Institut für Rechnergestützte Ingenieursysteme

Universität Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

Diplomarbeit Nr. 3697

Kritische Betrachtung der Sicherheitsaspekte von BPM in der Cloud

Sabrina Müller

Studiengang:	Informatik
Prüfer/in:	Univ-Prof. Hon-Prof. Dr. Dieter Roller
Betreuer/in:	Dipl.-Inf. Felix Baumann
Beginn am:	03. November 2014
Beendet am:	05. Mai 2015
CR-Nummer:	H.4.1, H.3.5, K.6.5

Kurzfassung

Das Thema Cloud Computing hat in den letzten Jahren immer mehr an Bedeutung gewonnen, insbesondere Klein- und mittelständische Firmen können von der Cloud profitieren, da z.B. weniger in den Aufbau einer eigenen IT investiert werden muss. Die Kombination von BPM und Cloud Computing steht allerdings noch am Anfang ihrer Entwicklung. Zwar bieten schon einige Unternehmen BPM in der Cloud an (BPMaaS) und der Markt wächst stetig aber das Angebot ist momentan noch überschaubar, in Bezug auf Benutzung und Entwicklung. Der Vorteil Geschäftsprozesse in der Cloud zu bearbeiten geht Hand in Hand mit den Vorteilen des Cloud Computing im Allgemeinen. Allerdings muss auch, ungeachtet der Vorteile, die die Cloud mit sich bringt, genau bedacht werden, welche Daten in die Cloud übermittelt werden und welcher Cloudanbieter ausgewählt wird. Insbesondere der Datenschutz und die Datensicherheit spielen hier eine große Rolle. Denn wenn in Deutschland personenbezogene Daten in die Cloud ausgelagert werden, müssen diese gemäß den Regelungen des Bundesdatenschutzgesetzes behandelt werden. Da der Cloudnutzer für den Schutz dieser Daten verantwortlich bleibt, auch wenn diese auf den Servern des Cloud Service Provider liegen, besteht hierbei große Vorsicht bei der Auswahl des Cloudanbieters. Vor allem wenn die Server desjenigen außerhalb des Europäischen Wirtschaftsraumes (EWR) liegen, wie z.B. in den USA, da dort ein weitaus geringeres Datenschutzniveau besteht als in Deutschland. Das Ziel dieser Diplomarbeit ist es, diese Schwierigkeiten in Bezug auf Datenschutz und Datensicherheit offenzulegen. Mittels eines Kriterienkataloges werden die wichtigsten Anforderungen und Sicherheitskriterien an die Cloud aufgelistet und mit denen der Cloudanbieter verglichen und eingeordnet. Vor diesem Hintergrund werden auch Möglichkeiten betrachtet, inwiefern und mit welchen Mitteln sensible Daten anonymisiert werden können, um eine rechtskonforme Speicherung der Daten, gemäß dem Bundesdatenschutzgesetzes, gewährleisten zu können.

Abstract

The topic of cloud computing became more important in the last few years, especially in relation to small enterprises, because they can benefit from the advantages of the Cloud, such as less investment in the own IT infrastructure. But the combination of BPM and Cloud Computing is only just beginning to develop. Although some companies offer Business Process Management in the Cloud and the market continues to grow, but the offer is relatively modest. The benefits of moving business processes into the cloud (such as BPMaaS) are the same as those which offers cloud computing in general. What need to be considered, however, is which data is to be outsourced in the cloud and which provider needs to be selected. In particular, data protection and data security play an important role in this topic. If german personal data are transferred into the cloud, the data must be treated in accordance with the German Federal Data Protection Act. The cloud computing user stays responsible for all content and data, even if this data will be stored on the provider's server, so caution is also recommended in this case. Especially when these servers are outside of the European Economic Area, such as USA, because there consist a much lower level of data privacy protection than in Germany. The purpose of this diploma thesis is to explore these difficulties in relation to data protection and data security. By means of a catalog of criteria, the most important requirements and security criteria will be listed and compared with those of the provider. Against this background a number of possible opportunities for a concept of 'anonymization' of data are considered, to secure that the data storage complies with legal requirements, such as the German Federal Data Protection Act.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Verzeichnis der Listings

Kapitel 1.

Einleitung

1.1. Vorwort

Der Begriff Cloud Computing ist zurzeit in der IT allgegenwärtig[1]. Cloud Computing steht für „Datenverarbeitung in der Wolke“. Für diese Datenwolke existieren inzwischen viele verschiedene Definitionen. Für die einen ist es eine neuartige Technologie bzw. die nächste Generation des Internets, für andere eine vielversprechende Chance für neue Geschäftsideen. Eine Allgemeine Umschreibung der Cloud wurde vom BSI (Bundesamt für Sicherheit in der Informationstechnologie) auf den Weg gebracht:

> „Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.“[2]

Um die Sicherheit von Daten in einer Cloud zu gewährleisten, müssen sich Unternehmen gründlich über den Anbieter und dessen Dienstleistungen informieren. Damit die IT-Dienstleistungen (BPM) aus der Cloud zuverlässig genutzt werden können, ist die Informationssicherheit einer der Schlüsselfaktoren.[3] Angesichts der weltweiten und hoch komplexen Verknüpfung von Rechenleistungen wird – über das bereits im Rahmen des „klassischen“ IT-Outsourcing hohe Absicherungsbedürfnis hinaus – die Umsetzung der regulatorischen Anforderungen an Datenschutz und Datensicherheit zur zentralen Herausforderung des Cloud Computing. Den Schwerpunkt dieser Arbeit bilden die Themen Datenschutz und Datensicherheit in der Cloud im Allgemeinen und im Speziellen in Bezug auf Business Process Management in der Cloud.

[1] http://www.business-cloud.de/wp-content/uploads/2014/07/STUDIE-Platform-as-a-Service01.pdf
[2] https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html
[3] http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Themen/cloud-computing.html

1.2. Motivation

Wie schon erwähnt ist Cloud Computing derzeit ein sehr aktuelles Thema, ebenso wie Business Process Management.[4] In dieser Arbeit sollen vor allem die sicherheitskritisch Fragen bei Cloud Computing und bei BPM in der Cloud untersucht werden. Da beide Themen momentan im Trend liegen, sollen unter anderem der Datenschutz und die Schutzwürdigkeit bei Geschäftsprozessmodellen in der Cloud und Verbesserungsvorschläge diesbezüglich analysiert werden. Denn bei der personenbezogenen Datenverarbeitung im Rahmen des Cloud Computing treten rechtliche und technische Fragestellungen auf, die bisher nur in geringem Maße aufgearbeitet sind. Da sich diese Form der Datenverarbeitung immer größerer Beliebtheit erfreut, ist es nötig, die Rahmenbedingungen des Datenschutzes zu untersuchen und zu benennen. Das zentrale Problem des Cloud Computing besteht darin, die Integrität und Vertraulichkeit der Datenverarbeitung des Cloud-Nutzers zu gewährleisten. Dies gilt nicht nur für die Verarbeitung personenbezogener, sondern sämtlicher Daten, bei denen es auf Vertraulichkeit und Integrität ankommt, z.B. für Betriebs- und Geschäftsgeheimnisse, für Forschungsdaten oder für anderweitig immateriell-rechtlich geschützte Daten. Es geht um das Unterbinden unberechtigter und schädigender Zugriffe Dritter.[5]

Gliederung

Die Arbeit ist in folgender Weise gegliedert:

Kapitel 1 – Einleitung: Vorwort und Motivation

Kapitel 2 – Grundlagen: Grundlagen dieser Arbeit - Cloud Computing und BPM.

Kapitel 3 – Kriterienkatalog: Erklärung und Aufbau des Kriterienkataloges

Kapitel 4 – Umfrageauswertung: Umfrageauswertung und Analyse der BPM Systeme

Kapitel 5 – Sicherheit und Datenschutz: Sicherheit und Datenschutz

Kapitel 6 – Anonymisierbarkeit: Anonymisierbarkeit von Daten in Geschäftsprozessen

Kapitel 7 – Zusammenfassung und Ausblick Zusammenfassung der Ergebnisse der Diplomarbeit und Ausblick

[4] http://www.kurze-prozesse.de/2014/02/26/bpm-quintessenz-wertet-35-studien-aus/
[5] https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html

Kapitel 2.

Grundlagen

In diesem Abschnitt sollen unter anderem die Grundlagen über Cloud Computing und Business Process Management vermittelt werden.

2.1. Cloud Computing

Was genau ist Cloud Computing, wie kann man es definieren? Momentan gibt es viele Interpretationen, aber keine standardisierte oder einheitliche Definition dafür. Im nächsten Abschnitt soll deutlich gemacht werden wie Cloud Computing einzuordnen ist.

2.1.1. Definition

Einige gängige Definitionen für Cloud Computing werden in diesem Abschnitt aufgeführt.

> „Cloud Computing erlaubt die Bereitstellung und Nutzung von IT-Infrastruktur, von Plattformen und von Anwendungen aller Art als im Web elektronisch verfügbare Dienste. Der Begriff Cloud soll dabei andeuten, dass die Dienste von einem Provider im Internet (bzw. im Intranet eines größeren Unternehmens) erbracht werden. Die Nutzer der Cloud-Dienste können ihre eigenen Angebote wiederum selbst als Dienste im Internet bzw. Intranet anbieten.“ (Baun u. a. 2010)

> „Cloud computing is a model for enabling 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.“[1]

> „Cloud Computing verspricht Rechenzeit, Netzwerkkapazitäten, Speicher, Datenbanken und selbst ganze Anwendungen als Service zur Verfügung zu stellen. Dieser Service ist schnell und flexibel verfügbar und kann durch den Nutzer selbst per Selfservice zugeordnet werden. Dazu sollen keine oder nur geringe

[1] http://www.nist.gov/itl/cloud

> Vorabinvestitionen notwendig sein, und die Abrechnung kann in Abhängigkeit von der Nutzung erfolgen.“ (Barton 2014)

Wie man, sieht gibt es unterschiedliche Ansichten in Bezug auf die Definition von Cloud Computing, allerdings gibt es durchaus auch Gemeinsamkeiten. Im Großen und Ganzen geht es bei Cloud Computing darum, IT-Dienstleistungen wie bzw. Infrastruktur (Rechenleistung, Speicherplatz), Plattformen und Software über ein Netzwerk zur Verfügung zu stellen. Diese Dienste werden von einem externen Dienstleister dem Cloud Service Provider (CSP) angeboten. Diese Cloud-Dienste sind dynamisch skalierbar, d.h. wenn eine Anwendung zusätzliche Ressourcen benötigt, können diese sofort und ohne großen Aufwand automatisch dazu geschaltet werden.

2.1.2. Organisationsformen

In der Praxis haben sich verschiedene Möglichkeiten bzw. Organisationsformen etabliert, die angebotenen Services in der Cloud bereitzustellen. Diese unterscheiden sich hauptsächlich nach dem Betriebsmodell, das heißt, nach dem Besitz der IT-Infrastruktur sowie der Zuständigkeit für Verwaltung und Betrieb. Ebenso wird unterschieden, ob die Services der breiten Masse oder ausschließlich bestimmten Benutzern zugänglich sind. (Lissen, Brünger und Damhorst 2014) In diesem Abschnitt werden die gängigsten Organisationsformen erläutert.

