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

Einleitung: In der Versicherungsbranche gibt es ein sehr breites Angebot an Versicherungsprodukten. Dieses breite Angebot und die hohe Komplexität der Produkte verursachen 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 Fraunhofer 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, p. 11). Diese neuen Technologien sollen eine erhebliche Effizienzsteigerung in der Versicherungsbranche ermöglichen. Laut Cloud Monitor 2019 setzen schon dreiviertel der Unternehmen in Deutschland Cloud Computing ein. Allerdings setzen hier nur 35 Prozent eine Public Cloud Lösung ein und für 37 Prozent ist diese Form des Cloud Computing derzeit kein Thema. (KPMG, 2019). Durch den Einsatz von Public Cloud Lösungen entstehen einige organisatorische und rechtliche Anforderung (A-SIT, 2016). Diese werden einerseits durch die ständige Steigerung der Datenmengen, aber auch durch gesetzliche Vorschriften (Datenschutzgesetz) notwendig. 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 (DSGVO) 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 der gegenständlichen 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 Verschlüsselung von Daten bei der Übertragung und Speicherung zu erwähnen.

Das konkrete Ziel der Arbeit war 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.

Hier ist besonders auf den bewussten beziehungsweise sensiblen Umgang mit Daten hinzuweisen. Es macht einerseits aus ökonomischer und ökologischer Sicht absolut Sinn gemeinsame IT Infrastrukturen zu nutzen, um sie zur Verfügung zu haben, wenn man sie braucht und anderen zur Verfügung zu stellen, wenn man sie nicht braucht. Allerdings müssen Integrität, Verfügbarkeit und Vertraulichkeit der Informationen gewährleistet sein um einen sicheren, sensiblen Umgang mit den Daten sicherzustellen.

Fragestellung: 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?

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

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

Bezüglich technischer Lösungen und die zukünftige Entwicklung wurden in Zusammenarbeit mit Experten aus dem Bereich Security, IT-Security und Cloudprovider durch Interviews sowie Literatur- und Internetrecherche die nötigen Informationen erarbeitet. Es wurden dazu aus den vorhandenen Themen wie Datenschutz, IT-Sicherheit und Cloud Themenblöcke gebildet und mit den erarbeiteten Informationen in Form von Brainstorming offene Fragen erarbeitet. Die Interviews wurden alle mit einem Leitfaden gestützt durchgeführt. (Vogt & Werner, 2014)

Bevor die Interviews durchgeführt wurden, wurde ein Entwurf eines Frameworks erstellt. Dieser Framework beinhaltet mehrere Checklisten mit denen einerseits die Auswahl des Cloudproviders unterstützt wird und andererseits die Maßnahmen für die Implementierung einer Lösung überprüft werden können. Diese Checklisten wurden im Zuge der Leitfaden unterstützten Interviews auf Vollständigkeit beziehungsweise Anwendbarkeit überprüft. Die Erkenntnisse dieser Prüfung wurden danach in der Erstellung des fertigen Frameworks berücksichtigt.

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

Ergebnisse: Von den Interviewpartnern wurde auf die drei Prinzipien Integrität, Vertraulichkeit und Verfügbarkeit verwiesen. Diese sollen einerseits durch organisatorische und aber auch durch technische Maßnahmen erfüllt werden. Zusätzlich zu den zwei angeführten Blöcken von Maßnahmen sind auch noch vertraglich festzuhaltende Maßnahmen notwendig. Als Ergebnis wurde ausgearbeitet, das es bei Einhaltung dieser Maßnahmen möglich ist, die Kernprozesse der Versicherung in Public Cloud Umgebungen, unter Einhaltung der Datenschutzgrundverordnung, umzusetzen. Die interviewten Spezialisten haben sogar angemerkt, dass durch die Einbeziehung eines Public Cloud Providers möglicherweise die Verfügbarkeit erhöht wird und teilweise einige Aufgaben besser und professioneller durchgeführt werden würden.

Es wurden drei Checklisten für die Überprüfung der umgesetzten beziehungsweise umzusetzenden Maßnahmen und eine für die Auswahl des Public Cloud Providers erstellt. Der Inhalt der Checkliste für die Auswahl des Cloud Providers (siehe Abbildung 1) soll es ermöglichen eine Wertung der möglichen Provider zu erstellen. Anbei die Abbildung dieser Checkliste.

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, PaaS und oder SaaS		
A17.1	Welche Referenzen gibt es für diese Modelle?	Vergleichbare Unternehmen bzw. Services		

Abbildung 1: Checkliste zur Auswahl des Cloud Providers

Die weiteren Checklisten beinhalten die notwendigen vertraglichen Inhalte wie in Abbildung 2 als Beispiel dargestellt. Der Fokus der Fragen beziehungsweise der Hinweise liegen einerseits bei allgemeinen Vertragsinhalten und andererseits speziell auf der Art des Public Cloud Models.

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 2: Checkliste zu vertraglichen Inhalten

In der Checkliste für die organisatorischen Maßnahmen (siehe Abbildung 3) werden alle Änderungen und Maßnahmen übergeprüft, die sich aus der Einführung von notwendigen Prozessen und Verantwortlichkeiten drehen.

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 3 Auszug aus Checkliste zu notwendigen organisatorischen Maßnahmen

Der Inhalt der Checkliste “durchzuführende technische Maßnahmen“ (siehe Abbildung 4)hat den Schwerpunkt auf der technischen Umsetzung der Maßnahmen. 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.

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 4 Auszug Checkliste durchzuführende technische Maßnahmen

Diese Checklisten wurden in den Interviews von den Experten als sehr hilfreich für die Evaluierung von Providern und Erarbeitung beziehungsweise Überprüfung von Maßnahmen für Public Cloud Implementierung angesehen. Die Experten schätzten diese vor allem als gute Grundlage zur Orientierung ein.

Eine der wichtigsten Erkenntnisse ist, dass ein besonderes Augenmerk auf der Überprüfung der umgesetzten Prozesse und technischen Maßnahmen liegen soll. Regelmäßige Überprüfungen dieser garantieren, dass die Wirksamkeit, Aktualität und Notwendigkeit der Maßnahmen noch gegeben ist und können zu notwendigen Änderungen dieser führen.

Es wurde allerdings angemerkt, dass trotz aller Maßnahmen und Kontrollmechanismen es notwendig ist, 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.

Literaturverzeichnis

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

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

KPMG, 2019. *Cloud Monitor 2019.* [Online]
Available at: https://hub.kpmg.de/hubfs/LandingPages-PDF/kpmg-cloud-monitor-2019.pdf?utm_campaign=Cloud%20Monitor%202019&utm_source=hs_automation&utm_medium=email&utm_content=73821190&_hsenc=p2ANqtz--L8yEzxql_Cc-Dl3vJPX3eYiyaRj5F71r8ZkUFqKQHY1uKJ1b2F0AT2OEWPgp29VGAvLMj
[Accessed 23 12 2019].

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

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

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