt es ein Modul, sozusagen zur Wiederholung und alle zwei Jahre gibt es dann sozusagen eine Auffrischung eben auch anhand was ist jetzt wirklich, irgendwelche Anpassungen vielleicht oder dass man das auch einfach dieses Wissen auffrischt.

A: Das heißt natürlich, alle diese Prozesse müssen natürlich IT-unterstützt passieren dahinter auch, sind auch die technischen Maßnahmen nachher auch noch mit anderen Kollegen besprechen will. Ich möchte noch allgemein vielleicht noch eine Frage dazu stellen, warum hat man sich das überhaupt angetan als Firma? Nur weil das DSGVO-Gesetz jetzt gekommen ist am 25. Mai oder hat das einen, was sind wirklich die ausschlaggebenden Punkte gewesen warum man das getan hat? Diese ganzen Aktionen gestartet hat und was ist wirklich der ausschlaggebende Punkt dafür? Also ja das ist ein Gesetz, ist halt so, haben wir vorher Datenschutzgesetz auch gehabt, aber warum hat man das Ganze nochmal aufgerollt? Warum aus deiner Sicht?

B: Naja es geht natürlich in Zeiten wie diesen um den Schutz, ich meine, die Kunden geben uns ihre persönlichsten Informationen und das sind Kontodaten, Beziehungsstatus etc. und die Unternehmen haben schon dafür zu sorgen, dass diese

Daten ordnungsgemäß nach dem Stand der Technik verarbeitet werden, aufbewahrt werden und entsprechend auch behandelt werden, diese Awareness zu schaffen auch vor allem im Unternehmen. Wir haben es halt wie gesagt in Österreich durch das Datenschutzgesetz ein sehr hohes Niveau bezüglich Datenschutzes. Also wenn man jetzt in andere Länder schaut, macht es schon Sinn. Der Hintergedanke der Datenschutzgrundverordnung von der EU, ich meine, es trifft, war natürlich, wenn wir jetzt denken an Facebook und Google, Was dort ausschlaggebend nicht wir jetzt als Versicherungen oder als Banken oder der Klein- und Mittelunternehmen und da wurde einfach versucht das auf ein Niveau auf ein gleichmäßiges, überall gleichgeltendes Niveau zu heben, diese Datensicherheit eben Stand der Technik.

A: Vielleicht ein Punkt noch abschließend zur Datenschutzgrundverordnung vielleicht nicht direkt aber doch, in meiner Arbeit geht es ja darum, dass ich feststellen will ob man den Kernprozess der Versicherung, die Kernprozesse der Versicherung in einer Public Cloud-Lösung, Infrastructure, Plattform, Software das muss man sich genau anschauen, umsetzen kann und was für Maßnahmen notwendig sind technisch und organisatorisch damit man die Datenschutzgrundverordnung nicht verletzt? Jetzt ich weiß du bist kein Techniker, aber grundsätzlich einmal von deinem Bauchgefühl hergesehen, glaubst du, dass es möglich ist?

B: Schwierige Frage ja, aber grundsätzlich die Datenschutzgrundverordnung spricht ja immer vom Stand der Technik bezüglich jetzt IT-Sicherheit und da muss man natürlich schauen, diese Cloud, wenn die dem Stand der Technik entsprechend abgesichert ist und vor allem überhaupt einmal die Definition was ist eine Cloud? Das ist ja mal schon, ich glaube nicht, dass es da eine juristische Definition davon gibt, aber ja, neuer Stand der Technik jetzt gerade in der IT ändert sich so schnell, unter Umständen über Nacht, dass es wahrscheinlich für die Unternehmen sehr schwierig oder mit einem enormen Kostenaufwand verbunden sein wird hier jederzeit den Stand der Technik zu gewährleisten, aber wenn man keine Kosten und Mühen scheut, also aus meiner, ich bin Wirtschaftsjurist, aus meiner

A: Da komme ich vielleicht noch dazu, weil es wird, das Ganze wird so aufgesetzt sein, dass ich eben zu einem Ergebnis bei der Arbeit kommen will, aber auch eine Checkliste machen will oder einen Framework schaffen will mit unterschiedlichsten

Checklisten zu sehen ob ich bestehende Lösungen schon umgesetzt habe oder auch eine Verfahrensanweisung drinnen quasi habe wie wähle ich einen Public Cloud-Provider aus, was muss der erfüllen? Was sind die vertraglichen Inhalte die notwendig sind? Was sind die organisatorisch notwendigen Maßnahmen? Und was sind die technischen Maßnahmen? Und das aufgebaut auf die verschiedenen Ebenen von Cloud und da ist ein Thema halt natürlich auch, da du ja Wirtschaftsjurist bist, ist für mich auch eine Checkliste was zu den vertraglichen Inhalten angeht. Jetzt was würdest du sagen, gibt es spezielle Auswirkungen der Datenschutzgrundverordnung die ich in so ein Outsourcing oder Cloud, sagen wir so, Cloud-Provider möglicherweise erfüllen muss? Oder sagen wir so, allgemein, ich habe einen Dienstleister der mir etwas im Versicherungsbereich, im Kernprozess macht, gibt es da bestimmte Sachen, die dir einfallen würden sofort wegen der Datenschutzgrundverordnung, das sind Punkte, die ich auf jeden Fall vertraglich festgelegt haben muss, bei einem Vertrag mit denen.

B: Ja. Da haben wir es natürlich viel leichter als jetzt bezüglich IT-Stand der Technik weil man hat ja gerade jetzt in der Datenschutzgrundverordnung im Prinzip zwei wesentliche Rollen, das eine ist der Auftraggeber und das andere ist der Dienstleister und für beides gibt es entsprechende Pflichten sowohl für den Dienstleister als auch für den Auftraggeber und die kann man sehr wohl in einen Vertrag gießen, das haben wir ja auch teilweise machen müssen mit unseren ganzen Dienstleistern, entsprechende Vereinbarungen zu treffen, wie haben sie mit den Daten umzugehen usw. usf. Also hier eben auf zum Beispiel Datensicherungsmaßnahmen gemäß Paragraph-14-Datenschutzgesetz sind zu treffen etc. Also hier rechtlich gesehen tun wir uns schon leichter so einen Vertrag aufzusetzen. Wie dann das Unternehmen da jetzt speziell Stand der Technik, IT-Security umzusetzen hat, das wird schon viel schwieriger.

A: Okay. Und

B: Aber vertraglich zwischen Auftraggeber und Dienstleister hier einen entsprechenden Vertrag aufzusetzen, das ist nicht das Thema. Also das ist ja, gibt es ja ganz viele Musterverträge auch, WKO, überall auf den ganzen Seiten von denen sind wir teilweise auch überschwemmt worden, weil die auch teilweise jetzt die Rollen ein bisschen unterschiedlich gesehen wurden, aber das war alles nicht das

Thema. Aber vertraglich sehe ich da überhaupt kein Thema, das kann man machen.
A: Okay. Und Richtung IT-Dienstleister gesehen sage ich jetzt mal so, habe ich da vertraglich, fallen dir da bestimmte Sachen ein, die man da auf jeden Fall beachten muss einmal? Das heißt, ich denke mir halt grundsätzlich, muss ich die Erfüllung der Datenschutzgrundverordnung immer einfordern in jedem Vertrag, jegliche Zusammenarbeit nehme ich einmal an.
B: Natürlich Überprüfungsrecht ist, dass man sich das anschauen darf wie dieses Unternehmen diese Punkte erfüllt und die sollte man auch entsprechend nutzen. Im Falle des Falles, dass man nachweisen kann jetzt als Auftraggeber, man hat seinen Dienstleister entsprechend überprüft, diese Rechte hat man auch, das wird, das Thema DSGVO, es gibt ja hier noch keine Erfahrungswerte jetzt bezüglich, möchte jetzt nicht sagen Urteile, aber wie da die Datenschutzbehörden im Falle des Falles dann wirklich entscheiden. Das wird noch viele Jahren dauern bis man hier wirklich Erfahrungswerte haben wird.
A: Eine Frage hätte ich noch und zwar jetzt wenn man IT-Dienstleister und vertragliche Inhalte gemeint haben und auch Umsetzung, dass man es kontrollieren kann usw. jetzt in Bezug auf Public Cloud dann, bekannt ist das Thema, das sind natürlich Riesenunternehmen wie AWS, Google, Microsoft, also da wird ein kleineres Unternehmen, vielleicht jetzt nicht die Allianz, die hat vielleicht schon ein bisschen einen größeren Stellenwert, aber kleinere Unternehmen oder kleinere Versicherungen möglicherweise, werden da kaum Möglichkeiten haben diese wirklich inhaltlich zu überprüfen ob sie in ihrem Betrieb Amazon usw. dann auch handeln. Wie denkst du, kann man das abfangen? Kann man das vertraglich sage ich jetzt einmal?
B: Ja natürlich sicher durch gewisse Zertifikate. Es muss irgendwie eine Art Standard natürlich ausgearbeitet werden in Zukunft. Also soviel ich weiß, der deutsche TÜV ist hier an etwas dran möglicherweise etwas auszuarbeiten, aber das ist wirklich der Punkt einerseits natürlich gewisse Zertifizierungen die es vielleicht jetzt ja schon gibt und ansonsten muss ich ehrlich gestehen natürlich die ISO-Zertifizierungen 27001 und 27008, aber ich denke, hier wird es auch speziell jetzt dann in den nächsten Jahren auch für die Datenschutzgrundverordnung etwas geben, aber wie gesagt, das ist jetzt wieder Stand der Technik. Momentaner Stand

der Technik sind diese ISO-Zertifizierungen und auf die muss man sich natürlich verlassen können und was die Zukunft bringt jetzt in Richtung Datenschutzgrundverordnung

A: Also du siehst das vertraglich und rechtlich auch so, dass man sich auf gewisse Standards und Überprüfungen nach Normen oder Zertifizierungen, die halt Stand der modernen Technik oder Art sind, bei den Großen natürlich verlassen muss können. Ich denke mir halt immer wieder, erstens einmal betreiben sie sich selber auch, also die werden jetzt nicht schlecht sein und sie sind ja Riesenkonzerne auf diesen Plattformen unterwegs und ein gewisses Vertrauen wahrscheinlich muss einfach trotzdem auch da sein, wenn man mit solchen Firmen zusammenarbeitet.

B: Ja natürlich man darf ja nicht vergessen, was wollte die Datenschutzgrundverordnung? Die Datenschutzgrundverordnung wollte jetzt ja nicht das reihenweise Unternehmen zusperren, weil sie sich irgendwelche Datensicherungsmaßnahmen nicht leisten können oder nicht wissen was sie tun sollen, sondern es ging hauptsächlich einmal um Awareness zu schaffen und eben noch einmal dieser Stand der Technik. Was anderes wäre Stand der Wissenschaft, aber es geht ja bei per se um den Stand der Technik. Weil der Stand der Wissenschaft dann nochmal eine Stufe drüber, aber was bringt es mir jetzt zum Beispiel vorzuschreiben ein Datenaustausch muss Stand der Wissenschaft entsprechen und das können genau zwei PCs, das kann der Acer-PC und ich weiß nicht welcher noch, sondern es steht ja extra drinnen Stand der Technik und darum geht es ja, dass man in den Unternehmen die Awareness schafft, geht mit den Daten der Kunden so um wie es ihr auch gerne hättet. Das ist ja im Prinzip, dass man hier einheitlich den Kunden nochmal genau sagt, was darfst du vom Unternehmen verlangen, dass das überall einheitlich ist innerhalb der EU.

A: Gut, ich sage mal danke für das Gespräch.

B3. Transkript Interview Stefan Biehl

Das Interview wurde am 6.3.2019 um 14:00 Uhr in Wien 14. Linzerstrasse 211 geführt.

A: Servus Stefan, das Interview, das Projekt habe ich dir vorher schon kurz vorgestellt, worum es geht, wir werden ungefähr, schätze ich mal, eine dreiviertel Stunde, Stunde brauchen dafür. Ich würde gleich einmal ins Thema einsteigen, du bist ja Internet Security Officer bei der Allianz Technology GmbH in Österreich. Ich würde gerne zu den Themen Datenschutzgrundverordnung, IT-Sicherheit und Public Cloud und da ich ja eine Checkliste auch erstellen will, ein Feedback zum Aufbau und Inhalt von dieser Checkliste von dir in diesem Interview abfragen. Beginnen wir mit dem Thema vielleicht Datenschutzgrundverordnung da hätte ich die Frage, wie siehst du die Umsetzung der DSGVO in Unternehmen aus deiner persönlichen Sicht?