2.1.2.1. Public Cloud

Die „Public-Cloud“ ist sicherlich die bekannteste Organisationsform im Cloud Computing. Eigentümer, Betreiber und Verwalter der „Public Cloud“ ist ein externer Cloud Service Provider (CSP), welcher es den Benutzern ermöglicht mittels eines Webbrowsers über das Internet auf in der Regel standardisierte IT-Ressourcen und Anwendungsprogrammen zuzugreifen. Die IT-Ressourcen sind das Eigentum des Serviceproviders und werden von diesem gemanagt, in einem Pool zusammengefasst und kundenübergreifend genutzt. Der Anbieter verfolgt einen One-to-many-Ansatz, d. h. die angebotenen Leistungen sprechen ein breites Kundenspektrum an. Webmailer-Dienste oder die bekannten Google-Docs[2] sind ebenso Beispiele für Public Cloud Angebote wie die kostenpflichtigen Services eines Microsoft Office 365[3]. Wesentliches Merkmal der Public Cloud ist, dass die Benutzer organisatorisch nicht miteinander verbunden sind, sondern sich lediglich eine virtualisierte, multimandantenfähige IT-Infrastruktur miteinander teilen. Dies bedeutet, dass Daten von unterschiedlichen Benutzern auf gemeinsamen IT-Ressourcen gespeichert und verarbeitet werden, jedoch logisch getrennt bleiben. Public Clouds stehen hinsichtlich ihrer Sicherheit im Fokus der öffentlichen Diskussion. Sie werden von Vertretern aus Wissenschaft und Wirtschaft als tendenziell unsicher eingestuft, da der Benutzer die Kontrolle über seine Daten und gegebenenfalls

[2]https://www.google.de/intl/de/docs/about
[3]https://www.microsoft.com/de-de/download/office.aspx

die seiner Kunden an den Cloud Service Provider abgibt. Somit hat der Benutzer keinen direkten Einfluss mehr auf die Sicherheit der Daten und die Einhaltung von gesetzlichen Vorgaben. Ungeachtet dessen behält er jedoch die Verantwortung für die Sicherheit der Daten in Bezug auf die Einhaltung der gesetzlichen Vorschriften, wie sie sich zum Beispiel aus dem Bundesdatenschutzgesetz ergeben. (Lissen, Brünger und Damhorst 2014)

2.1.2.2. Private Cloud

Private Clouds unterscheiden sich von Public Clouds im Leistungszugang: Während Public Clouds für jedermann zugänglich sind, ist der Zugang zu Private Clouds auf bestimmte Nutzergruppen beschränkt. Man könnte die Private Cloud als eine unternehmensindividuelle Cloud beschreiben, die oft von einem Unternehmen selbst betrieben wird. Daher ist der Zugang zu einer Private Cloud in der Regel begrenzt auf Mitarbeiter, eventuell auch auf Lieferanten und Kunden. Erfolgt der Betrieb durch einen externen Dienstleister auf Basis von individuell vereinbarten Service-Level-Agreements (SLA) und die IT-Infrastruktur ist Eigentum der nutzenden Organisation, spricht man von einer Managed Private Cloud. Verwaltet der externe Cloud Service Provider die Cloud nicht nur, sondern ist auch Besitzer der IT-Infrastruktur, spricht man von einer „Outsourced-Private-Cloud“. Im Gegensatz zur Public Cloud behält die Organisation vollständig die Kontrolle über ihre Daten. Nachteil der Private Cloud sind die potenziell höheren Kosten, da die Cloud-Infrastruktur nicht mit mehreren Benutzergruppen geteilt wird.

2.1.2.3. Hybrid Cloud

Die Hybrid Cloud bezeichnet Mischformen aus Private Cloud, wo datenschutzkritische Anwendungen und Daten im Unternehmen verarbeitet werden, Public Cloud mit skalierbaren Cloud-Diensten und traditioneller IT-Umgebung. Bei Spitzenbedarf lässt sich damit eine selbstverwaltete On-Premise IT-Infrastruktur mit weiteren Ressourcen und IT-Services aus der Public Cloud, wie bzw. Anwendungen, Rechenleistung oder Speicher, von einem oder mehreren Anbietern erweitern, ohne dabei die eigene Infrastruktur aufrüsten zu müssen. Die Herausforderung besteht hier in der Trennung der Geschäftsprozesse in datenschutzkritische und -unkritische Workflows. Ein geeignetes Anwendungsbeispiel ist ein großer Onlinehändler. Das Unternehmen bietet Privatkunden eine umfassende Plattform für den Onlinehandel im Internet mit mehreren Millionen Artikeln an. Der Online-Händler zählt im Monat bis zu mehreren Millionen Benutzeranfragen. Entstehende Lastspitzen, wie am Jahresende im Weihnachtsgeschäft, können signifikante Auswirkungen auf die Verfügbarkeit und Performance des Internetportals haben. Dieser Spitzenbedarf kann von dem Unternehmen durch eine intelligente hybride Cloud-Lösung abgefangen werden. Hybrid Clouds sind so konzipiert, dass man sie schnell und unkompliziert skalieren kann und somit ist es Unternehmen möglich flexibel auf den Bedarf der Kunden zu reagieren.

2.1.2.4. Community Cloud

In einer Community Cloud schließen sich Unternehmen oder Organisationen mit gleichen Anforderungen zusammen und bilden aus ihren Private Clouds die Community Cloud, die dann nur den Mitgliedern der Community zugänglich ist. Die gemeinsamen Interessen können beispielsweise in der Einhaltung von offiziellen Compliance-Vorgaben, Sicherheitsvorschriften oder Anforderungen an die Performance zu tun haben. Die Community Cloud kann entweder On- oder Off-Premise geführt werden und wird entweder von den teilnehmenden Organisationen selbst oder von externen Managed Service Provider (MSP) betrieben. Der Vorteil solcher Community Clouds liegt in der Reduzierung des Kapazitätsbedarfs durch gemeinsame Benutzung von Ressourcen und somit auch in der Reduzierung der Kosten. Ebenso können viele Anwendungsprogramme von den Community Mitgliedern gemeinsam genutzt werden.

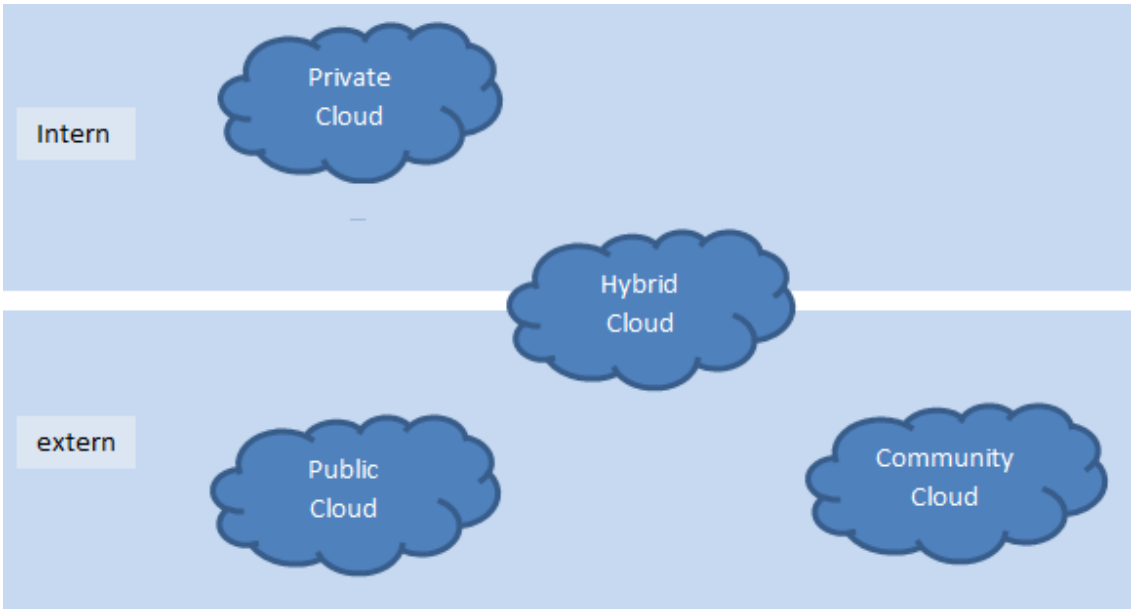


Abbildung 2.1.: Verschiedene Organisationsformen der Cloud

2.1.3. Servicemodelle

In der Cloud gibt es verschiedene Servicemodelle, die unterschiedliche Dienste und Leistungen bereitstellen. In der Praxis hat sich dabei die Unterscheidung in drei Ebenen durchgesetzt, Software as a Service (SaaS), Plattform as a Service (PaaS) und Infrastructure as a Service (IaaS). Bei allen drei Ebenen wird vom Cloud Service Provider die IT-Leistung als Dienst („as a Service“) zur Verfügung gestellt. Welche mittlerweile noch durch weitere Modelle ergänzt wurden. In diesem Abschnitt werden die wichtigsten erläutert.

2.1.3.1. SaaS (Software as a Service)

Unter „Software as a Service“ wird die bedarfsorientierte Bereitstellung von Anwendungsprogrammen durch einen Cloud Service Provider verstanden. Bei der Nutzung von SaaS wird dem Kunden eine Standardsoftwarelösung als Dienstleistung über das Internet zur Verfügung gestellt. Für die Nutzung der Anwendung zahlt er Gebühren an den Provider, der die Software für ihn bereitstellt. Der Kunde kann hierbei einen monatlichen Betrag wählen oder die Software On-Demand, also je nach Bedarf, nutzen und zahlen. Auf der Kundenseite entfällt in dieser Klasse die lokale Software-Installation und mithin auch die Bereitstellung der erforderlichen Ressourcen. (Baun u. a. 2010) Diese Art der Softwarenutzung bietet Vor- und Nachteile. Zum einen, weniger Investitionskosten in die eigene IT, ein geringeres Investitionsrisiko, mehr Mobilität, Konzentration auf die eigentlichen Aufgaben der Firma (Kerngeschäft). Zum anderen, entsteht eine Anbieterabhängigkeit (Vendor-Lock-in), geringere Datensicherheit, Abhängigkeit zum Internet (Datenübertragung). Daher sollte vorab geprüft werden ob der jeweilige SaaS-Anbieter gewisse Normen und Zertifikate einhält bzw. besitzt (z.B. ISO 27001). Beispiele für SaaS sind:

- ◇ Salesforce.com
- ◇ Microsoft CRM online, Office 365[4]
- ◇ Google Apps for Business[5]

2.1.3.2. PaaS (Platform as a Service)

Das Model „Platform as a Service“ richtet sich hauptsächlich an Softwarearchitekten oder Anwendungsentwickler und weniger an Endbenutzer. Die Laufzeitumgebung einer PaaS-Umgebung kann über APIs oder eine Weboberfläche konfiguriert werden. Services zur Entwicklung von Portal- und Anwendungsprogrammen, Integration sowie Datenbanken werden in dieser standardisierten Umgebung bereitgestellt, so dass Software-Hersteller ihre Geschäftslösungen entwickeln und auf die Zielplattform überführen können. (Lissen, Brünger und Damhorst 2014) Diese werden in Entwicklungs- und Ausführungsumgebung unterteilt angeboten, in denen sich eigene Software in einer bestimmten Programmiersprache entwickeln bzw. ausführen lässt. Im Unterschied zu IaaS hat der Benutzer hier keinen direkten Zugriff auf die Recheninstanzen. Im PaaS-Szenario bringt er ausschließlich seine Programmlogik in die Cloud ein, die ihm gegenüber als Programmierschnittstelle auftritt. Beispiele für PaaS sind:

- ◇ Force.com
- ◇ Google App Engine[6]

[4]http://www.microsoft.com/de-de/dynamics/crm-office-365.aspx
[5]https://www.google.com/work/apps/business/
[6]https://cloud.google.com/appengine/docs

- ◇ Microsoft Azure Services[7]

2.1.3.3. IaaS (Infrastructure as a Service)

Die unterste Ebene stellte Services für den Aufbau einer Infrastruktur zur Verfügung und wird mit „Infrastructure as a Service“ bezeichnet. Einem Nutzer wird auf dieser Ebene Rechen-, Speicher- oder Netzkapazität zur Verfügung gestellt. IaaS zeichnet sich zudem durch ein hohes Maß an Virtualisierung und Standardisierung durch den Cloud Service Provider aus. Diese erlaubt es, dass sich mehrere Nutzer einen physikalischen Server teilen. Der Benutzer greift über einen Internetbrowser oder ein mobiles Endgerät auf den IaaS-Service zu und baut darauf beispielsweise eigene Services zum internen oder externen Gebrauch auf. (Lissen, Brünger und Damhorst 2014) Dieser Service des Cloud Computing stellt die Grundlagen der IT zur Verfügung, wobei Nutzer nur für die Geräte zahlen, die sie nutzen: CPU Cores, RAM, Festplattenspeicherplatz und Datentransfer. Für Unternehmen - insbesondere kleine und mittelständische - ist Infrastructure as a Service eine mögliche Alternative gegenüber dem Erwerb und der Instandhaltung von eigener Hardware, was wiederum die Kosten und den Aufwand für die Firmen minimiert. Beispiele für IaaS sind:

- ◇ Amazon EC2[8]
- ◇ Microsoft Windows Azure[9]

2.1.3.4. SECaaS (Security as a Service)

„Security as a Service“ bezieht sich auf die Benutzung von IT-Sicherheitsfunktionen aus der Cloud. Dieser Service umfasst alle Aspekte des Sicherheitsmanagements wie das Login, die Autorisierung, die Authentifizierung, der Schutz von Informationen, Objekten, Diensten und Ressourcen. Da der Cloudprovider für die Upgrades und Wartung der Sicherheitskonzepte verantwortlich ist, ebenso wie für die Installation von Sicherheitsprogrammen und -komponenten gegen neue Bedrohungen, können die Kunden sich auf ihr Kerngeschäft konzentrieren und haben trotzdem immer einen aktuellen und sicheren Schutz. Abgerechnet werden die Leistungen nach der tatsächlichen Nutzung. Unter anderem wird angeboten: Antivirus, Anti-Malware/Spyware, DDoS[10] Protection, Data Loss Prevention (DLP), Verschlüsselung, Anti-Spam, Webfilter, Firewall und Authentifizierung.

[7] http://azure.microsoft.com/de-de/services/cloud-services/
[8] http://aws.amazon.com/de/ec2/
[9] http://azure.microsoft.com/de-de/
[10] https://de.wikipedia.org/wiki/Denial_of_Service

2.1.3.5. BPaaS (Business Process as a Service) / BPMaaS (Business Process Management as a Service)

„Business Process Management“ as a Service unterstützt den Geschäftsprozess nicht direkt sondern den dafür notwendigen Geschäftsprozesslebenszyklus. D. h. BPMaaS stellt Cloud-Services für das Design, die Implementierung, den Betrieb und die Optimierung von Geschäftsprozessen bereit. Business Process Management as a Service bietet mehr Möglichkeiten zur individuellen Anpassung des Prozesses, hat aber auch einen höheren Aufwand als Business Process as a Service[11]. Business Process as a Service ist die direkte Unterstützung eines Geschäftsprozesses. Dazu wird dieser als Cloud-Service gekapselt. Mit BPaaS werden ein oder mehrere Geschäftsprozesse in einen Cloud-Service hochgeladen, der sie ausführt und überwacht. Wie jede andere Cloud-Umgebung ermöglicht es auch BPaaS, Cloud-Software nach einem Pay-Per-Use-Modell zu nutzen, statt in Hardware und Wartung investieren zu müssen. Typische Anwendungsbereiche sind Prozesse, die von einem hohen Standardisierungsgrad und Transaktionsorientierung geprägt sind, z. B. Personalmanagement-, Finanz- und analytische Prozesse.

2.1.3.6. XaaS (Everthing as a Service)

XaaS ist ein Kollektivum, das für die Menge an unterschiedlichen Modellen steht, die mittlerweile als Service angeboten werden. Es bezieht sich auf die Services die heute über die Cloud bzw. das Internet beschafft werden und früher lokal in der firmeneigenen IT bereitgestellt wurden. XaaS ist das Kernstück des Cloud Computings, die obengenannten Services sind alle darin enthalten. Alle X-as-a-Service-Konzepte dienen unter anderem der Kostenreduzierung. Dabei werden Rechenleistungen, Plattformen, Infrastrukturen, Überwachungsaufgaben und viele andere Funktionen und Dienste von Cloud Service Providern übernommen und dem Anwender gegen Leistungsberechnung zur Verfügung gestellt.

2.1.4. Virtualisierung

Cloud Computing basiert unter anderem auf der Virtualisierung von IT-Ressourcen. Das Konzept der Virtualisierung erlaubt eine abstrakte, logische Sicht auf physische Ressourcen und umfasst sowohl Server, Datenspeicher, Netzwerke als auch Software. Die Virtualisierung ermöglicht die Aufteilung der zur Verfügung stehenden Ressourcen auf verschiedene Virtuelle Maschinen (VM). Die virtuelle Maschine bildet die Rechnerarchitektur eines real in Hardware existierenden oder hypothetischen Rechners nach, somit können bzw. mehrere unterschiedliche Betriebssysteme gleichzeitig auf derselben physischen Maschine betrieben werden. Die abstrahierende Schicht zwischen realem Rechner, auf dem die virtuelle Maschine ausgeführt wird und virtueller Maschine wird Hypervisor oder auch Virtual Machine Monitor (VMM) genannt. Der VMM stellt die Virtualisierungsschicht dar, die die

[11] http://www.soa-know-how.de/

gleichzeitige Ausführung mehrerer virtueller Maschinen sowie ihre Steuerung ermöglicht. Aus diesen Ressourcen-Pools können dann nach Bedarf einzelne Anforderungen befriedigt werden. Es ist z. B. möglich, eine bestimmte Plattform für eine spezifische Anwendung dynamisch und passgenau in dem Augenblick zu generieren, wenn sie gebraucht wird. Diese Dienste sollen dabei von mehreren Kunden gleichzeitig genutzt werden können - eine sogenannte multimandanten Architektur. Hierbei ist vor allem wichtig, dass die von den Kunden genutzten Ressourcen voneinander strikt getrennt sind und sich je nach Wunsch skalieren lassen. Um diese Technologie effizient bereitzustellen existieren einige verschiedene Virtualisierungskonzepte.

2.1.4.1. Betriebssystemvirtualisierung

Bei dieser Form der Virtualisierung, die man auch als Container oder Jails bezeichnet, spielt das Host-Betriebssystem in der Virtualisierungsschicht eine entscheidende Rolle (Vgl. Abbildung 2.2). Hier laufen unter einem Betriebssystemkern mehrere voneinander abgeschottete, identische Systemumgebungen bzw. Laufzeitumgebungen. (Baun u. a. 2010)

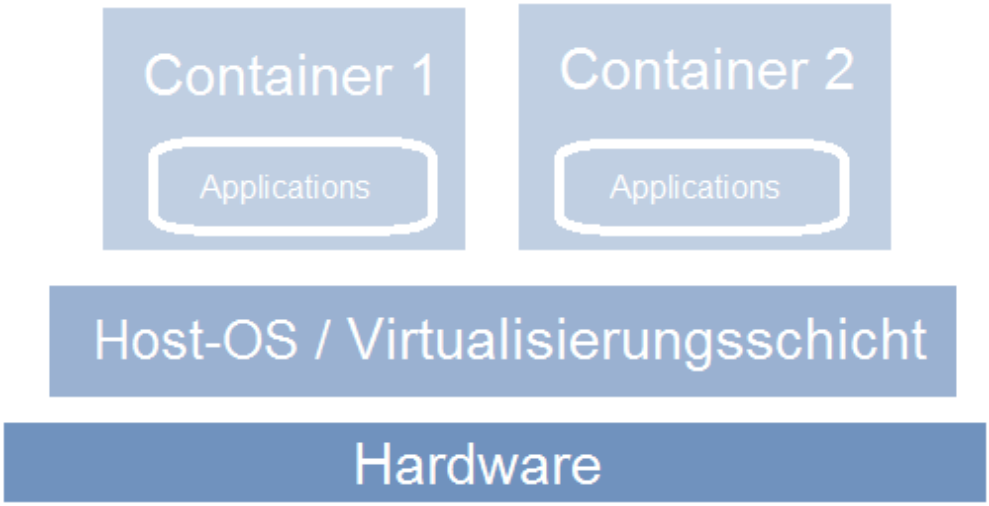


Abbildung 2.2.: Aufbau einer Betriebssystemvirtualisierung

Wobei das System den virtuellen Maschinen „private“ Ressourcen wie Dateisysteme, IP-Adressen, Hostnamen, User-Namespaces zuweist. Dieses Konzept der Virtualisierung bietet eine sehr hohe Performance, aufgrund der effizienten Ausnutzung der Ressourcen und einen hohen Grad an Sicherheit. Der Nachteil der Betriebssystemvirtualisierung ist die geringe Flexibilität, da ausschließlich mehrere unabhängige Instanzen desselben Betriebssystems und nicht verschiedene Betriebssysteme gleichzeitig eingesetzt werden können.