B: Also die Umsetzung der DSGVO hat aus unternehmerischer Sicht besonders für den Kunden Vorteile, sprich es erhöht sich für den Kunden die Transparenz wie, wo, wie viele seiner Daten für was für Zwecke verarbeitet werden, sprich hier müssen einfach Schnittstellen geschaffen werden um dem Kunden basierend auf der DSGVO dann die ihm rechtens zustehenden Informationen zukommen zu lassen, das beinhaltet zum Beispiel das Recht auf Berichtung der Daten, das Recht auf die Korrektur oder generell einmal den Einblick in die Daten was für Daten gesammelt werden, in welchem Ausmaß sie weiter verwendet werden oder in welcher, an welche Drittprovider sie zum Beispiel weitergegeben werden. Die Erfahrungen die daraus entstehen können recht unterschiedlich sein, auf der Firmenseite ist es oft ein sehr großer Aufwand seinen eigenen Datenbestand auf diesem Detailgrad für den Kunden auszubreiten, sprich da muss einfach rechtzeitig geschaut werden, dass zu dem Stichtag X die Mechanismen, Prozesse, Protokolle und Arbeitsanweisungen zur Verfügung stehen, sollte ein Kunde diese Auskunft von der Firma verlangen damit das automatisiert und möglichst schnell und unkompliziert auch durchgeführt werden kann. Anfangs wird das wahrscheinlich noch ein manueller Prozess sein, aber im Laufe der Entwicklung der DSGVO werden immer mehr Automatismen und Mechanismen zur Verfügung stehen damit die Firmen diese Auskunft möglichst

rasch und kostengünstig dem Kunden zur Verfügung stellen können. Die konkreten Umsetzungen die auf eine Firma zukommen bezüglich der DSGVO können unterschiedlichste Maßnahmen haben, das ist einerseits die schon vorher angesprochenen Schnittstellen bereit zu stellen um dem Kunden eine Auskunft über die Daten zu geben, andererseits müssen dementsprechend auch neue organisatorische Schreiben ausgeschickt werden damit der Kunde auch mit den neuen Datenschutzgrundverordnungsrichtlinien einverstanden ist, sprich hier gibt es auf Firmenseite noch einen organisatorischen Aufwand den Kunden quasi rechtzeitig über die neue Änderung und Gesetzeslage zu informieren und sich zusätzlich wieder seine Zustimmung zu holen, dass die Datenweiterverarbeitung stattfinden darf.

A: Es war aber, hast du jetzt gesagt, ist eine einmalige Aktion in dem Sinn jetzt mal gewesen bei der Einführung, ist es dann später noch mehr notwendig?

B: Die Rechte, also bei der Einführung ist es genau wie schon vorher gesagt, ist es recht wichtig diese Einverständniserklärung für bestehende Kunden zu erneuern bzw. die nochmal darauf hinzuweisen, bei Neukunden wird das automatisch dieser Informationstext in die AGBs oder in die Kundendokumente gleich eingetragen, sprich der Kunde ist bei einem Informationsgespräch oder bei einem Vertragsabschluss oder ähnlichem gleich schon informiert über seine Rechte, was natürlich permanent zur Verfügung stellen muss sind diese Schnittstellen oder Prozesse um dem Kunden diese Auskunft zeitnah und auch richtig zur Verfügung zu stellen.

A: Okay. Jetzt eine Frage dazu, ich habe da die Evaluierung der Daten, du hast vorher schon angemerkt die Schwierigkeit ist oder eine der Hauptschwierigkeiten war einmal zu evaluieren was habe ich denn überhaupt für Daten und wo habe ich diese Daten, wie verarbeite ich diese Daten. Also siehst du da auch, das war der Hauptpunkt, der Start für die ganze Umsetzung ist dieses Thema und darum auch der wichtigste Punkt eigentlich einmal, dass man überhaupt weiß wo hat man und was hat man für Daten.

B: Genau, oft erheben Unternehmen in großem Umfang viele unterschiedliche Daten auch aus den unterschiedlichen Systemen die für den Kunden jetzt nicht direkt so transparent sichtbar sind und im Zuge dieser DSGVO-Umstellung muss

natürlich dann auch evaluiert werden aus Firmensicht was darf ich denn überhaupt noch erheben, ist diese Erhebung so wie ich sie jetzt mache für die neue Gesetzeslage noch passend oder muss ich sie dementsprechend verändern und anpassen.
A: Das heißt auch im Prinzip, den Schutzbedarf der Daten auch festlegen.
B: Genau, wir sprechen da von einer groben Datenklassifizierung, sprich man teilt die Daten in so genannte Schutzbedarfskategorien ein oder bei uns auch Datenkategorien genannt, diese können je nach Unternehmen von high bis super critical sein wobei das Gesetz ja auch schon gewisse Vorgaben gibt ab was für einer Kategorie die Daten sensibel, personenbezogen oder einen gewissen Schutzwert genießen, also generell sprechen wir hier von Daten die Auskunft über ein Individuum und dessen Persönlichkeit geben, sprich von politischem Interesse oder anderen Orientierungen, solche Daten dürfen dann einfach nicht erhoben werden bzw. nur mit expliziter Einwilligung des Kunden.
A: Die Datenschutzgrundverordnung legt ja eigentlich nur zwei Arten von Daten fest, die geschützt werden müssen.
B: Genau, das sind einmal die sensiblen Daten und die personenbezogenen Daten.
A: Okay, also diese besonders schützenswerten personenbezogenen Daten. Okay. Es gibt dann noch ein Thema dazu, jetzt haben wir die Daten und alles, man muss ja auch irgendwie auch festlegen wer darf wo was an Daten verarbeiten oder sehen oder überhaupt bearbeiten. Da muss ja jede Firma irgendwie auch festlegen was darf wer. Ist das bei uns in der Firma zum Beispiel jetzt bei der Allianz Technology so durchgeführt worden, kennst du das oder?
B: Ja natürlich ist das so durchgeführt worden, da gibt es eben eine Erhebung welche Daten erhoben werden, die werden in Kategorien eingeteilt und basierend auf dieser Kategorie werden dann dementsprechende technische oder aber auch organisatorische Maßnahmen getroffen um den Mindeststandard oder darüber hinaus einen schützenswerten oder ein schützendes darum aufbauen, sprich Daten die eine gewisse Kritikalität haben dürfen zum Beispiel nur verschlüsselt übertragen werden und, und, und, da gibt es dann diverse technische Richtlinien die man dann umzusetzen hat, basierend auf der Datenklasse die mir die Daten halt bieten.
A: Also das war einmal im Prinzip zum Thema Datenschutzgrundverordnung, jetzt

kommen wir ein bisschen zu deinem Spezialgebiet die IT-Security und die daraus entstehenden Maßnahmen. Ich sehe, allgemein einmal auf was baut Security auf? Ich meine, ich würde mal sagen, früher ist IT-Sicherheit hauptsächlich nur der Firmenliebe gemacht worden, heutzutage steckt ein bisschen mehr dahinter durch die Datenschutzgrundverordnung, dass Daten so auch geschützt werden müssen. Jetzt gibt es die Schlagwörter Integrität, Verfügbarkeit und Vertraulichkeit von Daten, kannst du dazu ein bisschen ausschweifen und einmal ein bisschen näher deinen Blick darauf werfen. Vielleicht auch schon in Bezug ein bisschen auf, dass wir die DSGVO oder den Datenschutz miteinbeziehen.

B: Naja grundsätzlich hast du da schon Core-Prinzipien der Security dir herausgesucht, also wir sprechen hier von dem CIA-Prinzip oder wie du das schon zu Deutsch genannt hast Integrität, Verfügbarkeit und Vertraulichkeit, das sind sozusagen Grundprinzipien die wir aus der Security sicherstellen müssen damit wir überhaupt von einem sicheren Umgang mit Daten sprechen können. Wenn wir uns jetzt diese einzelnen Schlagworte etwas genauer anschauen was zum Beispiel hinter Integrität, Verfügbarkeit oder Vertraulichkeit steckt, entwickeln sich dann je nach Thema auch gewisse Schwerpunkte. Nehmen wir jetzt zum Beispiel die Integrität her, sind die Daten wie ich sie bekommen habe auch so richtig, sprich gibt es einen Integritätscheck der ganzen, werden sie überprüft, werden sie kontrolliert, werden sie auf ihre Richtigkeit hin geprüft, das kann in Bezug auf Cloud, Cloud Computing auch ein sehr wichtiger Punkt sein damit ich die Integrität gewährleisten kann, muss ich zum Beispiel technische Maßnahmen umsetzen die jetzt ein Verändern der Daten auf dem Transportweg in die Cloud zum Beispiel verhindern. Sprechen wir hier von Kundendaten habe ich natürlich als Serviceanbieter zum Beispiel die Pflicht diese Daten natürlich vertraulich, richtig und ordnungsgemäß in mein System einzuführen, sprich es muss einen gewissen Qualitätscheck geben in unseren Systemen, wir sprechen hier von den Mindestanforderungen an Informationen die wir zum Beispiel von einem Kunden benötigen um ein Versicherungsservice, eine Rechnung oder ein anderes Produkt anzubieten. Wenn wir uns den nächsten Punkt anschauen sind wir zum Beispiel bei der Verfügbarkeit, die Verfügbarkeit ist gerade in Bezug auf die Thematik Cloud und wenn man sich die ganzen modernen Themen anschaut wie IOT, Smartphones, es wird immer alles

integriert, mehr Systeme wachsen ineinander, müssen natürlich dann auch die dementsprechenden dahinterliegenden Systeme verfügbar sein und gerade bei einem externen Anbieter der mir Infrastruktur in einem mir unbekannten Datenzentrum oder Datenhaus zur Verfügung stellt, muss eine gewisse Verfügbarkeit geregelt sein. Sprich, regle ich die auf technischer Ebene über gewisse Bandbreite oder natürlich kann ich das Ganze auch auf organisatorischer Seite überprüfen, sprich ich sichere mir vertragliche Reaktionszeiten, Antwortzeiten oder zum Beispiel Verbindungsgeschwindigkeiten. Das ist natürlich jetzt kann man das nicht verallgemeinern auf was für Werte man hier geht, da das sehr abhängig davon ist was für ein Service und in was für einer Qualität man dieses Service dem Kunden zur Verfügung zu stellen hat, aber in diesem Themenbereich befinden wir uns wenn wir von Verfügbarkeit in der Thematik Cloud und DSGVO uns bewegen. Bezüglich der Vertraulichkeit das den letzten Eckpunkt unsere CIA-Pillars darstellt, kann man natürlich davon sprechen wer darf denn auf diese Daten zugreifen, hier ist aus technischer Sicht ganz wichtig Rollenkonzepte, sich ein Mitarbeiterkonzept auszudenken wo ich sozusagen nur die Minimum-Rechte vergebe die auch wirklich benötigt werden um eine Tätigkeit umzusetzen. Also hier spricht man grundsätzlich von dem Prinzip der Last Privilege oder der At Least Privileged Possibilities

A: So wie Need to Now Prinzip

B: Genau, nach dem oder auch nach dem Need-To-Know-Prinzip. Bezüglich Vertraulichkeit in einer Public Cloud hier sprechen wir halt natürlich von einen Infrastrukturservice das möglicherweise mit dritten oder unbekannten Firmen zusammen genutzt wird, sprich hier muss ich aus Eigeninteresse und auch um meine Kundendaten zu schützen, muss ich Mechanismen verankern oder generieren die mir die Vertraulichkeit der Daten einfach gewähren. Sprich Verschlüsselung der Kundendateien und sie werden nur entschlüsselt wenn ich sie gerade benutze, sprich wenn sie jetzt auf der Festplatte irgendwo herumliegen, dass sie niemals dort im Klartext verfügbar sind und dementsprechend auch nicht von Fremden oder anderen Benutzern die jetzt zufällig auf der gleichen Public Hardware arbeiten wie ich, irgendwie eingesehen werden können.

A: Wäre es zum Beispiel, dass ich nur aus einer bestimmten Applikation die Daten lesen kann. Das heißt, nur die Applikation hat den Schlüssel, dass sie es im Klartext

lesen könnte.

B: Genau.

A: Kein persönlicher User kann direkt auf die Daten zugreifen, sondern nur die Applikation kann zugreifen.

B: Wie diese konkreten Maßnahmen ausschauen ist aber sehr anwendungsfallspezifisch, weil je nach Usecase oder nach Businesscase verarbeitet einmal die Applikation Daten oder ist einmal nur der Datenspeicher oder ist einfach nur ein Transitsystem, also je nach Anwendung oder Usecase sind hier dann unterschiedliche Mechanismen, werden hier unterschiedliche Mechanismen benötigt.

A: Okay, wir haben es jetzt schon angesprochen, wir haben schon gesagt, nach Stand der Technik wir auch in der DSGVO immer beschrieben, wir haben auch gesprochen von Netzwerksicherheit und von Verschlüsselung usw. Vielleicht kannst mir du kurz aus deiner Sicht erklären was bedeutet eigentlich Stand der Technik und wie könnte jetzt zum Beispiel, weil ich ja so eine Checkliste machen will, wie könnte ich zum Beispiel überprüfen ob was Stand der Technik ist? Also einmal was bedeutet Stand der Technik für dich und wie wäre es möglich das überhaupt zu prüfen ob was Stand der Technik ist?

B: Das ist eine sehr schwierige Frage. Stand der Technik ist leider ein sehr weit dehnbarer Begriff, aber grundsätzlich gibt es auf Regierungs- oder Regulationsebene immer wieder Dokumente die ganz klar ausdefinieren was zum Beispiel für das Jahr oder für das Monat oder vielleicht sogar nur für eine Woche als Stand der Technik anzusehen ist, hier könnte man zum Beispiel recht gut auf das BSI verweisen, auf die Guidelines und so etwas herausbringen, aus unserer Sicht ist Stand der Technik bezüglich der Cloud-Thematik ist immer die höchstmögliche Sicherheit, sprich auf Allianzseite gibt es hier Mechanismen und Richtlinien die mir vorgeben, dass ich das höchstmögliche Sicherheitslevel auf einer Cloud-Applikation benutzen soll, wie das jetzt konkret in technischer Maßnahme ausschaut ist natürlich abhängig davon welches Betriebssystem oder welches System ich generell fahre, aber hier sprechen wir von Mechanismen die am Markt bekannt und auch anerkannt sind. Also sprich es ist nicht der kleine Entwickler, der sich einen Verschlüsselungsalgorithmus ausgedacht hat, sondern hier wird auf Algorithmen gesetzt die zum Beispiel durch

Gremien, durch Überprüfungen, vielleicht sogar Open Source also die nach außen hin möglichst offen sind und sich nicht und nicht versuchen irgendwelche Geheimnisse zu verstecken, natürlich zu bevorzugen sind. Bezüglich Datenspeicherung

A: Ja oder, gerade wenn es jetzt Stand der Technik, wenn darauf hinweist, also auch Datenspeicherung, Datensicherung, Datenwiederherstellung ist ja in Bezug auch zur Verfügbarkeit und Integrität ein ganz wichtiger Punkt. Nehme ich mal an. Ja gibt es da irgendwas Besonderes was man beachten sollte, vielleicht gerade bei Speicherung, Sicherung, Wiederherstellung was IT-Sicherheit-mäßig genannt werden kann?