2.1.4.2. Plattformvirtualisierung

Die Plattformvirtualisierung benutzt, im Gegensatz zur Betriebssystemvirtualisierung, eine andere Technologie. Hierbei können verschiedene beliebige Anwendungen und Betriebssysteme in einer virtuellen Umgebung ausgeführt werden. Die Voraussetzungen hierfür schafft ein Hypervisor bzw. ein Virtual Machine Monitor. Er fungiert dabei als Metabetriebssystem, welches die Ressourcen verteilt und die Zugriffe koordiniert. Der Hypervisor kann auf unterschiedliche Art implementiert sein, ein Typ-1 Hypervisor setzt dabei direkt auf der Hardware auf, ein Typ-2 Hypervisor läuft auf einem herkömmlichen Basisbetriebssystem. (Baun u. a. 2010)

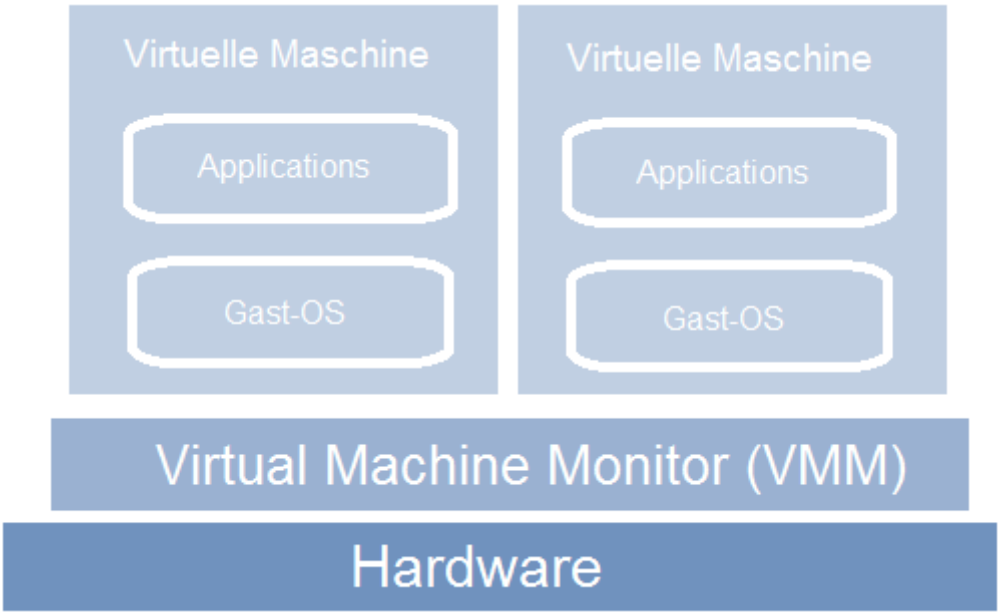


Abbildung 2.3.: Aufbau einer Plattformvirtualisierung mit Typ-1 Hypervisor

Ebenfalls unterschieden wird bei der Plattformvirtualisierung, wie viel des virtuellen Rechners simuliert wird. Auf der einen Seite die vollständige Simulation eines virtuellen Rechners, auf der anderen Seite eine lediglich eine Anwendungsschnittstelle. Bei der vollständigen Virtualisierung werden alle, für einen kompletten virtuellen Rechner benötigten Ressourcen wie z.B. CPU, Hauptspeicher, Laufwerke, Netzwerkkarten und BIOS (basic input/output system), vollständig simuliert.

Die Verarbeitungsgeschwindigkeit ist hierbei aufgrund des reinen Durchreichens von z.B. der CPU-Ressource nahezu gleich einem nicht virtualisierten System. Bei der Para-Virtualisierung stehen den Gast-OS's (Operating System) keine emulierte Hardware zur Verfügung sondern lediglich eine Anwendungsschnittstelle. Dies erfordert die Modifikation der Gast-Betriebssysteme, da alle direkten Hardwarezugriffe durch den entsprechenden Aufruf der

Schnittstelle zum Hypervisor zu ersetzen sind. Da hierbei das Gastsystem eine größere Rolle spielt und gewissermaßen aktiv an der Virtualisierung mitarbeitet, erreicht man tendenziell höhere Durchsatzraten als bei der vollständigen Virtualisierung. (Baun u. a. 2010)

2.1.4.3. Speichervirtualisierung

Die Speichervirtualisierung fügt der Speicherumgebung eine logische - virtuelle - Schicht hinzu, Anwendern gegenüber präsentiert sich das System damit als eine große Einheit. Speicherkomponenten werden dem Anwender in einer logischen Form zur Verfügung gestellt, der vorhandene Speicher kann somit flexibel aufgeteilt werden und ist nicht an die physischen Grenzen gebunden.[12] So können in einem Speichernetz mithilfe der Virtualisierung transparent Speichersysteme hinzugefügt oder entfernt werden, ohne dass der Anwender oder eine Anwendung dadurch beeinträchtigt wird. Anwendungen greifen dadurch also nicht mehr direkt auf z. B. eine bestimmte Festplatte zu, sondern auf die Virtualisierungsschicht. Sinn dieses Ansatzes ist es, eine Vielzahl an physischen Ressourcen logisch zusammenzuführen. Die Datentransfers laufen dabei über ein spezielles Speichernetzwerk (SAN - Storage Area Network) oder ein Firmennetzwerk (LAN - Local Area Network).

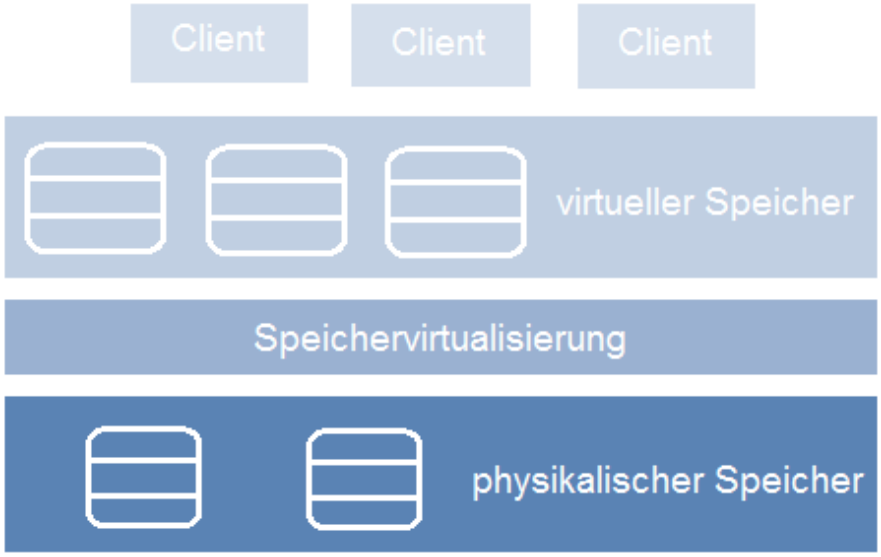


Abbildung 2.4.: Aufbau einer Speichervirtualisierung

[12] https://www.bitkom.org

2.1.4.4. Netzwerkvirtualisierung

Bei der Netzwerk-Virtualisierung werden Netzwerk-Ressourcen, mittels virtualisierende Switches oder Router, zu logischen Einheiten zusammengefasst oder aufgeteilt um unabhängig zu sein von den physischen Gegebenheiten. Die Netzwerkvirtualisierung fügt beispielsweise einem lokalen Netz (Local Area Network, LAN) eine logische - virtuelle - Schicht hinzu (Virtual Local Area Network, VLAN), welche den Anwender oder Kommunikations-Client abkoppelt von dem eigentlichen physischen Netzwerk und der Client somit nur mit der virtuellen Schicht kommuniziert. Diese VLAN's sind virtuell voneinander getrennt, so dass Geräte eines VLAN's nicht mit solchen in anderen VLAN's kommunizieren können. Was sich positiv auf die Sicherheit auswirkt, denn somit können bzw. bestimmte, besonders zu schützende Systeme können in einem eigenen Netz verborgen werden. Allerdings sind der administrative Aufwand und die Programmierung der aktiven Netzwerkkomponenten (Switches) für jene VLAN's höher als bei normalen Netzwerken.

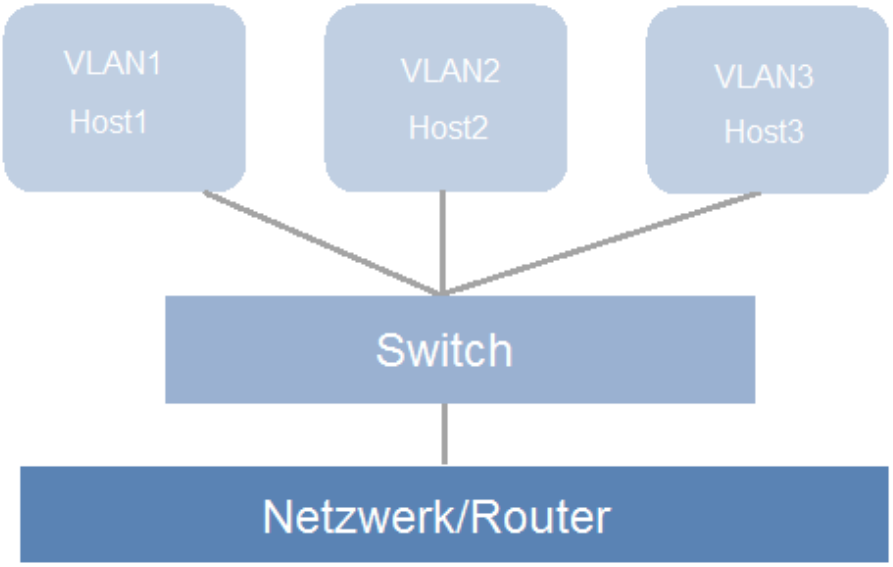


Abbildung 2.5.: Aufbau einer Netzwerkvirtualisierung

2.1.4.5. Anwendungsvirtualisierung

Bei der Anwendungsvirtualisierung handelt es sich um ein Software-Vertriebsmodell, bei dem Anwendungen zentral verwaltet und dem Kunden über ein Netzwerk angeboten werden. Das wesentliche Ziel von Applikationsvirtualisierung besteht darin, Anwendungen von ihrer Umgebung so weit zu isolieren, dass Konflikte mit anderen Programmen oder dem Betriebssystem vermieden werden. Hierbei wird nicht die Hardware virtualisiert, sondern es wird eine Abstraktionsschicht zwischen den einzelnen Anwendungen und dem

Betriebssystem erstellt. Die eigentliche Installation auf dem Zielrechner entfällt hierbei. Es gibt zwei unterschiedliche Verfahren zur Bereitstellung virtueller Anwendungen:

- **Hosted Application:** Hier liegt die Anwendung dem Kunden im Internet vor und wird über bzw. ein Streaming-Protokoll bereitgestellt.
- **Virtual Appliance:** Hier kann die Anwendung vom Kunden heruntergeladen und auf dem eigenen Rechner betrieben werden. (Baun u. a. 2010)

In beiden Fällen ist die Entfernung einer virtualisierten Anwendung um einiges einfacher als bei herkömmlichen Applikationen, da keine Verflechtungen mit dem Betriebssystem existieren oder diese nur virtuell bestehen. In Cloud Umgebungen bildet die Anwendungsvirtualisierung eine wichtige Grundlage für das SaaS-Konzept zur dynamischen Bereitstellung von Software-Komponenten.

2.2. Vorteile und Risiken des Cloud Computings

Wie in vielen Bereichen, so auch im Cloud Computing, ergeben sich Vor- und Nachteile in Bezug auf deren Benutzung. Hier werden einige Chancen und Risiken des Cloud Computing aufgelistet und näher erläutert.

2.2.1. Vorteile

2.2.1.1. Kosten

Ein großer Vorteil, vor allem für mittelständische und Startup-Unternehmen, ist die Kostenersparnis die das Cloud Computing mit sich bringt. Insbesondere Startup-Unternehmen profitieren sehr davon, sich die Investition in eine eigene IT zu ersparen und stattdessen in flexible und dynamische Cloud Services zu investieren. Denn häufig ist es billiger einen On-Demand Service zu mieten anstatt eigene IT-Ressourcen aufzubauen. Aber nicht nur für Startups ergeben sich Kostenvorteile, auch in bereits bestehenden Unternehmen kann Geld eingespart werden, da in der Cloud meistens nur für Leistungen Kosten anfallen die auch benutzt werden (Pay-Per-Use). Bei notwendigem Mehrbedarf können die Ressourcen einfach dazu gebucht bzw. skaliert werden. Ebenso können die Personalkosten gesenkt werden, die für die IT-Abteilung anfallen. Es müssen keine eigenen Server verwaltet werden, die eigene IT auf ein Minimum reduziert werden, Aufwand für eine redundante Infrastruktur (z.B. Backups) fällt weg und falls ein Problem auftritt, kann eine bedarfsgerechte Anmietung von IT-Dienstleistern vorgenommen werden, welches meist billiger ist, als eine eigene kontinuierliche IT-Abteilung zu unterhalten. Auch die Kosten für die Sicherheit können

sinken, denn meist haben Cloud Provider die Möglichkeit Sicherheitsmaßnahmen für mehrere Kunden günstiger und professioneller anbieten als die Kunden mit einer individuellen Implementierung in der eigenen IT.[13]

2.2.1.2. Skalierbarkeit

Eines der wesentlichsten Merkmale der Cloud ist u.a. die Skalierbarkeit der gemieteten Ressourcen. Cloudsysteme sind dynamisch skalierbar, sowohl nach oben (skaling up) wenn z.B. Lastspitzen im Unternehmen auftreten als auch nach unten (skaling down) wenn z.B. saisonal bedingt weniger umgesetzt wird. So können Unternehmen sich umstandsbedingt ihre Ressourcen dynamisch auswählen und sind somit sehr flexibel. Auch in Bezug auf die Sicherheit wirkt sich die gute Skalierbarkeit in der Cloud positiv aus. Bei einem möglichen Ausfall (z.B. auf Grund einer DDoS-Attacke) des Servers des Providers, können die Ressourcen auf andere Server (Redundanz) verteilt werden um somit die Verfügbarkeit des Systems aufrechterhalten zu können.

2.2.1.3. Verfügbarkeit

Auch im Punkt Verfügbarkeit bietet die Cloud einige Vorteile, beispielsweise kann der Verlust von Daten in der Cloud im Vergleich zur eigenen IT verringert werden, wenn die Provider die Kundendaten redundant speichern, d.h. Datenfragmente werden auf mehreren Systemen gespeichert und dupliziert. Somit können vermeintlich verlorene Daten, durch Ausfälle oder Löschungen, oft dennoch wiederhergestellt werden. Ebenso bieten manche Cloud Service Provider eine Hochverfügbarkeit[14] ihrer Services an. Beispielsweise bietet Amazon bei seinem S3 Service eine Beständigkeit der Daten von 99,999999999% und eine Verfügbarkeit von Objekten von 99,99 % an.[15]

2.2.1.4. Mobilität

Mit Mobilität ist gemeint, dass das Unternehmen nicht an einem bestimmten Ort oder PC gebunden ist, wenn es seine Anwendungen in der Cloud ausführen möchte. Die Anwendungen können ortsunabhängig von jedem internetfähigen PC oder Laptop (unabhängig vom Betriebssystem) aufgerufen und benutzt werden. Ein aufwendiges Synchronisieren mit verschiedenen Rechnern oder Versionen entfällt somit. Ebenso können mehrere Mitarbeiter an einem Projekt arbeiten ohne am gleichen Standort sein zu müssen, hierbei werden die Flexibilität und die Mobilität der einzelnen Unternehmen um ein vielfaches verbessert, als wenn ein Produkt nur lokal auf den Firmenrechner gespeichert und verfügbar wäre.

[13] http://www.bitkom.org/de/presse/81149_78524.aspx
[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandG/G2_-Definitionen.pdf
[15] https://aws.amazon.com/de/s3/details/

2.2.1.5. Sicherheit

Über die Sicherheit der Daten in der Cloud lässt sich streiten, viele Unternehmen fürchten um ihre sensiblen Kundendaten, wenn diese auf fremden Rechnern gespeichert werden.[16] Diese Bedenken sind auch nicht immer unbegründet (Siehe Nachteile). Allerdings muss man auch die andere Seite sehen, denn nicht jedes klein- oder mittelständische Unternehmen kann sich die allerneusten Sicherheitsmaßnahmen leisten, wobei diese auch in regelmäßigen Abständen geprüft und aktualisiert werden müssen. Somit ist ein professionell geführtes Cloudunternehmen mit eigens dazu ausgebildeten Mitarbeiten mit mehr Knowhow, besser in der Lage für die Sicherheit der Daten zu sorgen. Falls es doch zu einem Fehler auf Seiten des Providers kommen sollte und dieser in dessen Verantwortungsbereich liegt, ist der Provider Schadenersatzpflichtig gegenüber dem Kunden, sofern dies nicht ausdrücklich gesetzlich ausschließen kann. Anders hingegen ist es, wenn man als Kleinunternehmer selbst für seine Daten verantwortlich ist, so ist man auch selbst für deren Sicherheit und mögliche Fehler zuständig. Dies muss allerdings nicht für Großunternehmen gelten, die selbst ein großen Rechenzentrum haben und nicht direkt auf Services aus der Cloud angewiesen sind bzw. Vorteile daraus ziehen.

2.2.2. Nachteile

2.2.2.1. Verfügbarkeit

Auch wenn ein Cloud Service Provider seine Cloud Services professionell und effizient verwaltet und eine Hochverfügbarkeit von 99,9%, kann es trotzdem zu einem technischen Problem kommen, infolge dessen der Cloud Service dem Kunden nicht zur Verfügung steht, z.B. durch Unwetter oder Stromausfälle. Selbst in hochkomplexen Systemen ist immer mit Fehlern zu rechnen. Wenn ein Kunde nun wichtige Firmendaten, auf Grund eines Ausfalls für längere Zeit nicht verwenden oder abrufen kann, kann dies bereits Schäden verursachen. In Extremfällen kann dies auch zur Insolvenz des betroffenen Unternehmens führen. Deshalb sollte man sich als Nutzer eines Cloud Services gut überlegen, welche Daten man in die Cloud auslagern möchte, bzw. hochsensible Daten die zur Unternehmensweiterführung nötig sind, eher in einer Private Cloud oder auf firmeneigenen Servern redundant zu speichern (Backup).

2.2.2.2. Lock-in

Ein sogenannter Vendor-Lock-in, bezeichnet die Abhängigkeit des Cloud Nutzers an den Cloud Service Provider. Dies kann dadurch geschehen, dass ein CSP keine Möglichkeiten anbietet, die vorhanden Kundendaten auf andere Systeme migrieren und dort nutzen zu können. Unter anderem kann dies der Fall sein, wenn der Kunde einen Anbieterwechsel

[16] http://www.bitkom.org/de/markt_statistik/64026_81203.aspx

vollziehen möchte, der aktuelle CSP aber keine offenen Standards und Schnittstellen[17] anbietet, mit denen dies möglich wäre. Ein weiteres Problem kann sich ergeben, wenn der Provider insolvent wird und der Cloud Service nicht mehr verfügbar ist aber die Firmendaten noch auf den Servern des CSP liegen, deshalb sollte, wenn möglich, vorab vertraglich festgehalten werden, wie mit den Firmendaten verfahren wird, falls der CSP insolvent wird, um sicher zu gehen, dass man als Nutzer nicht von seinen Daten „abgeschnitten" wird. Allgemein betrachtet, ist es ein großer Nachteil des Cloud Computing, dass man als Nutzer, vom Prinzip der Cloud her, keinen direkten administrativen Zugang zu seinen Daten hat (Serverstandort), da nur der Cloud Service Provider Zugang zu Hard- und Software besitzt.

2.2.2.3. Datenschutz

Viele Unternehmen haben Bedenken sensible Firmendaten in die Cloud auszulagern, denn besonders personenbezogene Daten sind, laut BDSG[18], explizit zu schützen (Siehe Kapitel 5). Wobei hier die Verantwortung für die Daten beim Nutzer des Cloud Services liegt und nicht beim Anbieter, deswegen sollte man sich vor Vertragsabschluss sehr genau über den Datenschutz beim CSP erkundigen. Es kann nicht ausgeschlossen werden, dass der CSP das Nutzungsverhalten der Kunden protokolliert, z.B. für die Abrechnung (Pay-Per-Use) des Services, was zu einem Problem werden kann, wenn der Provider diese Daten zu eigenen Zwecken nutzt und diese an Dritte wie z.B. Werbeunternehmen weitergibt. Insbesondere bei Speicherung der Daten in den USA und in anderen Ländern, mit nach deutschem Recht unzureichenden Datenschutzvorkehrungen, hat der Nutzer wenig Möglichkeiten gegen einen solchen Verstoß der deutschen Datenschutzbestimmungen vorzugehen.

2.2.2.4. Sicherheit

Zwar hat ein Cloud Service Provider, der ein professionelles und effizientes Unternehmen führt, mehr Möglichkeiten sein System vor Viren oder Angriffen von außen (z.B. Datenklau oder DDoS-Angriffe), aber ist deswegen vielleicht auch anfälliger für solche Angriffe, da die Angreifer davon ausgehen das bei größeren Provider, mit viel mehr Servern, mehr geeignete Daten zu finden sind als in Kleinunternehmen mit firmeneigenen Servern, auch wenn es für sie mehr Aufwand bedeuten würde. Unbedingt sollten vor Vertragsabschluss die Sicherheitsmaßnahmen des Providers analysiert und vertraglich festgehalten werden, dass der CSP diese Maßnahmen aktuell hält und Sicherheitsgefahren vorbeugt. Außerdem sollte beim Provider ein effektives Verschlüsselungssystem der Daten und der Kommunikation,

[17] http://www.tecchannel.de/server/cloud_computing/2039576/offene_standards_und_schnittstellen_fuer_-die_cloud/

[18] http://www.gesetze-im-internet.de/bdsg_1990/

vorhanden sein (z.B. AES 256-bit Verschlüsselung[19], SSH[20] (Secure Shell), VPN[21] (Virtual Private Network)).