B: Ja natürlich, also wenn man sich die Applikation anschaut besitzt die ja sozusagen mehrere Ebenen, besitzt die mehrere Ebenen. Auf Cloud, wenn wir von den Cloud-Systemen sprechen dann hat das Betriebssystem oder das Basis-Image wird meistens vom Cloud-Anwender zur Verfügung gestellt, das heißt, genau vom Betreiber zur Verfügung gestellt, das heißt, dieser ist grundsätzlich auch für die Wartung dieses Basis-Image verantwortlich. Wo dann sozusagen die Firma mit einsteigt ist sozusagen auf der Applikationsebene, die Applikation wird in dem Fall von uns, von der Firma die das Cloud-Service benutzt quasi zur Verfügung gestellt, entwickelt oder installiert und das heißt, hier gibt es dann noch quasi auf der Applikationsebene Securitymaßnahmen die man hier enforcen muss, also zum Beispiel Input-Validierung, Output-Sentimenzation, Überprüfung auf Cross-Side Scripting oder mögliche andere Querverweise in Systeme die das, die unsere Applikation hat, die hier einfach überprüft werden müssen, das ist dann natürlich sehr applikationsabhängig, das kann von öffentlichen Zugriffen auf APIs bis hin zu dem Datenaustausch mittels eines Files von CSV bis XML, alles Mögliche beinhalten. Also hier ist es sehr wohl interessant sich den gesamten ISO OSI Layer-Stack anzuschauen und die Applikation anhand dieses ISO-OSI Layer-Stacks quasi nochmal aufzubrechen und in den unterschiedlichen Ebenen die Securitymaßnahmen die sinnvoll sind zu enablen. Das kann jetzt sein von https-Verbindungssicherheit die mir einen möglichst sicheren Transfer in meine Cloud zur Verfügung stellt bis hin zu wie verschlüssele ich meine Daten in der Cloud selber, benutze ich hier zum Beispiel von dem Cloud-Provider zur Verfügung gestellte

Maßnahmen oder benutze ich hier eher Mechanismen die ich mir selber in der Firma aufgebaut habe und inkludiere diese nur in dem Service. Das kann je nachdem wie das Business-Modell ausschaut auch eine Business-Entscheidung sein, aus Security-Sicht ist es aber so, dass man hier grundsätzlich besteht immer die Möglichkeit, dass sich ein Cloud-Anbieter in irgendeiner Form bösartig verhält oder möglicherweise, dass er bösartige Kunden auf der gleichen Infrastruktur laufen hat, sprich hier gibt es einen gewissen Mistrust gegenüber dem Cloud-Anbieter. Wobei der Worst Case sozusagen, dass der Cloud-Anbieter an sich böse wird oder turns malicious, wird sozusagen würde ja sein gesamte Business-Modell kippen. Das heißt, da ist die Wahrscheinlichkeit, dass der Cloud-Anbieter einen Missbrauch irgendwie günstig billigt oder verheimlicht ist zwar vorhanden, aber sehr gering, weil das sein gesamtes Kerngeschäft eigentlich zerstören wird und er damit auf einen Schlag seinen gesamten Kundenstock verlieren würde.

A: Da waren wir eigentlich eh schon, ich meine Sicherung, Wiederherstellung da geht es eigentlich darum nur, dass man da vereinbart wahrscheinlich auch und Regeln festgesetzt wie wird gesichert, wie kann wiederhergestellt werden usw. Beim nächsten Punkt, haben wir eh schon angesprochen gehabt, Datenübertragung, Netzwerksicherheit, dann hast du schon gesprochen.

B: Vielleicht noch kurz zur Datensicherung. Gerade bei Cloud-Providern ist es auch wichtig sich sozusagen eine Ausstiegsstrategie zu definieren oder zu erstellen, sprich sollte ich das Cloud-Konzept nicht mehr benötigen, nicht mehr wollen, damit ich auch eine vertraglich zugesicherte Strategie habe wie ich denn meine Daten oder Applikationen aus dieser Cloud wiederbekomme. Soll das jetzt ein formeller Nachweis sein, dass mir der Cloud-Anbieter formell nur mit einem Dokument bestätigt, dass er die Daten gelöscht oder vernichtet hat bzw. das kann sogar bis dahin gehen, dass mir der Cloud-Provider per Laster quasi meine Festplatten vor die Tür stellt und ich dann persönlich für die Vernichtung zuständig bin. Also je nach Businesscase muss hier aber auch die richtige Strategie gewählt sein. Also sprechen wir hier von Kundendaten mit möglicherweise medizinischen Informationen oder so was, dann gibt es, dann reicht zum Beispiel der formelle Nachweis nicht aus, sprich da muss dann eine konkrete Strategie gefahren werden wo nachweislich die Daten aus der Cloud zurückgezogen werden. Der nächste Punkt

Datenübertragung ist natürlich auch ein ganz entscheidender Punkt wie kriege ich meine Daten überhaupt in die Cloud, hier gibt es natürlich auch Mechanismen die vom dynamischen Übertragen, Push-Pull-Prinzip bis hin zu einem reinen Datenaustausch via File unterschiedliche Möglichkeiten bieten, hier gibt es auch von dem Cloud-Anbieter oft eine Schnittstelle die zur Verfügung gestellt wird wie diese Daten zu nutzen sind, das kommt dann auch je nach Sensibilität der Daten an die ich da jetzt hin übertrage, muss ich dann dementsprechend auch die geeignete Datenübertragungsmethode wählen. Grundsätzlich sollten keine Daten mehr unverschlüsselt übertragen werden als Daumenregel, also als Mindestanforderung ist hier eine Form von https oder verschlüsselten Datentransfer zu sehen. Also das Ganze nur noch per Klartext zu übertragen würde jetzt zum Beispiel schon lange nicht mehr der Definition vom Stand der Technik

A: Ich denke nicht nur in die Cloud sondern das ist ein allgemeines Thema.

B: Natürlich auch ein allgemeines Thema, aber gerade auch speziell im Cloud-Thema da sollte nichts mehr unverschlüsselt übertragen werden, weil ich ja per se nicht mehr weiß was der Cloud-Anbieter oder was zwischen mir und dem Cloud-Anbieter da passieren kann oder passiert.

A: Ja dann nächster Punkt wäre zum Thema Netzwerksicherheit im allgemeinen IT-Sicherheitsbereich, ich würde mal sagen, da geht es Zugriff aufs Netzwerk wahrscheinlich? Einfach dass ich sage, mit IT-Sicherheit es ist ganz einfach wichtig, dass nur Befugte ins Netz kommen können.

B: Genau, also die Netzwerksicherheit zwischen mir und dem Cloud-Provider ist natürlich auch ganz essenziell, ob das jetzt mittels einer VPN-Verbindung passiert oder ob das eine Stand-Alone-Applikation nur in der Cloud ist, das hängt natürlich ein bisschen davon ab wie die Applikation aufgebaut ist. Grundsätzlich wenn man quasi eine Infrastruktur rein in der Cloud betreibt ist die Netzwerksicherheit eine sehr softwaregetriebene Komponente, sprich ich erstelle mir virtuelle Cluster, Buckets oder je nachdem wie so ein Zugehörigkeitsbegriff des Cloud-Providers ist, ein internes Netzwerk in meiner Cloud, das kann ich ganz klassisch mit Routing-, Switching-Protokollen versehen wie wir es aus der klassischen Netzwerksicherheit schon kennen, sei das jetzt von IP/TCP bis hin zu irgendwelchen exotischen Protokollen. Wenn wir hier von der Anbindung der Cloud-Applikation in ein

Firmennetzwerk sprechen, sprechen wir von Technologien wie VPNs oder Point-To-Point-Verbindungen wo sich die Cloud-Applikation über einen gewissen Punkt oder über eine gewisse Schnittstelle in das Firmennetzwerk anbinden kann, dementsprechend muss ich dann dort auch meine Sicherheitsmaßnahmen ganz wie gewohnt aus dem Netzwerk nachziehen, hier verhält sich die Cloud-Applikation abgesehen davon, dass vielleicht ein anderes Übertragungsprotokoll verwendet wird ziemlich äquivalent zu meinen anderen Systemen die halt einen hohen Sicherheits- oder Risikobedarf haben. Netzwerksicherheit kann auch bedeuten, dass ich nur definierte Endpoints habe, die auf meine Applikation zugreifen können bzw. könnte ich meine Cloud-Applikationen je nach Risiko oder Sicherheitsbedarf auch in abgeschottete Netzwerke kapseln damit ich eben sicherstellen kann, damit Unbefugte keinen Zugriff auf diese Daten und Applikationen haben.

A: Also von der IT-Sicherheit her jetzt gesehen noch ein Berechtigungskonzept bzw. Zugriffsschutz. Ich denke da nur bei Zugriffsschutz auf Authentifizierungsformen zum Beispiel oder Berechtigungskonzept, auch dass ich, das haben wir im Prinzip schon einmal gehabt mit dem need to know usw. sind die Konzepte, diese Rollenkonzepte, aber genau genommen auf den Zugriffsschutz, auf Systeme, auf Daten, auf sonst irgendwas, was könntest du dazu noch?

B: Naja Zugriffsschutz, da muss man sich eher globale System ausdenken wie zum Beispiel Zugriffsschutz basierend auf Rollen zum Beispiel wie wir es hier in der Allianz sehr oft benutzen, sprich es gibt definierte Rollen, diese Rollen werden dann an einen Benutzer dran gehängt und nur wenn ich die entsprechende, ich sage jetzt mal Cloudrolle besitze oder Leserolle für einen Kundenstamm, dann kann ich auch wirklich diese Daten einsehen. Wichtig hier ist es nur sich dieses Konzept vorher in einem möglichst breiten Ausmaß zu überlegen um dann genügend Rollen und Untergliederungen zu haben um dann im tatsächlichen operativen Betrieb auch ein sinnvolles Berechtigungsmanagement und so umsetzen zu können. Sprich basierend auf meinem Rollensystem kann ich dann den Benutzern unterschiedliche Tätigkeiten basierend auf ihrer Stellenbeschreibung zuordnen und das sollte dann dementsprechend auch DSGVO-konform sein bezüglich der Zugriffsschutz und Zugriffsrichtlinien.

A: Wegen Zugriffsschutz nochmal, Authentifizierungsmaßnahmen in der IT-

Sicherheit, was würdest du sagen, was ist so das Mindestmaß was man heutzutage anwenden sollte wenn man Zugriffsschutz realisiert? Ich sage jetzt mal, oft sind überhaupt keine Daten, die nicht wichtig sind usw. passwortgeschützt und aus, Username und Passwort, aber so ein Zugriff auf eine Applikation wo ich zum Beispiel Kundendaten verarbeite.

B: Ja ich würde hier grundsätzlich gerne zwei verschiedene Themenbereiche ansprechen. Das ist einmal der Zugriff von einem sozusagen Servicemitarbeiter auf einen Kundenstamm oder sozusagen quasi das klassische Supportmodell, ein Kunde ruft an, ich benötige Metadaten oder Informationen von dem Kunden, also quasi der klassische Kundenoperativbetrieb hier ist es so, dass der Zugriffsschutz eben schon über die klassischen Passwort, Username und Passwort-Methoden oder möglicherweise Token oder Zertifikat-basiert geschieht, spricht da gibt es schon vorher eine Authentifizierung und dann kann ich erst auf die Daten zugreifen, wenn wir hier aber von Zugriff auf Systemebene reden, sprich Administrationszugriff, Datenbankzugriff auf der technischen Ebene werden hier wesentlich strengere Richtlinien benötigt, hier sprechen wir zum Beispiel von einem User-Passwort und einem zweiten Faktor oder X Faktoren je nachdem wie kritisch diese Daten sind. Also Zwei-Faktor-Authentification wird im Systemumfeld sehr oft und auch sehr viel empfohlen, da es einfach einen zusätzlichen Schutzmechanismus bietet, sollte der Angreifer irgendwie irgendwo an verschwundene Usernamen und Passwörter gekommen sein.

A: Fallen dir noch so bestimmte, IT-Sicherheitsmaßnahmen Richtung was notwendig ist für DSGVO sage ich mal oder bestimmte IT-Maßnahmen ein? Mir fällt da jetzt nur zum Beispiel ein die Integrität oder die Nachvollziehbarkeit von Änderungen zum Beispiel, ja.