2.2.3. Konklusion

Bevor man sich für Cloud Computing entscheidet, sollte man sich genau überlegen welche Daten man in die Cloud auslagern möchte und die Anbieterauswahl sollte sehr genau und zielorientiert sein, das heißt, dass die Firmendaten, die in der Cloud gespeichert werden, möglichst sicher vor Missbrauch und Verlust sind. Denn wenn zwar auf der einen Seite durch die Cloud Services Kosten eingespart wurden aber auf der anderen Seite sensible Daten gefährdet wurden, bringt dies dem Unternehmen am Ende keinen Gewinn, was durchaus abschreckend für manche Firmen ist. Geht man aber nach Prognosen (siehe Abb. 2.6) so nimmt der Umsatz mit Cloud Computing auch in Deutschland immer mehr zu, sowohl im Geschäfts- als auch im Privatbereich. Was darauf schließen lässt, dass immer mehr Firmen Ihr Vertrauen in die Cloud setzen.

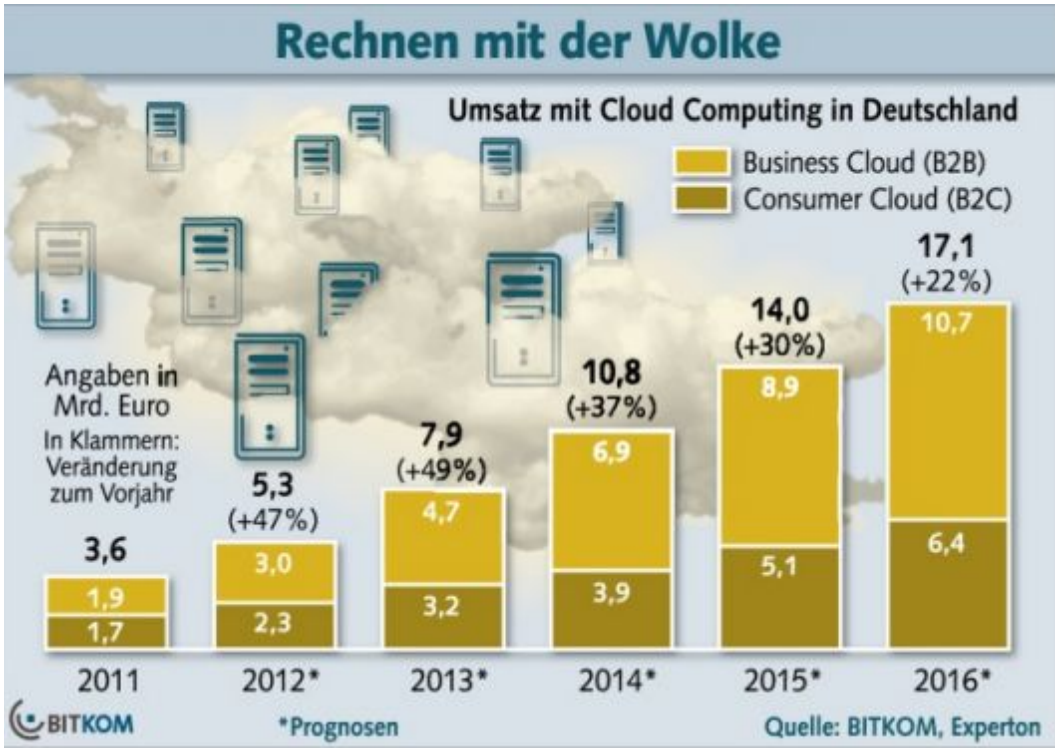


Abbildung 2.6.: Prognose der Umsatzentwicklung von Cloudprodukten

[19]http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[20]http://www.itwissen.info/definition/lexikon/secure-shell-SSH-SSH-Protokoll.html
[21]http://www.itwissen.info/definition/lexikon/virtual-private-network-VPN-Virtuelles-privates-Netzwerk.html

2.3. Business Process Management (BPM)

In diesem Abschnitt sollen unter anderem die Grundlagen über Business Process Management und die Möglichkeiten von BPM in der Cloud erläutert werden.

2.3.1. Definition

In der heutigen, besonders in der IT, schnelllebigen Zeit, ist es für Unternehmen unerlässlich schnell und flexibel reagieren und agieren zu können. Um den wirtschaftlichen Erfolg zu steigern, müssen Unternehmen schnell und effizient auf neue Ereignisse eingehen können, sei es um Kundenwünsche erfüllen zu können oder um neue Märkte zu erschließen. Je schneller und besser ein Unternehmen sich diesen Herausforderungen stellen kann, desto größer wird sein Vorsprung vor den Mitbewerbern sein. (H. Fischer, Fleischmann und Obermeier 2006) Eine Möglichkeit diese Flexibilität und Agilität im Unternehmen zu erreichen, ist seine Geschäftsprozesse zu optimieren. Hier setzt das Business Process Management ein. Das Geschäftsprozessmanagement, als Mittel zur prozessorientierten Unternehmensgestaltung, befasst sich mit dem Dokumentieren, Gestalten und Verbessern von Geschäftsprozessen und deren IT-technischer Unterstützung.[22] Die Geschäftsprozess-Dokumentation und -Gestaltung basiert im Allgemeinen auf standardisierten Modellierungssprachen wie z. B. der Ereignisgesteuerten Prozesskette (EPK) oder der Business Process Model and Notation (BPMN[23]). .

2.3.2. BPM-Lifecycle

Um die Arbeitsweise des Business Process Management verständlich zu machen, wird in der Praxis häufig der BPM-Lifecycle benutzt. Dieser 'Lebenszyklus' erklärt die einzelnen Stationen im Ablauf des Geschäftsprozess Management. In Abbildung 2.7. wird dies deutlich. Die einzelnen Phasen des BPM-Lifecycle sind folgendermaßen aufgebaut:

- ◇ Design
- ◇ Modeling
- ◇ Execution
- ◇ Monitoring
- ◇ Optimieren

Die Design-Phase beinhaltet die Identifizierung von existierenden Prozessen, ebenso wie Entwicklung von neuen wertschöpfenden Prozessen. Die identifizierten Prozesse werden

[22] ftp://ftp.informatik.uni-stuttgart.de/pub/library/medoc.ustuttgart_fi/STUD-2451/STUD-2451.pdf
[23] http://www.bpmn.org

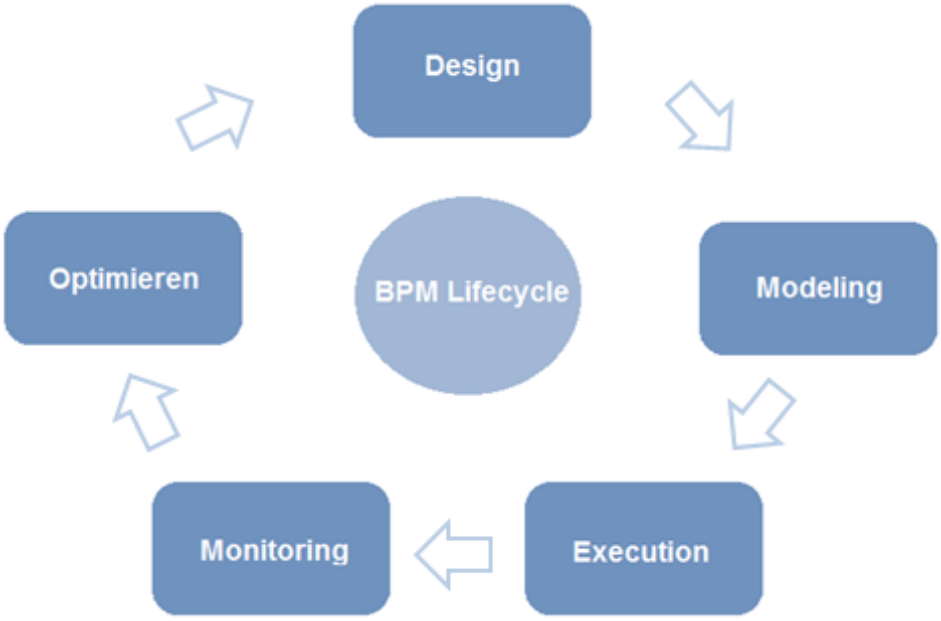


Abbildung 2.7.: Veranschaulichung des BPM-Lifecycle

hinsichtlich Erfolgsfaktoren und Kostentreibern analysiert und deren Anforderungen zur Prozessabwicklung aufgenommen.[24]

In der Modeling-Phase werden die identifizierten Prozesse gestaltet und modelliert, hauptsächlich mit Modellierungstools wie BPMN oder EPK (siehe nächstes Unterkapitel). Hier werden die Prozesse analysiert, modelliert oder angepasst, um z.B. mögliche Konflikte zu entdecken. Dabei fließen die in der Design-Phase evaluierten Daten in die Prozessmodellierung mit ein.

Die Execution-Phase beinhaltet die Implementierung und das Ausführen der modellierten Prozesse. Auch die Automatisierung von Prozessen mittels Workflowmanagementsystemen[25], falls eingesetzt, fällt in diese Phase.

In der Monitoring-Phase werden die Prozesse anhand vorher festgelegter Indikatoren (wie z.B. Effizienz, Kosten) gemessen und überwacht. Anhand dieser Auswertung können dann Durchlaufzeiten und Ressourcenauslastung ermittelt und mit den gewünschten Werten verglichen werden. Mit dem Prozess-Monitoring werden Soll-Ist-Abweichungen analysiert und für das kontinuierliche Geschäftsprozessmanagement zur Verfügung gestellt. Genaue und zeitnahe Informationen sind die wichtigste Voraussetzung für die spätere Optimierung.

In der Optimierungs-Phase werden die gewonnen Erkenntnisse aus dem Monitoring (z.B. Soll-Ist-Abweichung) genutzt um Verbesserungsmaßnahmen und Vorgaben für die Gestal-

[24]http://wwwkrcmar.in.tum.de/lehre%5Clv_materialien.nsf/
[25]http://www.ipd.uni-karlsruhe.de/ ipd/institut/workflow/kap05.pdf

tung der neuen Geschäftsprozesse zu entwickeln. Solche Maßnahmen können u.a. das Verbinden von Prozessen oder die Automatisierung einzelner Teilaufgaben sein. Die Erkenntnisse aus der Optimierung fließen dann wieder in die Design-Phase ein und somit entsteht ein geschlossener Kreislauf.[26]

2.3.3. Modellierungssprachen

Aktuell existieren eine Reihe von verschiedenen Modellierungssprachen für Business Process Management. In diesem Abschnitt werden einige der gängigsten und bekanntesten erläutert. Zur standardisierten Beschreibung von Prozessen werden diese Modellierungsmethoden verwendet, man unterscheidet zwischen graphischen und ausführbaren Modellierungsmethoden, wie z.B. BPMN (graphisch) und BPEL (ausführbar). Beide Methoden werden hier berücksichtigt.