B: Ja gut, grundsätzlich haben wir schon relativ oft gesagt die DSGVO bietet aus Kundensicht einfach mehr Information, sprich der Kunde hat das Recht auf die Information was erhoben wird, wie, dass es richtig erhoben wird, dass es möglicherweise Veränderungen gibt oder es gar gelöscht wird, dementsprechend muss ich diese Schnittstellen halt auch in der Cloud zur Verfügung stellen und je nach System und Daten die ich da drin verarbeite, müssen diese Schnittstellen dann auch die Mindestsicherheitsansprüche entweder intern oder dem Regulatorischen

entsprechen. Bezüglich DSGVO der Kunde sollte sich dessen bewusst sein, dass seine Daten da jetzt in der Cloud zum Beispiel verarbeitet werden, das ist aber, wird aber eher schon aus der organisatorischen Ecke abgefangen, sprich ist es ein Neukunde, wird er beim Erstellen des Service darauf hingewiesen, ist es ein Bestandskunde wo das System gerade in die Cloud gesetzt wird, muss er im Nachhinein darauf hingewiesen werden. Ist deine Frage so halbwegs beantwortet?
A: So dann kommen wir jetzt zum letzten Punkt, das ist nämlich einfach, da möchte ich ein bisschen eine Info und deine Erfahrungen oder dein Wissen zu Public Cloud und mögliche Maßnahmen die dir dazu einfallen und da würde ich zuallererst deine allgemeine Einschätzung von Public Cloud-Providern gerne abfragen, wobei ich dazu sagen muss, also von meiner Sicht her gesehen ist es so, dass ich durch die Versicherung, große Konzern meistens ich denke und auch in der Arbeit eher mich auf die großen Anbieter wie Amazon, Google und Microsoft konzentriert habe in der Arbeit und den Fokus dorthin gelegt habe.
B: Also dann würde ich sagen bleiben wir auch gleich bei den großen Anbietern thematisch vorerst mal. Wo man eigentlich sagen kann, alle die Cloud-Anbieter in der Größe von Google, Amazon, Microsoft, sei das jetzt die AWS-Cloud oder eine Asia-Cloud bieten einfach durch die schon doch ein paar Jahre aktive Betreuung und stetige Weiterentwicklung schon sehr stabile Services an, was einerseits natürlich die Marktpräsenz auch sehr stark beeinflusst, manche Cloud-Anbieter setzen mehr gewisse Schwerpunkte in Infrastructure as a Service oder in Software as a Service oder andere Dienste, also es gibt hier schon kleine und feine Unterschiede zwischen den gesetzten Schwerpunkten, was man aber allgemein sagen kann, dass die drei großen Cloud-Anbieter sehr wohl das Ganze auf sich genommen haben die Data-Center zu zertifizieren, die ganzen Protokolle, Mechanismen über die Jahre zu verbessern, zu verfeinern, zu improvisieren, spricht man heute von einem Cloud-Anbieter á la AWS, á la Google dann bekommt man dort schon ein sehr professionelles, gut durchdachtes und sehr leistungsfähiges System das auch in gewissen Umständen für das Business auch manchmal sehr kostengünstig sein kann, das darf man natürlich auch nicht vergessen. Wenn man das Ganze jetzt mehr aus der Securitysicht betrachtet bieten diese großen Anbieter wie schon kurz erwähnt eine Großzahl an Zertifizierungen die auf organisatorische zumindest schon

einmal dem Kunden versichern, dass sie sich mit den Themen und den Problematiken die sich mit Cloud Computing ergeben schon beschäftigt haben, sich damit auseinandergesetzt haben oder gar sogar eigens entwickelte Lösungen dafür anbieten. Wenn man sich das Ganze jetzt auf der technischen Seite ansieht, sieht man sehr stark diese organisatorischen Maßnahmen auch durchschlagen, sprich die standardisierten Prozesse um etwas anzufordern, um einen zum Beispiel Penetration Test zu fahren, hier bieten die großem Cloud-Anbieter natürlich sehr viele Möglichkeiten und natürlich auch sehr schnelle Möglichkeiten diese Security-Maßnahmen auf technischer Ebene zu überprüfen und sollte man hier doch Findings oder Anmerkungen bezüglich Bedenken oder anderen Informationen haben, sind die großen Anbieter auch aus erfahrungsgemäßer Natur sehr kooperativ denn alle diese Findings die jetzt von Penetration Tests, von Audits, von organisatorischen Maßnahmen oder technischen Maßnahmen her gefunden werden, erhöhen natürlich die Gesamtsicherheit für alle Cloud-Anbieter. Das heißt, diese Anbieter sind was das betrifft sehr offen und zeigen sich auch sehr kooperativ was natürlich aus Firmensicht ein enormer Vorteil ist weil man sieht, sie wollen nichts verstecken, sie greifen Randthemengebiete an die vielleicht eine kleinere Cloud so jetzt nicht direkt anspricht und sie gehen bezüglich, was die Dokumentation und die Auskunftsqualität betrifft, sind sie natürlich meist sehr gut aufgestellt und bieten da sehr qualitativ hochwertige Dokumente, aber auch Expertisen und Expertenratschläge.

A: Dann hätte ich, tun wir gleich weiter was diese Public Cloud, also die Auswahl. Also was würdest du sagen, was sind so die wichtigen Werte, die man nimmt und deswegen nehme ich diesen Anbieter? Diesen Public Cloud-Anbieter.

B: Also aus meiner Sicht kann ich das nur aus technischer Sicht beurteilen, der Kostenfaktor ist jetzt für mich einmal eher nachrangig würde ich sagen, hier geht es ganz klassisch in die Möglichkeit mal vorab Zertifizierungen vorzulegen, sprich eine ISO27000 sei das jetzt in Form von Prozessen, Frameworks oder einen ganzen Cloud-Data-Center-Zertifizierung, sind hier enorm wichtig was natürlich auch ganz klar ist, dass die Zertifizierung möglichst international anerkannt sind, sprich es interessiert mich keine lokale, ich sage jetzt mal kleine Österreich-Zertifizierung wenn ich die im Vergleich einer ISO oder eines anderen internationalen Frameworks

wie COBIT oder ITIL oder so etwas vergleiche. Das ist zumindest mal die organisatorische Maßnahme. Das Zweite ist natürlich, das ist aber jetzt nur Allianz-bezogen, wir haben bei uns im Haus die Richtlinie, dass Applikationen auch auf Sicherheit getestet werden müssen, also wir sprechen hier von technischen Penetration Tests, in diesem Gebiet befinden wir uns jetzt und natürlich muss auch aus Firmensicht die Möglichkeit bestehen diese Penetration Tests auf meiner Cloud-Plattform zu fahren und je nachdem wie die Reaktion des Anbieters drauf ist, kann man schon in gewissem Maße abschätzen wie sie sich mit der Sicherheit, mit der Thematik der Sicherheit einfach befasst haben, wie offen sie zu dem Thema sind und welche Supportmöglichkeiten sie in diesem Bereich hier bieten. Grundsätzlich haben wir aus Allianz-Erfahrung mit der AWS ziemlich gute Erfahrungen gemacht, sprich der Prozess eines Penetration Tests, anzumelden und schlussendlich dann auch durchzuführen ist ein sehr rascher, hier ist recht wenig organisatorisches Overhead sozusagen nötig, sprich im Fall von AWS kann man hier sagen, wir haben hier einen sehr gut und einen sehr gut dokumentierten und technisch ausführlich beschriebenen Weg um solche Penetration Tests ordnungsgemäß durchführen zu können. Und das ist schon, vorab sind das dann viele kleine Zeichen, die einem einen groben Überblick über die Sicherheit so eines Cloud-Anbieters geben.

A: Da noch eine kurze Frage, also ich nehme mal an, dass natürlich ein Unterschied auch sein wird für was ich ihn brauche, ob jetzt Infrastructure as a Service, Plattform as a Service und Software as a Services nehme, dementsprechend unterschiedlich sind die Anforderungen, die ich habe.

B: Absolut. Also die Anforderungen, also der Businesscase spielt hier aus meiner Sicht, wie du schon erwähnt hast, auch einen sehr großen (?), weil je nachdem was für ein Service ich hier benutze oder aufziehe, sind da natürlich die Anforderungen an die Sicherheit auch komplett anders teilweise. Also wenn wir hier Infrastructure as a Service betreiben, sind die Sicherheitsmaßnahmen oder Richtlinien, an die wir uns halten wesentlich umfangreicher als wenn es nur eine Application alleine in der Plattform ist wo wir uns dann nur um den Application Layer sozusagen kümmern müssen.

A: Nächste Frage, nachher gleich wieder dazu, ich weiß schon, es ist immer, man muss es immer ein bisschen unterschiedlich betrachten oft noch in dem Bereich

nämlich eben für was wir es nehmen, gesagt haben Infrastructure, Plattform oder Software as a Service, aber allgemein Datenschutz in der Cloud, ich nehme mal an, die Großen sind schwer zu überprüfen von einer Firma selbst auch wenn Allianz vielleicht nicht so klein ist, dass sie schon ein bisschen einen Einfluss haben kann, aber grundsätzlich auf was kann man sich dann verlassen, dass die auch dementsprechend nach den Gesetzen arbeiten?

B: Naja grundsätzlich unterliegen diese Firmen genauso mal den regulatorischen Anforderungen des Landes und dann möglicherweise auch internationalen oder kontinentalen regulatorischen Anforderungen, also EU-Raum, Asia-Raum oder ähnliche, also hier geht man sozusagen den Schritt vom Lokalen immer größer werdend in internationalen Raum, die Anforderungen aus den nationalen regulatorischen Gesetzgebungen oder ähnlichem sind hier leider komplett unterschiedlich, Österreich hat hier einen recht pragmatischen Ansatz gewählt, wir haben von überall ein bisschen was, also aus lokaler österreichischer Anforderung, sprich in unserem Fall nicht Cloud-Services zu nutzen, einzusetzen, auch wenn man nicht genau weiß auf welcher Adresse sich das Datenzentrum befindet, man kriegt eine Zuordnung, einen geografischen Raum zugewiesen oder kann sich den je nach Service oder Vereinbarung auch aussuchen wo man sich hier befindet, also zum Beispiel im EU-Raum oder im amerikanischen Raum oder im Asia-Raum, aber eine konkretere, genauere Angabe als eine geografische Richtlinie zu dem Ort wird es hier vom Cloud-Anbieter nicht geben weil es ja auch in gewisser Weise im Interesse des Cloud-Anbieters ist sein Datenzentrum quasi möglichst gut zu schützen und da gehört es dann auch eben dazu, dass man nicht konkret die Adresse seines Datenzentrums angibt. Um jetzt aber nochmal zurückzukommen auf deine Frage, wie ich als Firma quasi diese Anforderungen überprüfe. Hier kann man entweder auf starke Kooperation mit dem Cloud-Anbieter setzen, sprich der Cloud-Anbieter hat sich schon im Vorfeld darüber informiert und hat sich dann entschieden dieses Service überhaupt in dem Land anzubieten, das heißt, ist ein Service grundsätzlich von dem Anbieter verfügbar, kann ich natürlich auch davon ausgehen, dass er zumindest den regionalen oder den in unserem Fall österreichischen Anforderungen sich befasst hat und dort die Mindestanforderungen erfüllt sind. Zusätzlich die Zertifizierung von internationalen Regelwerken die mir dann eben auch von dritten

Betreuern, also eines externen Audit-Teams wie einer ISO-Zertifizierung wie zum Beispiel der ISO27018 für eine Cloud-Data-Zertifizierung ausgewiesen haben, diese werden von externen Anbietern überprüft, sprich hier habe ich quasi eine neutrale Überprüfung der ganzen Richtlinien die ich mir vorher vertraglich ausmache und definiere oder als Mindestanforderung definiere, andererseits gibt es dann natürlich auch stichprobenartige Möglichkeiten in dieses System seine Überprüfungsmaßnahmen einzubauen.

A: Ich sage jetzt einmal Zugriffssicherheit und die Integrität, Verfügbarkeit und Vertraulichkeit haben wir im Prinzip vorher schon besprochen gehabt weil wir ja auch schon vorher bei der IT-Sicherheit sehr Richtung die Cloud-Thematik eingebunden haben, ein Punkt ist, das hast du auch vorher gerade erwähnt, ist nämlich der Standort, wo ich verarbeite und wo ich Daten habe, also aus meiner Sicht, du hast es eh erklärt, regional kann ich schon entscheiden wo ich es haben will, aber ich kann halt nicht genau die Adressen festlegen.

B: Genau. Das kann halt natürlich aus rechtlicher Sicht zu komplizierten Verhältnissen führen, aber grundsätzlich spricht man hier davon, dass aus österreichischer Sicht nichts dagegen spricht die Daten in einem anderen Land weiter zu verarbeiten, sprich ich muss im Vorhinein nicht genau wissen wo meine Daten liegen, solange ich sie in einer rechtlichen Zone habe, also in unserem Fall sprechen wir vom EU-Raum, sprich da gibt es durch die DSGVO bzw. das darüberstehende EU, die EU-Richtlinie und diese besagt, dass ich eben Standorte hier nicht genau wissen muss und Österreich hat sich auch entschieden das so zu übernehmen. Es gibt hier andere Länder die hier wesentlich strenger sind wo natürlich das ein sehr wichtiger Punkt, dass die Daten quasi nicht das eigene Land verlassen, hier ist es natürlich für den internationalen Cloud-Anbieter schwierig Fuß zu fassen weil das oft seinem eigenen Businesscase quasi widerspricht was für einen Standort für ein Data-Center zu wählen.

A: Ich habe jetzt da noch als nächsten Punkt Vertragsinhalte, wenn man jetzt, ich sage jetzt einmal, wenn man mit der Public Cloud, eine Lösung in der Public Cloud umsetzen möchte, logischerweise muss es ja eine Vereinbarung, einen Vertrag damit geben und da hätte ich jetzt gerne einmal von dir so aus deiner Sicht gerne erfahren was du denkst, was sind so oder wie soll ich sagen? Ich habe es ja auch schon

ausgearbeitet, es gibt ja einige, im Internet schon einige zu finden auch Beispiele genannt werden was alles drinnen sein, vielleicht nicht jetzt alles was drinnen sein muss, aber was du sagst, das sind so die wichtigsten Bestandteile eines Vertrages mit einem Public Cloud-Anbieter, die man unbedingt regeln sollte.

B: Naja also das ist zum ersten Mal quasi das Service was ich kaufe, ich muss mir im Vorfeld genau überlegen was ich denn von der Cloud genau will, betreibe ich da drinnen nur eine Applikation, betreibe ich darin eine ganze Infrastruktur und dann basierend dann auf dieser Definition sind halt unterschiedliche Möglichkeiten im Vertrag zu regeln, sprich wir haben vorher schon kurz genannt diese drei Pillars Integrität, Verfügbarkeit und Vertraulichkeit, diese Inhalte wandern teilweise direkt oder aber auch indirekt in die Vertragsinhalte, vor allem wenn wir von Verfügbarkeit sprechen wie lange, wie oft ist dieses Service verfügbar, ist das nur unter den Betriebszeiten, also in den Business Hours verfügbar oder ist das 24 mal 7 verfügbar, wie schaut es aus mit den Inhalten in Form eines Fehlers, wann kann ich damit rechnen eine Antwort zu kriegen? Wenn wir das Ganze jetzt auf Security hinunter brechen und uns auf den Security-Schwerpunkt da konzentrieren, sind die vertraglichen Inhalte wer auf meine Daten Zugriff hat natürlich auch sehr wichtig, sprich ist es ein allgemeines Team, sind es dezidierte Ressourcen die mir zugeteilt worden sind, habe ich, gibt es einen Freigabeprozess den ich als Kunde bestätigen muss damit mir Amazon oder der Cloud-Anbieter überhaupt technische Unterstützung für mein System geben kann, vertraglich natürlich sollte auch rudimentär geregelt sein welche Security-Ansprüche wir an das Service erwarten, sprich welche Mindestverschlüsselung verfügbar sein muss damit wir das Service überhaupt kaufen bzw. natürlich auch wäre eine klare Abgrenzung wer für welche Bereiche zuständig ist, also in unserem Fall habe ich schon öfters genannt, wenn wir nur eine Applikation in der Cloud betreiben, dann interessiert uns als Cloud-Kunde eigentlich nur der Application Layer und nicht der Betriebssystem-Layer, sprich vertraglich muss natürlich ganz klar abgrenzt sein wo die Aufgaben des Cloud-Providers aufhören und wo die Aufgaben des Kunden quasi anfangen. Vertraglich würde ich dann noch sagen, natürlich die Kosten müssen in irgendeinem Fall, also in irgendeiner Form auch ganz klar definiert sein, Security ist ein Budgetfresser, natürlich müssen hier gewisse Grundsätze gewährleistet sein im Sinne von ich, der

Cloud Provider kann mir jetzt für Security-Maßnahmen nicht zu viel verrechnen, sondern nur das was ich auch wirklich haben wollte. Was ganz wichtig ist wie auch schon einmal erwähnt, sind die Exit-Strategien bzw. auch die Regelung für Transaktionen, sprich wie schaut der Zugriff aus, wie schauen, wie gestalte ich meine Schnittstelle, wie haben die aus Kundensicht auszuschauen bzw. wie haben die aus Cloud-Providersicht auszuschauen? Da fallen dann von Schnittstellenspezifikationen bis hin zu ganz klassischen Zugriffskonzepten eigentlich alle Themen herein. Und dann schlussendlich noch die Exit-Strategie. Wie steige ich möglicherweise aus? Wird das Ganze formell geregelt? Kriege ich einen Laster mit meinen Festplatten vor die Tür geliefert? Oder irgendetwas dazwischen.

A: Gut. Jetzt wären wir schon eigentlich beim ganz letzten Punkt, ich würde dir gerne kurz vorstellen wie ich diese Checkliste aufbauen möchte und würde einfach nur gerne dein Feedback dazu einholen. Also aus der momentanen Sicht würde dieses Framework wie es genannt wurde so aufgebaut sein, dass ich, dass das Ganze aus ein, zwei, drei, vier Checklisten besteht, nämlich einerseits eine Checkliste zur Auswahl des Public Cloud Providers wo ich zum Beispiel inhaltlich drinnen habe welche Zertifizierungen oder Überprüfungen von Dritten, also eigentlich was wir hauptsächlich schon gesagt haben mit Recht bzw. Gerichtsstands Ermittlung, Offenbarungspflichten, eh den Stand der Technik, dass es zumindest bestimmte Passwortmindestlängen hat, also Voraussetzung sein muss usw. das würde da in den Public-Bereich fallen, vielleicht auch welche Referenzen oder so mindestens drei Firmen mit größer so und so Umsatz quasi hat, das wäre der eine Teil als Checkliste zur Auswahl, ich suche einen, auch vielleicht mit Referenzen zu diesem Modell das ich machen will spezifisch, so in dem aufgebaut, würde dir da noch irgendwas dazu einfallen was ich vielleicht

B: Also du hast da die Kernthematik aus meiner Sicht schon recht gut erfasst. Zertifizierung und organisatorische Nachweise, die der Cloud-Anbieter mir liefern kann für die Umsetzung von Security-Maßnahmen sind hier in erster Linie die Thematik, nach der wir suchen. Und je internationaler und standardisierter oder spezifischer diese Zertifizierungen sind die da vorhanden sind, desto besser ist es aus Kundensicht weil dann sehe ich, dass gewisse Themenbereiche schon sehr stark behandelt worden sind und dass die Prozesse und die eingesetzten Maßnahmen dort

natürlich dementsprechend auch einem gewissen Reifegrad unterliegen.
A: Und die restlichen Checklisten wären dann eher dazu aufgebaut, entweder, dass ich, sage ich, wenn ich jetzt was Neues mache, dass ich mal mein Konzept überprüfe ob das so passt bzw. wenn ich eine bestehende Lösung habe, dass ich dies überprüfe, erfülle ich das Ganze und das würde drei verschiedene Checklisten nur geben, einerseits, dass ich den Vertrag überprüfe, den Vertrag überprüfe, das nächste ist das ich die Checkliste organisatorische notwendige Maßnahmen überprüfe und auch technische notwendige Maßnahmen, da geht es einfach nur zum Beispiel die Verschlüsselung der Datenübertragung, wie wird die ausgeführt? Ist die Stand der Technik? Ist die da usw. In diesem Maß würde das aufgebaut sein.
B: Okay, also vertragliche Maßnahmen haben wir eh vor Kurzem besprochen, da haben wir ein paar Kernpunkte genannt, Exit-Strategie, Reaktionszeiten, Verfügbarkeiten die dem Kunden da quasi geboten werden, die sich auch direkt dann auf den Preis auswirken sind hier ganz klar zu definieren und abzugrenzen, hier sollten möglichst wenig quasi Interpretationsspielräume vorhanden sein einfach um die Fronten zwischen Kunde und dem Cloud-Anbieter möglichst klar zu definieren weil je klar das definiert ist, desto einfacher ist die Zusammenarbeit. Die organisatorischen Maßnahmen und die technischen Umsetzungen sind halt sehr von dem Businesscase abhängig, hier müsste man sich konkret das vorliegende Modell anschauen und dann anhand von dem Service ob das jetzt ein Infrastructure as a Service, ein Plattform as a Service oder Application as a Service ist und anhand dessen nochmal genauer herunterbrechen.
A: Ja die vorherigen Fragen zur Checkliste haben wir jetzt auch kurz besprochen, ein Thema noch zusätzlich was du kurz jetzt angesprochen hast mit organisatorischen und technischen Maßnahmen, organisatorische Maßnahmen würde ich als Beispiel, ich habe jetzt nicht genauer die Prozesse, nehmen, wäre zum Beispiel das Verarbeitungsregister gewesen wo überprüft werden muss ob das auch wirklich so durchgeführt wird, ob das auch noch immer aktuell ist, ob die Daten aktuell sind, ich glaube, da gehört einfach ein regelmäßiger Prozess eingeführt und das muss ich abprüfen auch. Diese Sachen möchte ich in der Checkliste abprüfen.
B: Ja das ist schon ein ganz wichtiger Punkt aus meiner Sicht, dass die Prozesse die in der Cloud stattfinden möglichst nachvollziehbar sind, dass die Maßnahmen die

da getätigt werden auch ein gewisses technisches Fundament haben bzw. dass halt die organisatorischen Maßnahmen hier nicht vernachlässigt werden weil ich muss in dem Crowd-Service oder bei dem Cloud-Anbieter sehr wohl auch meine Zugriffsrechte aktualisieren in einem gewissen Intervall, ich muss meine Passwörter ändern, ich habe auch hier gewisse organisatorische Prozesse davor die einfach eingehalten werden müssen, sonst funktioniert das gesamte Cloud-Konzept nicht. Und so wie du gesagt hast zum Beispiel ein Melden an das Register, ob das notwendig oder nicht ist, das muss natürlich im Vorfeld schon evaluiert werden und das würde für mich ganz klar unter die organisatorischen Maßnahmen fallen, dass diese Evaluierung stattfindet bevor das konkrete Projekt dann umgesetzt wird in der Cloud.

A: Der letzte Punkt wären noch die technischen Maßnahmen. Wo ich als Beispiel da jetzt einmal wieder nennen will die Verschlüsselung der Datenübertragung, dass ich sage, es muss dieser Standard entspricht dem Stand der Technik und als Hinweis überprüfbar über diese wie du genannt hast zum Beispiel über das österreichische Informationshandbuch oder den vom BSI in Deutschland nach diesen Vorgaben. Und so würde ich diese verschiedenen technischen Möglichkeiten abbilden. Würdest du sagen, dass das so passt oder dass man da noch was aufpassen müsste besonders?

B: Grundsätzlich ist das eine sehr gute Herangehensweise, vielleicht aus meiner Sicht anzumerken ist, dass die technischen Vorgaben die ein Gesetzgeber ausspricht zwar eine gute Basis darstellen, aber wenn man es sich genau anschaut oft auch nur die Mindestanforderungen so ein System definieren, sprich das sind meine Mindestanforderungen sollte ich als Firma einen höheren Schutzwert benötigen oder mir selbst auferlegen oder definieren, dann ist das die Basis auf der ich aufbauen kann und basierend auf dem kann ich dann zum Beispiel noch sogar höhere Verschlüsselungsstandards oder so etwas implementieren als der Gesetzgeber eigentlich vorgibt um eben erstens zukunftssicher zu sein oder um eben eine besonders kritische Information zu schützen. Was man hier vielleicht auch noch sagen könnte ist, dass die großen Cloud-Anbieter diese Thematiken oft schon in ihre Produkte inkludieren, sprich da kann man mit einfachsten Möglichkeiten eine Full Disk Encryption oder ein Key Management betreiben oder sogar ein Key Management auslagern, sprich die stellen schon Methoden zur Verfügung um

möglichst einfach hochwertige technische Maßnahmen schnell umzusetzen und auch fehlerfrei umzusetzen weil eine technische Maßnahme kann sehr gut sein wenn sie aber falsch konfiguriert oder umgesetzt wird, kann sie natürlich auch wieder quasi der berühmte Schuss ins Knie werden, sprich eine Fehlkonfiguration kann mein genauso verwundbar gegen Angreifer machen wie ein schlechter Standard für die Verschlüsselung.

A: Gut, ja. Was vielleicht noch erwähnenswert ist, wo ich vielleicht auch noch ein Feedback haben möchte. Diese Checkliste die ich da erstellen will, wird logischerweise so, dass es immer einen Basisteil haben wird den man immer hat und geplant wäre einen Teil für Infrastructure as a Service, einen Teil für Plattform as a Service, einen Teil für Software as a Service weil ich glaube, je höher ich komme brauch ich das von vorher aber auch umgesetzt sonst funktioniert es nicht und das ich sie in diese Richtung aufbauen werden die Checkliste , das heißt den einen Basisteil den ich immer habe, ist egal was ich verwende und dann diese drei Ebenen, ob jetzt die Checkliste komplett in der Masterarbeit schon vollständig gemacht wird oder nur ein bestimmter Bereich wird man noch sehen, aber in dieser, so sollte sie aufgebaut werden.

B: Ist aus meiner Sicht eben auch ein relativ praxisnaher Ansatz, weil wenn wir von Cloud-Providern sprechen, sprechen wir eigentlich nicht davon was für ein Service wir von dem eigentlich benutzen wollen. Es gibt wie du schon gesagt hast ein gewisses, ein Basis-Set an Anforderungen die ich vielleicht an den Cloud-Provider habe, aber je nachdem was für eine konkrete Umsetzung ich da betreibe, wie du schon gesagt hast, Plattform as a Service oder andere Dinge, schaut dann die technische und die organisatorische Implementierung dann eine Spur anders aus. Mit dem Ansatz das Ganze zuerst in einem Basisfragebogen oder Checklist zusammenfassen, ist aus meiner Sicht auch eine sehr gute Idee, weil basierend auf dem kann man dann die Spezialgebiete für ein gewisses Thema weiter forcieren oder sich dann weiter anschauen.

A:Abschließend noch die Frage ganz allgemeine gesehen. Kann man aus deiner Sicht Public Cloud Provider unter Berücksichtigung der DSGVO einsetzen?

B: Ja, ich denke das diese Provider Stand der Technik sind und durch ihre Zertifikate auch konform sind.

669 **A:** Gut, okay. Dann machen wir es jetzt wirklich und ich sage Danke für das
670 Interview.

B4. Transkript Interview Thomas Schober

Das Interview wurde am 13.3.2019 um 14:00 Uhr in Wien 14. Linzerstrasse 211 geführt.