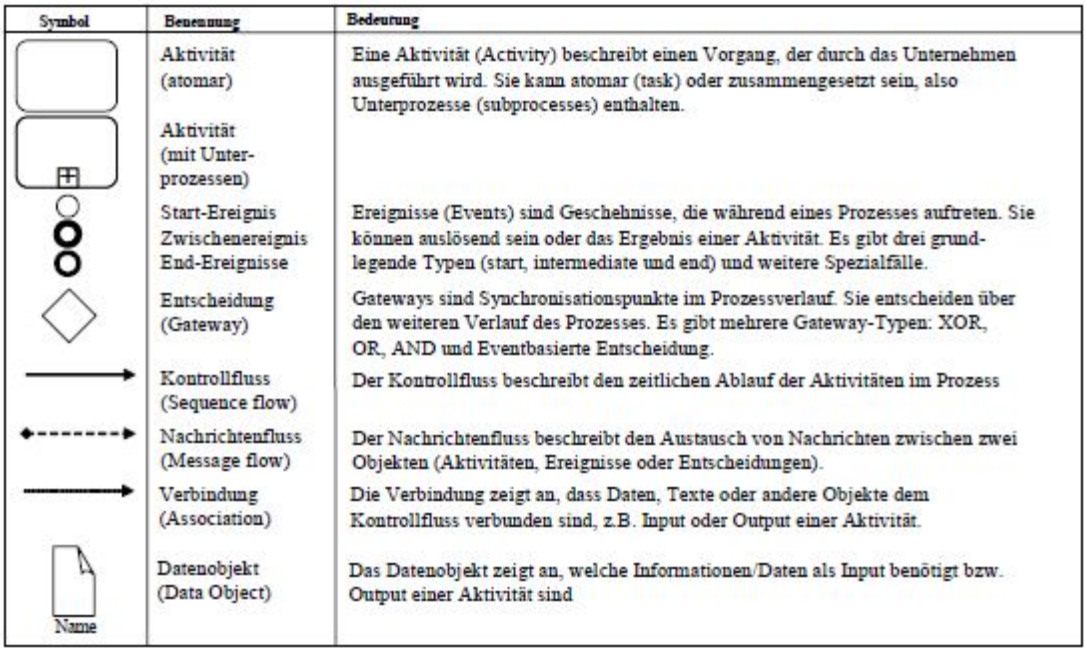
2.3.3.1. BPMN 2.0 - Business Process Model and Notation

Die Business Process Modeling Notation wurde 2001 von Stephen A. White (IBM-Mitarbeiter) zur graphischen Darstellung von Geschäftsprozessen entwickelt und 2004 von der Business Process Management Initiative (BPMI[27]) veröffentlicht. Seit 2006 ist BPMN in der Version 1.0 offiziell ein OMG-Standard (Object Management Group[28]), inzwischen ist die Version BPMN 2.0 ebenfalls verabschiedet worden. Am 15. Juli 2013 ist die BPMN 2.0.1 in der ISO/IEC 19510:2013[29] zum internationalen Standard erhoben worden. Die BPMN ist eine leicht verständliche graphische Modellierungssprache für Geschäftsprozesse aber darüber hinaus ist es ebenfalls möglich, komplexe Geschäftsprozesse darzustellen. Sie richtet sich an alle Beteiligten im Prozessmanagement, also Mitarbeiter der Fachabteilung, Modellierer und Entwickler. (Gadatsch 2008) Die wesentlichen Symbole sind in Abb. 2.8. dargestellt.

- ◇ Rechtecke sind Aktivitäten (Aufgaben)
- ◇ Kreise beschreiben verschiedene Ereignistypen (Nachrichten, Timer, Blanko)
- ◇ Rauten entsprechen Entscheidungen bzw. Gateways (paralleles, inklusives, exklusives Gateway)
- ◇ Pfeile bezeichnen den Kontroll- und Nachrichtenfluss
- ◇ Pentagon bezeichnet Konversationen

Im Kern besteht die BPMN aus Geschäftsprozessdiagrammen, welche jeweils einen oder mehrere Gesamtprozesse abbilden und die verschiedenen Modellierungselemente beinhalten.

[26] http://www.manager-wiki.com/unternehmensanalyse/84-business-process-management-bpm#Lifecycle
[27] http://www.bpmi.org
[28] http://www.omg.org
[29] http://www.iso.org/iso/catalogue_detail.htm?csnumber=62652



Symbol	Benennung	Bedeutung
	Aktivität (atomar)	Eine Aktivität (Activity) beschreibt einen Vorgang, der durch das Unternehmen ausgeführt wird. Sie kann atomar (task) oder zusammengesetzt sein, also Unterprozesse (subprocesses) enthalten.
	Aktivität (mit Unter-prozessen)	
	Start-Ereignis Zwischenereignis End-Ereignisse	Ereignisse (Events) sind Geschehnisse, die während eines Prozesses auftreten. Sie können auslösend sein oder das Ergebnis einer Aktivität. Es gibt drei grund-legende Typen (start, intermediate und end) und weitere Spezialfälle.
	Entscheidung (Gateway)	Gateways sind Synchronisationspunkte im Prozessverlauf. Sie entscheiden über den weiteren Verlauf des Prozesses. Es gibt mehrere Gateway-Typen: XOR, OR, AND und Eventbasierte Entscheidung.
	Kontrollfluss (Sequence flow)	Der Kontrollfluss beschreibt den zeitlichen Ablauf der Aktivitäten im Prozess
	Nachrichtenfluss (Message flow)	Der Nachrichtenfluss beschreibt den Austausch von Nachrichten zwischen zwei Objekten (Aktivitäten, Ereignisse oder Entscheidungen).
	Verbindung (Association)	Die Verbindung zeigt an, dass Daten, Texte oder andere Objekte dem Kontrollfluss verbunden sind, z.B. Input oder Output einer Aktivität.
Name	Datenobjekt (Data Object)	Das Datenobjekt zeigt an, welche Informationen/Daten als Input benötigt bzw. Output einer Aktivität sind

Abbildung 2.8.: einige verfügbare Symbole in BPMN 2.0 (Gadatsch 2008)

Diese Elemente sind in vier unterschiedliche Klassen unterteilt worden, welche jeweils einen spezifischen Teil der Prozessinformationen abbilden können. Hierzu gehören die Klasse der Ablaufelemente, der Verbindungselemente, der Swimlanes und der Artefakte. (H. Fischer, Fleischmann und Obermeier 2006) Mit Hilfe der Swimlanes lässt sich der Geschäftsprozess in Verantwortlichkeitsbereiche gliedern. Dafür stehen zwei unterschiedliche Elemente, Pool und Lane zur Verfügung. Pools repräsentieren in der Regel ein Unternehmen oder eine unabhängige Einheit mit einem eigenen Prozess, der mit den Geschäftsprozessen anderer Unternehmen oder unabhängiger Einheiten interagiert. Mit diesen Werkzeugen lassen sich intuitiv Geschäftsprozesse erstellen. Die Modellierung kleiner Prozesse ist bereits nach kurzer Zeit und meist auch ohne Schulungsaufwand für die Mitarbeiter möglich. Gerade in kleinen bis mittelständischen Unternehmen bringt dies enorme Vorteile. Für große Unternehmen und komplexe Prozesse bedarf es natürlich einen höheren Schulungsaufwand um die Geschäftsprozesse effizient modellieren zu können.

2.3.3.2. EPK - Ereignisgesteuerte Prozess Kette

Die Ereignisgesteuerte Prozesskette (EPK) ist eine grafische Modellierungssprache zur Darstellung von Geschäftsprozessen, sie wurde 1992 von einer Arbeitsgruppe unter Leitung von August-Wilhelm Scheer an der Universität des Saarlandes in Saarbrücken im Rahmen eines

Forschungsprojektes mit der SAP AG[30] zur semiformalen Beschreibung von Geschäftsprozessen entwickelt. (A. W. Scheer 2002) Sie wurde aufbauend auf Petri-Netzen entwickelt, jedoch nach und nach um neue Symbole und Semantik erweitert, so dass sie heute als erweiterte Ereignisgesteuerte Prozessketten (eEPK) verwendet wird, auch wenn der Begriff „EPK " heute synonym zu „eEPK" steht. (H. Fischer, Fleischmann und Obermeier 2006) Die Modellierung des Kontrollflusses erfolgt nachrichtengesteuert mit Ereignissen zwischen den Objekten. Da innerhalb des Prozesses Entscheidungen auf Basis von Bedingungen und Regeln getroffen werden, gibt es in der EPK Verknüpfungsoperatoren („und", „oder", „exklusiv-oder"). Das Grundmodell der Ereignisgesteuerten Prozesskette umfasst neben diesen Operatoren auch Ereignisse und Funktionen. Die wesentlichen sind in Abb. 2.9. dargestellt.

Symbol	Benennung	Bedeutung
	Objektklasse	Betriebswirtschaftliche Leistung (Geschäftsobjekt), die zur Bearbeitung relevante Funktionen (Methoden) und Daten (Instanzvariablen) kapselt
	Ereignis/Nachricht	Beschreibung eines eingetretenen Zustandes, von dem der weitere Verlauf des Prozesses abhängt
	Methode/Funktion	Funktion (Methode) eines Objektes zur Manipulation von Daten (Instanzvariable). Private Methoden sind im Gegensatz zu öffentlichen Methoden außerhalb des Objektes nicht sichtbar
	Instanzvariable/Attribut	Daten (Instanzvariable) die durch Methoden eines Objektes manipuliert werden
	Organisatorische Einheit	Beschreibung der Gliederungsstruktur eines Unternehmens
	Konnektor	Logische Verknüpfungsoperatoren der EPK-Methode (AND, OR, XOR) beschreiben die logische Verknüpfung von Geschäftsobjekten und Ereignissen
	Kontrollfluss	Zeitlich-logischer Zusammenhang von Ereignissen und Geschäftsobjekten
	Auftrags-/Leistungs-beziehung	Ereignisgesteuerter Nachrichtenaustausch zwischen Geschäftsobjekten
	Kante	Zuordnung von Methoden, Instanz-variablen und organisatorischen Einheiten zu Objekten

Abbildung 2.9.: einige verfügbare Symbole der EPK (Gadatsch 2008)

Durch das Aneinanderreihen von Funktionen und Ereignissen lassen sich komplexe Abläufe bilden, die zusammengenommen die Abfolge der Funktionen zur Bearbeitung eines betriebswirtschaftlichen Objektes darstellen. Die EPK ist in Deutschland weit verbreitet und bietet eine intuitive Möglichkeit, Prozesse zu modellieren, allerdings ist die EPK kein Standard wie die Business Process Model and Notation (BPMN).

[30]http://www.sap.com

2.3.3.3. BPEL - Business Process Execution Language

Im Gegensatz zu den beiden vorher betrachteten Modelliersprachen (BPMN und EPK) die auf die graphische Modellierung ausgelegt sind, liegt der Schwerpunkt der Business Process Execution Language auf der Ausführung der Prozesse. Sie basiert auf XML[31] zur Beschreibung von Geschäftsprozessen, deren einzelne Aktivitäten durch Webservices[32] implementiert sind, deswegen wird sie häufig auch WS-BPEL[33] genannt und ist ein industrieller Standard von OASIS[34].