A: Ich beginne jetzt einmal. Hallo Thomas ich würde ich gerne kurz dein Feedback oder Informationen von dir einholen bezüglich der Datenschutzgrundverordnung, IT-Sicherheit und bei IT-Sicherheit und Datenschutzmaßnahmen bezüglich Benutzung Public Cloud, ich habe das Ganze auf drei Blöcke aufgeteilt, einmal die Datenschutzgrundverordnung, einmal die IT-Sicherheit und einmal die Public Cloud und würde gerne einmal mit Informationen von deiner Erfahrung, deines Wissens zur Datenschutzgrundverordnung von dir zu bekommen. Als ersten Punkt einmal vielleicht die Umsetzung der DSGVO im Unternehmen, einerseits bei dir im Unternehmen wie, ich nehme an, also Versicherungsunternehmen, dass es umgesetzt ist und was waren die Schwerpunkte darin in dieser Umsetzung aus deiner Sicht?

B: Kurz nur zu meiner Person, Mag. Thomas Schober, Information Security Officer in der Allianz Elementarversicherung und in der AzTech Österreich seit 2001 in dieser Funktion und seit über 25 Jahren im Unternehmen. Gut, Datenschutzgrundverordnung. Die Umsetzung der Datenschutzgrundverordnung war ein ganz wichtiges Thema für das Jahr 2018. Eigentlich vom Vorgehen her ist es darum gegangen einmal zu schauen welche Applikationen mit welchen Daten für welche Fachbereiche und Usergruppen zur Verfügung gestellt werden. Und das Ganze sozusagen bottom up von den Daten her zu klassifizieren und zu sagen, welche Daten fallen jetzt zum Beispiel in Richtung gesundheitsrelevante Daten usw. also in die höheren Schutzklassen rein. Die Allianz Elementar hat einen Riesenvorteil dadurch, dass wir keine Legacy-Systeme seit 2000 ungefähr im Einsatz haben, das heißt, die Software-Landschaft besteht de facto aus drei Applikationen, einer Versicherungskernapplikation, im Folgenden GFB oder ABS genannt, einer großen SAP-Implementierung und einer Data Warehouse-Implementierung, das heißt, man konnte sich einmal auf der Softwareseite genau auf diese drei Stück Software konzentrieren für die Erhebungsphase für die

Datenschutzgrundverordnung. Zweiter Punkt was sind die Schwerpunkte für Unternehmen, zum Beispiel Maßnahmen. Nachdem das relativ schnell gegangen ist dieses Mapping aufzustellen hat man dann gesehen wo zum Beispiel für bestimmte Datentöpfe Mehrfachzugriffe aus unterschiedlicheren Fachbereichen möglich waren und das hat man dann relativ schnell als erste Maßnahme sozusagen gesäubert und diese Zugriffsregeln dahingehend geändert, dass halt wirklich genau ein eindeutiger Zugriff ohne irgendwelche Doppeldeutigkeiten usw. möglich war. Erfahrungen der Evaluierung der Daten, ich meine, die Allianz hat den Riesenvorteil, wir haben ein unternehmensweites Datenmodell, das heißt, man sieht welche Hauptentitäten wie Kunde, Vertrag, Schaden usw. modelliert sind, in welchen Relationen die in den verschiedensten Tables abgelegt sind und damit sieht man eigentlich relativ gut wie in den Applikationen die Daten gehalten werden. Auf der SAP-Seite ist das relativ gut auch dokumentiert, da gibt es auch ein eigenes Datenmodell, im SAS gibt es kein eigenes Datenmodell, sondern da verwenden wir das das wir eben aus ABS und GFB verwenden, strukturell natürlich mit den ganzen Anpassungen, die halt für ein Business Intelligence System halt notwendig sind. Erfahrungen in den Evaluierungen haben wir gehabt, Erfahrung der Evaluierung des Schutzbedarfs der Daten. Naja, wie soll ich sagen, diese Hauptklassifizierung wo ich sage welchen Sensitivitätsgrad die Daten haben, das muss man halt einmal als Basis haben und dann kann man schauen welche Möglichkeiten man hat. Also einerseits, dass man sagt man schränkt den Zugriff massiv an, andererseits, dass man sagt es gibt Möglichkeiten sozusagen auf der Datenhaltungsebene das Ganze noch zu verbessern, zum Beispiel durch Verschlüsselung, da kann man gleich dazu sagen, dass bei uns alle Operativdaten immer sowohl End-To-End als auch At-Rest in der Datenbank verschlüsselt sind. Genau. Erfahrungen der Erstellung Verarbeitungsregister, ja das ist ein Thema das müsstest du mit dem Heinrich Riedl genauer besprechen, da hat er die Erfahrungen wie man das in dieses Register rein bekommen hat, aber wie gesagt, dadurch, dass das relativ klar dokumentiert und strukturiert war bei uns wir keine Versicherung sind mit ich weiß nicht, 20 Legacy-Systemen aus den 70er Jahren, war das eine relativ einfache Übung.

A: Ich hätte vielleicht noch eine Frage noch zur Datenschutzgrundverordnung allgemein, wo siehst du die Schwerpunkte der Datenschutzgrundverordnung oder

von Maßnahmen, die jetzt notwendig waren zu setzen? Prozessmäßig, organisatorisch, IT-sicherheitsmäßig?

B: Ja das ist relativ quer drüber über alle unsere Prozesse. Also interessant war, dass man sehr viel Aufmerksamkeit und Energie reingesteckt hat in den ganzen Meldungsteil im Sinne von wir haben eine eigene Unit, die sich mit Beschwerdemanagement beschäftigt, es hat eigentlich keiner genau sagen können wie viele Anfragen jetzt aus diesem DSGVO-Titel sozusagen bei uns einlangen werden. Da hat es Horrorszenarien gegeben von Tsunami mit 100 Anfragen pro Tag, bis hin zu naja 2, 3 im Monat und also die Tsunami-Variante ist nicht gekommen Gott sei Dank, aber sagen wir mal so, es war relativ schwierig diese ganzen Prozesse so zu sizen, dass das halt irgendwie zur Realität dazu passt. Ich glaube, das hat ganz gut funktioniert, falls da wirklich einmal aufgrund von irgendeinem IT-Incident oder so einmal dann eine massive Welle an Anfragen von Behörden, Medien usw. käme, würden wir wahrscheinlich da aufstocken müssen.

A: Mit den Regeln, die du da gemeint hast geht es um die Rechte und Pflichten ganz einfach von der Person, über die wir die Daten haben, dass wir auskunftsfähig sind und andererseits die Meldeverpflichtungen die wir haben bei Verletzungen, diese Prozesse umzusetzen?

B: Genau richtig. Also wenn wirklich ein Incident ist wo man dann sagt, gut ja, wir haben 1,2 Millionen Kunden in unserer Kundendatenbank, also wie viele davon werden sich dann ans Telefon hängen und bei der Allianz anfragen ob ihre Daten auch betroffen sind. Man muss das Ganze dann mit den PR-Abteilungen gescheit koordinieren, wir haben bereits vorbereitete Texte die für die verschiedensten Szenarien halt einmal so die wichtigsten Kernpunkte enthalten, man muss dann halt nur mehr den wirklichen Incident-Titel und das Datum einsetzen, also wir haben da einiges in der Vorbereitung, aber wenn es einen erwischt, dann wird wahrscheinlich wie überall in großen Unternehmen halt einmal, sagen wir mal so, die Organisation eher mal gefordert sein.

A: Das heißt, ein wichtiger Punkt für die ist auch diese Notfallszenarien vorzuplanen, dass man vorbereitet ist falls so was passieren sollte.

B: Genau richtig.

A: Gut. Dann würde ich eigentlich schon zum Punkt IT-Sicherheit und die daraus

entstehenden Maßnahmen; da hätte ich gerne von dir einfach nur deine Info von dir, was bedeutet für dich die Integrität, Verfügbarkeit und Vertraulichkeit von Daten? Wenn man das kurz umschreiben kann.

B: Wir haben einen ganz klaren Auftrag vom globalen COO der sagt, Aufgabe der IT-Sicherheit ist es sozusagen das Vertrauen das 75 Millionen Allianz-Kunden weltweit in uns haben und zwar weltweit als Marke, dass das nicht gebrochen wird dieses Vertrauen und das deckt eben Integrität, Verfügbarkeit und Vertraulichkeit der Daten ab. Das heißt, diese 3 Themen zeigen eigentlich nur auf wo Problembereiche, Angriffsvektoren, was auch immer daheim sein können, das heißt, bei uns ist sozusagen die IT-Security-Strategie damit umschrieben, dass wir sagen, wir wollen auf der Landkarte keine weißen Flecken haben. Es gibt Unternehmen, die legen bestimmte Schwerpunkte, was weiß ich, keine Ahnung, Behandlung von möglichen Zero-Day-Exploits durch irgendwelche eingekauften Systeme. Wenn man dann fragt, okay und wenn es dann irgendeinen Patch gibt, wie lange braucht ihr bis ihr den eingespielt habt? Und dann heißt, ja was weiß ich, 6 Wochen. Also da passt das eine mit dem anderen nicht zusammen. Uns ist wichtig, dass wir jeden Bereich abdecken können, das fängt an bei sagen wir mal Nesus-Scans damit wir nicht nur einmal im Jahr einen Securitycheck machen, sondern die 7mal 24 und, und, und. Da können wir dann eh noch drauf näher eingehen. Aber eigentlich geht es eben darum, kein Thema komplett unbehandelt zu lassen, weil meistens wie der Teufel will, erwischt es einen dann genau dort. Was bedeutet Stand der Technik und wie kann man es überprüfen? Also das ist natürlich ein ganz wichtiger Punkt, die IT-Sicherheit muss mit der technischen Entwicklung mit gehen, also wenn man immer nur in Host-Entwicklung, Kleinserver usw. unterwegs wäre und keine Ahnung, die ganzen Mobile Devices und das Thema von mir aus agile Entwicklung verschläft, kriegt man sehr wahrscheinlich ein Riesenproblem aus dem Titel. Wie kann man es überprüfen? Da kommen wir dann eh noch dazu. Wir haben sehr früh damit begonnen nicht nur im eigenen Saft zu kochen, sondern eben über die Nutzung von externen Zertifizierungen, also da hauptsächlich ISO27001, ISO20000 und ISO15504, immer sozusagen auch die Außensicht auf das was wir tun zuzulassen weil der Riesenvorteil von einer Zertifizierung ist ja nicht nur, dass man sozusagen was nach außen zum Herzeigen hat, sondern sie zwingt einen dazu regelmäßig,

dauernd im kontinuierlichen Verbesserungsprozess die Systeme sozusagen a jours zu halten und das ist eigentlich aus meiner Sicht der weitaus größere Nutzen von diesen Zertifizierungen. Und damit kann man jetzt einmal auch diese Frage beantworten wie man diesen Stand der Technik auch laufend überprüfen kann. Datenspeicherung, Sicherung, Wiederherstellung. Das ist Tagesgeschäft, Brot und Butter sozusagen, auch von der Security ist bei uns aufgrund der ganzen Globalisierungsgeschichten bzw. Rechenzentrumsverlagerungen her extrem interessant weil die Gefahr natürlich besteht, dass man Lösungen die man lokal in Österreich über viele Jahre aufgebaut und optimiert hat und die man dann sozusagen aufgeben muss weil man in die globalen Rechenzentren, Netzwerke usw. hin migriert, da besteht die Gefahr, dass man dann qualitativ sozusagen einen Schritt zurück macht. Das heißt, da muss man ganz, ganz genau schauen wie diese Lösungen ausschauen, die da global angeboten werden, aufgrund des sozusagen Size Matters kann man sagen, ist das natürlich oft schwieriger in dem großen Umfang das dann so zu machen, dass allen Recht getan ist, aber die Gefahr besteht natürlich, dass man da dann Einbußen erleidet im Sicherheitsniveau. So, Datenübertragung. Ja ist auch so wie Datenspeicherung kann man sagen ein wichtiger Punkt. Also man kann fix davon ausgehen, dass der Vollzustand für jegliche Art der Datenübertragung einmal verschlüsselt ist. Also eine unverschlüsselte Datenübertragung vermeiden wir wo es nur irgendwie möglich ist. Gott sei Dank sind auch die, sagen wir mal wichtigen Partner bei uns, also sei es Versicherungsverband, andere Versicherungen, deren Rechenzentren usw. Behörden da jetzt auch sehr auf diesen Themen sozusagen sensibilisiert und das allgemeine Niveau was so was anlangt in Bezug auf Sicherheit steigt doch mit der Zeit ziemlich gut. Netzwerksicherheit auch ein ganz wichtiges Thema, sowohl in den WLAN-Strecken, LAN-Strecken. Die Allianz setzt ein globales IT-Netzwerk ein das über 2 globale Firmen sozusagen eingekauft wurde und damit wird sozusagen die, das Datennetzwerktechnische, das Rückgrat, das Backbone sozusagen für die Kommunikation aller Landesgesellschaften mit der Zentrale in München bzw. den Rechenzentren in Frankfurt bzw. auf den jeweiligen Kontinenten sichergestellt. Interessant ist in dem Zusammenhang auch so Komponenten wie Proxys, Firewalls, die Bordergateway-Firewalls, das was bisher in den lokalen Netzen sozusagen von

der jeweiligen Organisationseinheit selber verantwortet wurde wie diese Regeln da ausgestaltet sind, muss natürlich bei den globalen Systemen halt neu definiert und ausgehandelt werden, führt natürlich gerade am Anfang dann zu Hoppalas die da passieren können, aber das muss man halt dann irgendwie gescheit managen. Zugriffsschutz und Berechtigungskonzepte. Also das ist auch was wo man relativ einfach einen Realitätscheck machen kann, das heißt, wenn man in einem Unternehmen drinnen ist, man sucht sich einen Arbeitsplatz raus und sagt so ähnlich wie ein Auditor, so wer sitzt da? Name, User-ID und jetzt hätte ich gerne auf einem Zettel alle oder in einem File welche Systeme verwendet derjenige oder diejenige, welche Rechte sind dort jeweils dahinter, wie schaut es mit Fileshares aus, wie schaut es aus in Bezug auf Internetzugriff usw. Wenn das sozusagen auf Knopfdruck verfügbar ist, dann zeigt das meistens einen gewissen höheren Reifegrad in der IT-Sicherheit, wenn das eben aufgrund von vielen Systemen ein Ding der Unmöglichkeit ist, dann sage ich mal, ist es schwierig höherwertige oder sagen wir mal gefinkeltere IT-Sicherheitsthemen dort überhaupt in so einem Unternehmen zu platzieren.

A: Ich hätte da vielleicht ganz kurz eine Zwischenfrage noch, Berechtigungskonzept allgemein jetzt bezogen auch auf Datenschutzgrundverordnung vielleicht gesehen usw. was ist besonders wichtig inhaltlich bei so Konzepten? Gibt es da irgendwie bestimmte Regeln, die man schauen sollte oder aufpassen sollte oder?

B: Naja eh so das klassisch Handwerkliche. Also man sollte versuchen die ganzen Berechtigungen immer über Gruppen abzuwickeln, also nie auf sozusagen, auf Einzelebene sozusagen zu arbeiten, was hilft ist Templates und was bei uns auch ganz wichtig ist, es muss alles von der Berechtigungsanforderung über die Eintragung bis zur Löschung muss in einer revisionssicheren Datenbank abgespeichert sein, also da kann man sich nicht mit irgendwelchen Zetteln beheben, wir setzen da seit vielen Jahren auf ein System wo das eben in einer relationalen Datenbank drinnen ist mit einem Anforderungsworkflow und wir haben Gott sei Dank ein einziges Team in der Anwenderbetreuung, die Security-Administration die ausschließlich solche Berechtigungsanforderungen macht und wichtig ist auch die Unterscheidung zwischen den persönlichen Usern und den Usern für Administratoren wo dann so Sachen wie Zwei-Faktor-Authentifizierung usw. dann

ins Spiel kommen.
A: Okay. Jetzt als einen Punkt dazu noch vielleicht die notwendige weitere Maßnahme, was wir bis jetzt vielleicht keinem direkt zuordnen haben können was du sagst, IT-Sicherheit die DSGVO, durch die DSGVO sind IT-mäßig noch ganz bestimmte notwendige Maßnahmen umzusetzen gewesen. Was wir bis jetzt vielleicht noch nicht so erwähnt haben wo man da jetzt durch aufgezählt haben.
B: Wie gesagt, wir waren Gott sei Dank in der Lage, dass wir sowohl die Dokumentation hatten als auch aufgrund dessen der vielen Jahre mit der ISO27001 Zertifizierung, dass wir da nicht wirkliche Maßnahmen hatten, die wir umsetzen mussten. Wie gesagt, es hat diese kleinen Bereinigungen gegeben wo man bei den Teams im Fachbereich halt gesagt hat, nein die brauchen eigentlich diesen Zugriff auf diese Art von Daten eh nicht mehr, das kann man wegnehmen. Übrigens, es gibt auch zumindest einmal, manchmal auch zweimal im Jahr einen Realitätscheck wo jeder Vorgesetzte für seine Mitarbeiter die Liste der vergebenen Berechtigungen bekommt, das wird dann sozusagen unterzeichnet und geht wieder an die Sec-Admin zurück, damit stellen wir sicher, dass trotz aller Prozesse usw. die wir haben auch immer wieder geschaut wird, gibt es die Leute noch und arbeiten die noch in diesen Bereichen wo ursprünglich die Rechte vergeben wurden, also wir sind da sehr dahinter, dass wir nicht so Szenarien haben, dass jemand der ein paar Stationen im Unternehmen hatte dann die Rechte so kumuliert und dann halt ein Rechteportfolio hat das mit seinem letzten Job sozusagen in keinster Weise zusammen passt. Also da sind wir sehr dahinter und das ganze Thema Berechtigungen wird auch jedes Jahr bei den Rezertifizierungsaudits oder bei den Surveillance-Audits für die 27001 überprüft mit Stichprobenziehung in der Datenbank und mit sozusagen Review der einzelnen Tickets, die da gezogen werden.
A: Okay. Ja dann wären wir schon beim Punkt 3 jetzt, die Erfahrung, Entschuldigung 4, wie ist die Erfahrung zu Public Cloud? Da hätte ich zu allererst gern einmal von dir eine allgemeine Einschätzung zu den Public Cloud Providern. Prinzipiell will ich sagen, geht es mir jetzt für Versicherungen, renommierte Unternehmen um die großen Anbieter die bekannt sind am Markt wie Amazon, Google, Microsoft, man muss jetzt nicht ins Detail was man von einem jeden hat, aber so eine allgemeine Einschätzung von diesen Providern was, sage ich jetzt

einmal, Sicherheit angeht, was vertragliche Vereinbarungen angeht, also allgemein die Zusammenarbeit mit denen.

B: Also es hat einen Auftrag gegeben von der Holding zu prüfen ob es möglich ist unser Kernsystem ABS, GFB auch in so einer Public Cloud-Umgebung lauffähig zu machen, das Ganze sozusagen auch mit einem Usecase zu unterfüttern der in Produktion ist, wir haben das gemacht und also auf Applikationsseite an sich natürlich keine Änderung weil der Applikation ist es jetzt wurscht ob es in einer Public Cloud oder in einem eigenen Rechenzentrum läuft, aber was schon zu sehen war, die ganze Awareness des Gesamtkonzerns bei dem Projekt war sehr hoch, also wir hatten sehr viele Diskussionen dahingehend wie wir eben die Sicherheit da gewährleisten und es haben sich eigentlich zwei Maßnahmen herauskristallisiert, das eine war einmal End-To-End-Verschlüsselung klarerweise, aber vor allem echte Datenverschlüsselung der Data Adress, also die Datenbank und da verwenden wir eben DW2 was eher ein Exot ist im Vergleich zu den üblichen Oracle-Implementierungen, also da haben wir einen Verschlüsselungsalgorithmus gebraucht den wir dann zugekauft haben und der genau das sicherstellt ohne große Performance-Einbußen und das zweite Thema war Schlüsselmanagement und da aber halt immer wieder auch die Anfrage vom Konzern, naja wenn ihr da den Schlüssel verwendet oder das Key Management von Amazon, dann kann ja doch ja in irgendeiner Form irgendwie möglicherweise so á la Snowden dann irgendeiner der dort Admin-Berechtigungen hat dann doch auf die Daten zugreifen und das haben wir dahingehend verhindert, dass wir eben nicht das Key Management-System von Amazon in diesem Fall verwendet haben, sondern unser eigenes Key Management und das steht in Wien. Also es gibt schon Möglichkeiten um einmal sozusagen die Hausaufgaben für solche Public Cloud-Implementierungen zu machen, sodass man nicht angreifbar ist, auf der anderen Seite die Erfahrungen haben gezeigt diese Großunternehmen sind extrem professionell aufgestellt was dann so große Kunden wie eine Allianz angeht, also der Support war erstklassig und aufgrund der ganzen Hardware-Virtualisierung und Hardware oder sagen wir Infrastructure as Code kriegt man unheimlich tolle Turnaroundzeiten zusammen wenn man sagt, okay, man möchte jetzt einen neuen Mandaten oder so aufsetzen mit 100, 150 Serverimplementierungen überall quer drüber sozusagen erfordert,

dann kann man das mit zwei, drei Klicks in diesen Systemen machen und dadurch, dass diese Infrastructure as Code-Files ja wirklich lesbar sind, sieht man auch genau was man eigentlich da jetzt implementiert hat und das Zusammenspiel zwischen Serverinfrastruktur, Netzinfrastruktur, Sicherheitsinfrastruktur ist extrem gut und abgestimmt, was man auch von diesen Providern lernen kann ist sozusagen Stringenz, wenn es 100 bestimmte Services gibt die angeboten werden, dann kann auch eine Allianz nicht kommen und sagen, sie hätte gerne einen 101. Service und das ist eine Lektion die man in der sozusagen unserer Infrastruktur Kunden vielleicht auch ein bisschen stärker berücksichtigen sollten.

A: Also von dem was du gesprochen hast, was man umgesetzt das Projekt, da ist es gegangen um Infrastructure as a Service, also wir haben keine Plattform as a Service oder Software as a Service-Umsetzungen in dem Sinn in die Cloud von unserer Applikation logischerweise, sondern Infrastructure as a Service haben wir.

B: Genau richtig.

A: So, dann als nächsten Punkt hätte ich die Frage an dich, was waren so die Schwerpunkte wo du sagst, das sind die Punkte die wichtig sind bei der Auswahl der Public Cloud oder es Providers, des Public Cloud Providers, was sind so wo du sagst die, was weiß ich, 4, 5, 6 Punkte die sind, das ist mir aufgefallen, da kann man feststellen ob man dort gut aufgehoben ist oder nicht gut aufgehoben ist.

B: Naja sagen wir so, die, das ergibt sich in gewisser schon einmal aus der Größe der Allianz jetzt einmal ganz goschert gesagt. Wir werden, wir hätten nie irgendwelchen kleinen Provider sozusagen in der Auswahlliste gehabt, sondern eh die die du angeführt hast, also Amazon, Google und die Microsoft mit der Asia und dann ist es eigentlich darum gegangen zu sehen, es geht eigentlich immer um die Strukturen und um die handelnden Personen wer wird uns da geschickt und da muss man sagen, da war dieses Amazon-Team extrem professionell und dadurch, dass das Ganze ja als, sagen wir als Pilot oder als Proof of Concept gedacht war, war das ganze Thema Kostenoptimierung und so jetzt nicht so im Vordergrund. Also die Sachen die wir von Amazon gezeigt bekommen haben waren so gut, dass das dann eben der Grund war für den Zuschlag. Es hat dann auch einen Globalvertrag gegeben der zwischen Amazon-Webservice und Allianz AzTec SE abgeschlossen wurde, das heißt, da gibt es eine enge Zusammenarbeit, das heißt, Folgeprojekte, die in dem Umfeld

unterwegs sein werden, können sich schon einmal auf diesen Globalvertrag sozusagen draufsetzen und müssen da nicht noch einmal die ganzen Evaluierungen machen.

A: (?) also nur zum Verständnis nochmal, du meinst, bei diesen 3 Großen ist jetzt kaum ein Unterschied jetzt zu sehen, sage ich jetzt mal so, was die eigentliche Leistung usw. angeht vom Technischen her usw., natürlich hat jeder seine anderen Schwerpunkte, Microsoft ist eher Microsoft lastig usw. usf., aber da ist auch sehr viel Renommee auch wen haben sie als Kunden? Sind es vergleichbare Kunden schon in dieser Cloud drinnen, dass man sagt, okay, da gibt es schon Erfahrungen usw. usf. Und bei der Auswahl, ich meine, bei den 3 großen ist es schwer, die sind alle zertifiziert wahrscheinlich nach allen Richtungen, aber ich würde sagen, das glaube ich, ist auch so ein wichtiger Punkt, wenn man eine Auswahl macht sollte man schauen, weil man es selbst nicht überprüfen kann gescheit.

B: Genau, also die AWS ist 27001 zertifiziert und wenn wir die Möglichkeit haben versuchen wir immer solche Partner vorrangig auszuwählen, weil wir damit so Zertifizierungsketten aufbauen können.

A: Gut, deine Meinung kurz oder deine Info dazu, Datenschutz in der Public Cloud bei den Großen? Ich sage jetzt mal, es ist unterschiedlich, es kommt wahrscheinlich auch immer drauf an was für ein Modell implementiert ist, Infrastructure as a Service, Plattform as a Service oder Software as a Service, aber vielleicht ein bisschen Info von dir dazu noch.

B: Naja sagen wir, eben genau auf welcher Ebene setzt es an und wir haben die Erfahrung gemacht, über gewisse Sachen diskutieren wir einfach nicht. Also wir wären nie in eine Public Cloud gegangen wenn wir nicht die Möglichkeit gehabt hätten wirklich diese End-To-End-Verschlüsselung zu implementieren mit dem externen Key Management, alles andere ist sozusagen auf Treu und Glauben wie wir seit Snowden wissen, man weiß ja eigentlich nie wer dann als Sub-Sub-Subunternehmer von diesen Providern auch angestellt wird, also bevor wir uns da auf irgendwelche rechtlichen, vertraglichen oder organisatorischen Regelungen verlassen, versuchen wir immer lieber technische Lösungen die sozusagen 100%ig wasserdicht sind zu implementieren und das haben wir eben über dieses externe Key Management gemacht und damit ist die, sind, fallen eine ganze Menge von

Bedrohungsvektoren eigentlich weg.
A: Okay. Ja, ich nehme mal an Zugriffssicherheit in der Public Cloud ähnlich gestaltet wie das was wir jetzt gerade (?) verschlüsselt, nur mit wie oben genannt Berechtigungskonzepte usw.
B: Genau
A: Die Frage für mich, ich meine, grundsätzlich hätte ja der Public Cloud-Provider auch Zugriff auf gewisse Sachen, also ich sage jetzt einmal auf die Server oder Infrastructure as a Service, ich glaube, Betriebssystem-Oberkante ist beim Provider im Prinzip auch.
B: Genau, aber das ist die Grenze und sobald es in die Applikationsschicht geht, ist es sichergestellt, dass auch niemand der sozusagen Admin-Rechte auf diesem Server hat, irgendwelche Files auslesen könnte oder in die Datenbank reinschauen kann weil die eben verschlüsselt ist und damit haben wir durch die Verschlüsselung eine klare Grenzlinie eingezogen zwischen der Applikationswelt und der darunterliegenden Infrastrukturwelt. Und aus meiner Sicht ist es nur so möglich für ein großes Unternehmen die Vorteile und die bestehenden definitiv vom Public Cloud zu nutzen.
A: Gut. Dann haben wir, machen wir die Integrität, Verfügbarkeit, Vertraulichkeit der Daten wo wir vorher oben schon darüber gesprochen haben, gibt es da vielleicht irgendwelche Themen, die man besonders im Fokus haben muss, wenn man sagt, man verwendet die Public Cloud für eine Applikation oder für ein System?
B: Naja Integrität ist klar, Vertraulichkeit ist auch klar, Verfügbarkeit, also wir haben natürlich mit Amazon Webservices den Vorteil, dass die sozusagen im Regional Desaster-Fall auch sozusagen zwei oder Multi-Standortkonzepte fahren, einerseits im kleineren Bereich, also ich glaube, bis 20 Kilometer und dann natürlich auch die Ausweichrechenzentren, das heißt, man kriegt eigentlich, wenn man jetzt rein die Infrastruktur-Plattform hernimmt, sehr hohe Verfügbarkeitszeiten zusammen und ich meine, wir haben ein bisschen den Vergleich weil die Allianz selbst in Frankfurt das neue Rechenzentrum hat, also diese Verfügbarkeitszeiten die sozusagen diese professionellen Betreiber haben sind schon extrem gut, ist natürlich auch was man zahlt, aber ich sage mal dieses mögliche Argument von Gegnern von Public Cloud-Lösungen, naja aber die Verfügbarkeit usw. also da haben

wir eher die Erfahrung gemacht, dass das Gegenteil da ist, dass man auf der Publicseite bessere Verfügbarkeitszahlen hat als auf den internen, aber das ist natürlich auch eine Kostenfrage.

A: Okay, ein Thema was man immer wieder liest in Bezug auf Public Cloud ist diese Standardregelung, wenn ich sage, es gibt ja gesetzliche Vorschriften oft, dass die Daten nicht irgendwo auf der Welt liegen dürfen, sage ich jetzt mal so, wie siehst du dieses Problem in, bei den Public Cloud-Lösungen?

B: Da hat Österreich als EU-Mitgliedsland natürlich da ein bisschen leichtere Voraussetzungen, also es gibt Länder wie Spanien, Polen, Schweiz natürlich als Nicht-EU-Land, die sehr strikte Regeln haben dahingehend, sagen wir es mal überspitzen, die Daten das Land nie verlassen dürfen. In Österreich ist das nicht so krass. Ich sage mal, auch hier hilft uns das ganze Thema Verschlüsselung und Key Management, weil auch sozusagen ein Zugriff auf diese Daten, ein unberechtigter Zugriff auf diese Daten ja noch immer nicht dazu führt, dass ein Angreifer dann wirklich verwertbare Daten in der Hand hat. Also die Encryption die da verwendet wird, ist schon so, dass man das nicht so über das Wochenende sozusagen entschlüsseln kann und da Österreich halt auf der anderen Seite auch keine rechtlichen Vorgaben, dass man jetzt nicht nach Deutschland gehen dürfte mit diesen Rechenzentrumsleistungen war das eigentlich kein Thema. Und wie gesagt, in Bezug auf Standorte, kleinräumiges Desaster, Recovery und großräumiges Desaster, Recovery sind diese Infrastrukturprovider im Public Cloud-Bereich extrem gut aufgestellt.

A: Ich glaube, (?) gibt es ja die Möglichkeit sogar einzuschränken was für Regionen man verwenden darf. Also ja. So dann hätte ich noch zu den Public Clouds kurz eine Info von dir noch gerne gehabt was Vertragsinhalte angeht sage ich das mal, wenn man so einen Vertrag abschließt mit einem Public Cloud-Provider, was ist deiner Meinung nach, sind so wichtige Punkte die unbedingt geregelt gehören vertraglich? Wir wissen, wir haben jetzt vorhergesagt, man will sich nicht unbedingt auf diese Vertraglichen verlassen, sondern man will technische Lösungen, dass man es nicht braucht, aber was sind trotzdem aus deiner Sicht Dinge, vertragliche Inhalte die unbedingt geregelt gehören, wenn man mit einem Public Cloud-Provider zusammenarbeitet?

B: Ja also diese ganzen Vertragsverhandlungen waren insofern interessant weil wie ich vorher schon gesagt habe, diese Unternehmen nicht diskutieren jetzt im Sinne von, dass man diese Vertragsinhalte sich da in gegenseitigem Dialog da irgendwie aushandelt, sondern es ist so, dass die einen Katalog von Vertragspunkten haben und den kann man als Kunde sozusagen akzeptieren oder man sagt, nein man kann es nicht akzeptieren, dann kann man aber auch nicht Kunde dort sein, also wie gesagt, die sind da sehr strikt. Die anderen Sachen wie die Preise usw. die Volumina usw., die gehen auch nach einem definierten Modell das eigentlich für den Kunden nicht zur Verhandlung steht, das heißt, man kann sozusagen einmal schauen ob die Punkte die einem als Unternehmen wichtig sind in diesen Vertragsinhalten drinnen sind und das wenn man es jetzt aus Securitysicht heraus betrachtet, sind eben genau die Punkt wie Verfügbarkeit, Integrität, Vertraulichkeit und zum Beispiel ein Punkt war ob es eben möglich ist dieses Amazon Key Management durch unser eigenes Key Management zu ersetzen und das war der Fall, also das war an sich kein Problem und wurde auch dann so in dem Vertrag eben festgehalten, das bedeutet bei uns zum Beispiel, dass wir regelmäßig die Encryption Keys auf USB-Stick auslagern bei uns und bei einem Notar hinterlegen damit, falls in irgendeiner Form einmal ein Problem auftritt, wir nicht nur unsere eigenen Kopien vom Schlüssel haben, sondern die auch noch extra hinterlegt haben. Wenn wir jetzt die Verschlüsselungslösung von Amazon genommen hätten, dann wären diese Prozesse natürlich alle fix fertig schon da gewesen, also man muss dann schauen wo die Andockstellen sind in diese Vertragswerke aufgrund dessen weil man halt bestimmte Sachen anders haben möchte, aber nochmal, also die Flexibilität von diesen großen Unternehmen ist sehr, sehr eingeschränkt und die können eigentlich von ihrem Geschäftsmodell her nur so operieren wenn sie eben keine Sonderlocken zulassen.

A: Okay. Dann das waren im Prinzip einmal die inhaltlichen Themen vom Interview was ich abfragen wollte. Was ich jetzt noch kurz mit dir machen will, ich würde dir nur gerne einmal so einen groben Überblick über die Checkliste, die ich erstellen möchte dir zeigen und hätte gerne einfach ein Feedback von dir dazu ob du sagst, ja, die geht in die richtige Richtung oder nein, da solltest du was anders machen oder das würde nicht so passen. Also grundsätzlich zur Erklärung, ich habe 4, also im Plan sind 4 Checklisten die natürlich miteinander ein bisschen verwoben auch sind,

aber grundsätzlich einmal eine allgemeine davor für die Auswahl des Public Cloud-Providers, da sind so Themen drinnen, gibt es Zertifizierungen bzw. Überprüfungen von Dritten, Rechts- und Gerichtsstand passt der zu meinem Rechts- und Gerichtsstand dazu den ich als Unternehmen habe, Offenbarungspflichten, Ermittlungsbefugnisse, die Lokation, Geschäftsbedingungen, also diese Sachen einmal, gibt es Verschlüsselungsverfahren usw. das einmal für die Auswahl die wären eh das meiste was wir im Gespräch jetzt gehabt haben würde ich da einmal für die Auswahl, dann würde es weiter gehen, dass ich sage in der Hinsicht was sind für vertragliche Inhalte, da würde es, also was man dazu auch noch erwähnen sollte, bei allen Checklisten sollte das so aufgebaut sein, dass ich einen Basisteil habe der für alle Arten der Implementation zählt und dann möglicherweise einen speziellen Teil für Infrastructure as a Service, einen speziellen Teil für Plattform as a Service, einen speziellen Teil für Software as a Service weil ich denke, Infrastructure as a Service da habe ich sehr viele Pflichten die noch bei mir selber liegen wenn ich es verwende Public Cloud und das wird immer mehr Richtung Cloud-Provider verlagert je mehr ich Richtung Software as a Service gehe und deswegen habe ich gemeint, dass man diese einzelnen Teil so ein bisschen anders darstellt drinnen. Also nächster wären eben nachher die vertraglichen Inhalte, eh schon wie wir vorher gerade gesagt haben auch, das ist vieles ähnlich mit der Auswahl, nämlich auch hat man Service, ist mein Service überprüft nach einer Zertifizierung, das ich nutzen will drinnen. Wie kann ich ein Ausstiegsszenario und diese Sachen, was vertraglich halt regelbar sind, dass die alle abgefragt werden in der Checkliste, das wäre von den vertraglichen Inhalten her und dann würden schon die organisatorischen und technischen Maßnahmen kommen wo ich sage, bei organisatorischen Maßnahmen würde es so abgebildet sein, wie habe ich einen Prozess umgesetzt, dass ich Auskunft geben kann über die Daten? Habe ich einen Prozess umgesetzt, dass ich es richtigstellen kann die Daten auf Wunsch? Habe ich, dass ich sie übertragen kann die Daten auf, dass ich, habe ich Prozesse, die überprüfen ob ich das in einem Jahr immer noch machen kann zum Beispiel. Habe ich auch Benutzer so wie du gesagt hast, also bei uns bei der Allianz passiert, dass ich jedes Jahr einen Check von dem Rollenmodell habe, ob ich jedes Jahr einmal checke, muss der Mitarbeiter überhaupt diese Rolle noch haben die er da zugeteilt hat, dass ich das überprüfe. Also diese

Thematiken würde ich da in dieser Checkliste abdecken und als letzte nachher die technischen Maßnahmen wo ich sage, überprüfbar, ist die Implementation noch Stand der Technik, ich bin der Meinung, einen Stand der Technik kann ich überprüfen zum Beispiel mit dem BSI-Katalog, BSI bringt, ist zwar sehr Deutschland lastig teilweise, aber bringt jedes Jahr ein Dokument raus für alle möglichen Technikumsetzungen was da momentan der Stand ist der aktuelle für die Bundesbehörden zum Beispiel in Deutschland. Ich glaube, das ist was an dem man sich anhalten kann, wenn man da in diesem Level fährt, steht man recht gut, wenn man das vergleicht.

B: Ja wir haben überhaupt immer eine Policy, dass wir vor jeder Go-Live Phase egal welches Projekt wo halt Daten verwendet werden, immer einen Penetration-Sicherheitstest vorschalten, das heißt, knapp vor dem Go Live wird das von externen Firmen in unserem Namen gemacht, auch in dem Fall wie ich angeführt habe, mit diesem AWS-Kunden und auch da sieht man wie professionell dieser jeweilige Public Cloud-Provider dann auf solche Anfragen hin reagiert. Da muss man auch sagen, also Amazon Webservices hat da extrem pragmatisch und gut reagiert und die Ergebnisse von dem Penetration Test waren auch sehr positiv, also es war eine der besten Implementierungen, die wir jemals gehabt haben. Weil den Applikationsteil selber, den haben wir eh laufend selber im Test, aber auch bei den darunterliegenden Infrastrukturkomponenten waren eigentlich keine Findings, naja, ist auch nicht so schwierig weil natürlich diese großen Provider nicht die Probleme haben mit irgendwelchen toxischen Komponenten die halt schon (?) sind usw. wie es halt in sozusagen Unternehmensumfeldern passieren kann. Also die sind immer am letzten Stand mit ihren Software-Produkten, immer am letzten Stand in Bezug auf Patching und damit ist natürlich der Angriffspunkt für irgendwelche Pen-Tests natürlich viel geringer.

A: Was in technischen notwendigen Maßnahmen bei mir auch noch drin sind, wie eben ist die Übertragung in die Cloud verschlüsselt, ja ich sage jetzt so vom Client draußen, ist die Datenbank verschlüsselt? Ist es auch sichergestellt, dass man nur von der Applikation selbst Daten lesen kann usw. Das würde dann in der Checkliste auch abgefragt werden. Und

B: Genau, ist auch handwerklich!

A: Im Zuge dessen auch noch Software as a Service muss ich natürlich das Ganze dann verlagern Richtung ich fordere es vom Provider, dass er mir es liefert oder dass er eine Zertifizierung dieser Applikation herzeigt, dass es von einem Dritten überprüft wird, dass das der Fall ist. Weil ich selbst kann es schwer überprüfen, es gibt wahrscheinlich bei vielen so Standardüberprüfungsszenarien die ich als Kunde auch machen kann, die sie mir anbieten, aber ich glaub, im Großen und Ganzen muss ja dann nachher auch ein gewisses Vertrauen da sein zum Provider, man kann nicht alles auf Punkt und Siegel immer prüfen und das ist meine persönliche Meinung. Gut. Ja, der Aufbau glaube ich

B: Ja passt schon, eben vor allem die Stufung, weil natürlich Software as a Service einen ganz anderen Umfang hat, also in dem Sinn wo man sagt, okay, es geht nur rein ums Infrastruktur- und Plattform-Providing, aber das ist eh klar.

A: Ja das sehe ich aus dann würde ich sagen, bei der Auswahl des Providers muss man auch ganz genau schauen was will ich für einen Service umsetzen, ob vielleicht bei gewissen Services ganz einfach ein anderer Provider schon mehr Erfahrung hätte. Ja. Ich nehme zum Beispiel jetzt, wenn ich Office 365 hernehme, würde ich wahrscheinlich nicht AWS gehen, sondern das würde Microsoft logischerweise sein. Okay, Thomas dann danke ich dir für das Interview.