Wie bereits vorher erwähnt, ist BPEL eine XML-basierte Sprache und somit ist sie für Business Analysten und Manager, die eigentlichen Architekten der Geschäftsprozesse, schwieriger in der Handhabung und dazu weniger intuitiv, als z.B. BPMN.

In BPEL wird ein Prozess durch mehrere Eigenschaften eindeutig definiert:

- ◇ Aktivitäten, die verschiedene Dienste im Unternehmen darstellen
- ◇ Kontrollflüsse, um Daten zwischen verschiedenen Diensten übermitteln zu können
- ◇ Vordefinition der Struktur von notwendigen Nachrichten

Aus den Definitionen wird ein ausführbarer Prozess gebildet, außerdem wird definiert, mit welchen Ereignis oder Ereignissen der Workflow gestartet wird. Bei der Ausführung wird eine Instanz des Prozesses erzeugt und Definitionen mit konkreten Daten gefüllt. Der <*process*>-Container ist das äußerste Konstrukt im BPEL-Dokument. Neben den auszuführenden Aktivitäten werden hier Variablen deklariert, Links zu externen Partnern definiert und einige andere Steuerungsfunktionen festgelegt.[35] Anschließend folgt das Unterelement <*sequence*>, das die Definition einer Reihenfolge für den Aufruf von Diensten angibt. Das Unterelement <*invoke*> gibt an, dass ein anderer Web Service aufgerufen werden soll und enthält unter anderem die Attribute *partnerLink, portType, operation, inputVariable*. Mit <*partnerLink*> werden alle verknüpften Dienste mit deren Eigenschaften aufgelistet. Das Attribut *portType* spezifiziert die Anwendungsformen der Operation und *inputVariable* gibt die zur Speicherung im Prozess benötigten Daten an. Mit dem XML-Element <*receive*>wird auf die Antwort eines anderen Web Services gewartet. Der tatsächliche Inhalt eines BPEL-Dokuments ist wesentlich umfangreicher, da sämtliche Informationen für die Steuerung des Geschäftsprozess dort enthalten sind.[36]

Beispielcode:

[31] http://www.w3.org/XML
[32] http://www.w3.org/TR/ws-arch/
[33] http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html
[34] https://www.oasis-open.org/
[35] http://www.informatik.uni-jena.de/dbis/lehre/ss2009/bpmsem/03_arbeit.pdf
[36] http://www.itransparent.de/kompetenzen/bpm-business-process-management

Listing 2.1 Beispielprozess in BPEL

```
<process name =" ProcessName ">
<extensions > ... </extensions >
<import >
<partnerLinks > ... </partnerLinks >
<messageExchanges > ... </messageExchanges >
<variables > ... </variables >
<correlationSets > ... </correlationSets >
<faultHandlers > ... </faultHandlers >
<eventHandlers > ... </eventHandlers >

<! -- ... 1 to N activities -->

</process>
```

BPEL selbst beinhaltet keine graphische Darstellung der modellierten Prozesse, allerdings ist es möglich hierfür die Business Process Model and Notation zu verwenden die eine Beschreibung von BPMN nach BPEL enthält.[37] Allerdings lassen sich nicht alle mit BPMN modellierten Prozesse zu BPEL transformieren, z.B. ein unstrukturierter Loop lässt sich nicht direkt mit WS-BPEL darstellen. Abb. 2.10. stellt eine mögliche Transformation von BPMN zu BPEL dar.

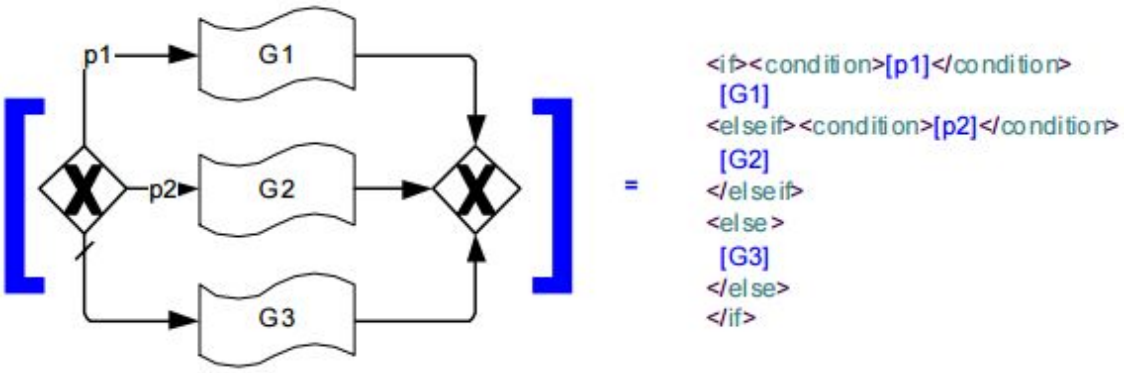


Abbildung 2.10.: Beispieltransformation BPMN zu BPEL (www.omg.org)

2.3.4. BPM in der Cloud

Da Cloud Computing in der IT ein immer wichtigerer Faktor wird - der Anteil der Unternehmen die Clouddienste nutzen ist im Laufe des Jahres 2013 auf 40% gestiegen[38] - gibt es

[37] http://www.omg.org/spec/BPMN/2.0/PDF/
[38] http://www.bitkom.org/files/documents/Cloud_Monitor_2014_KPMG_Bitkom_Research.pdf

inzwischen auch Anbieter für Business Process Management in der Cloud. Doch wie sieht eine Kollaboration von BPM und Cloud Computing aus? Durch die Hinzunahme des Cloud Computing entsteht für das Business Process Management ein größerer Wirkungsbereich. Insbesondere klein- und mittelständische Unternehmen oder auch Start-ups können hiervon profitieren. Denn durch BPM in der Cloud sind keine großen Investitionen in die eigene IT-Infrastruktur nötig, ebenso besteht die Möglichkeit für Pay-Per-Use.

Ein weiterer Vorteil Business Process Management in der Cloud zu nutzen, liegt in der Zusammenarbeit und Flexibilität. Durch die Nutzung der Cloud ist eine Kollaboration der Mitarbeiter möglich - unabhängig von deren Standort. Mehrere Beteiligte können somit gleichzeitig an einer Modellierung arbeiten auch wenn sie sich nicht am selben Standort befinden. Zudem unterscheidet sich die On-Demand Nutzend nur wenig von der On-Premise Nutzung. Die cloud-basierte Nutzung wird häufig über den Internetbrowser abgewickelt und unterliegt somit natürlich den Bedingungen einer guten Internetanbindung.

Was Unternehmen von der Nutzung der Cloud immer noch abschreckt, ist der Schutz von sensiblen Daten, die -aus der Hand- in die Cloud ausgelagert werden sollen. Durchaus sind diese Bedenken berechtigt, vor allem wenn es sich um Cloudbetreiber handelt, die außerhalb von Europa sitzen. Da spielt insbesondere der Schutz von personenbezogenen Daten im Zusammenhang mit dem deutschen Bundesdatenschutzgesetz eine große Rolle (Näheres hierzu in Kapitel 5).

In Kapitel 4 werden verschiedene BPMaaS-Anbieter aufgelistet und anhand ausgewählter Punkte aus dem Kriterienkatalog auf Ihre Funktionalität und Sicherheitsbestimmungen überprüft und analysiert. Ziel soll es sein, aufzuzeigen, welcher Anbieter als sicher eingestuft werden kann - in Bezug auf Datenschutz und Datensicherheit. Einige Anbieter die untersucht werden sind:

- Microsoft Dynamics - Windows Azure[39]
- IBM Business Process Manager on Cloud[40]
- iGrafx Cloud[41]
- Cloud BPM Adonis[42]
- Fabasoft Cloud[43]
- PICTURE[44]

[39]http://www.microsoft.com/de-de/dynamics/default.aspx
[40]http://www-03.ibm.com/software/products/de/business-process-manager-cloud
[41]http://www.igrafx.com/de/products/igrafx-cloud
[42]http://www.boc-group.com/de/adoniscloud/adoniscloud-landingpage/
[43]https://www.fabasoft.com/cloud/de-de/
[44]http://www.picture-gmbh.de/

Kapitel 3.

Kriterienkatalog

In diesem Abschnitt soll der Kriterienkatalog erklärt und dessen Aufbau analysiert werden. Im Anhang ist der gesamte Kriterienkatalog zu finden.

3.1. Einleitung

Cloud Computing wird in der heutigen Zeit und der rasanten Entwicklung in der IT immer wichtiger und profitabler. Allerdings ist derjenige, der seine Daten über das Internet austauscht bzw. auf fremden Servern speichert, auch großen Sicherheitsrisiken (Datenverlust, Datenklau) ausgesetzt. Aus diesem Grund soll hier ein Kriterienkatalog entstehen, an dem sich Firmen orientieren können, welche Punkte ein Cloud Computing Service erfüllen sollte um größtmögliche Sicherheit, in Bezug auf sensible Firmendaten, zu bieten.

Die Idee eines Kriterienkataloges für Cloudnutzer entstand durch einige Gespräche mit klein- und mittelständischen Unternehmen im Rahmen meiner Studienarbeit "Situationsanalyse: BPM in Deutschland"[1]. Es zeigte sich, dass viele Firmen, vor allem Kleinunternehmen, die keine eigene IT haben, zwar gerne die Cloud nutzen würden, aber selbst zu wenig Hintergrundwissen besitzen um dieses sicher und effizient zu vollziehen. Mit diesem Hintergrund wurde in dieser Diplomarbeit ein Kriterienkatalog entwickelt, anhand dessen sich Firmen orientieren können, was ein Cloudprovider mindestens leisten muss, um bei diesen sensible Daten sicher in die Cloud auslagern zu können.

Es soll eine Möglichkeit entstehen, schnell und einfach abklären zu können ob ein Cloud Service, wie bzw. SaaS, den eigenen und den empfohlenen Sicherheitsansprüchen für sensible Firmendaten entspricht oder nicht. Besonders personenbezogene Daten müssen laut Bundesdatenschutzgesetz explizit vor Missbrauch geschützt werden. Da der Nutzer der Cloud Services vollständig für die Personenbezogenen Daten verantwortlich ist, also auch für deren Schutz (siehe auch Kapitel 5), ist es unerlässlich sich vorher genau über die möglichen Cloud Service Provider (CSP) zu informieren. In Anlehnung an das Eckpunktepapier des BSI[2], welches sich an Cloud Service Provider richtet, soll sich der Kriterienkatalog an Cloud

[1] ftp://ftp.informatik.uni-stuttgart.de/pub/library/medoc.ustuttgart_fi/STUD-2451/STUD-2451.pdf
[2] https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html

Service Nutzer richten und eine Hilfestellung bieten, um einen sicheren und optimalen Cloud Service Provider zu finden.

3.1.1. Definition

Der Kriterien Katalog setzt sich aus 8 Unterthemen zusammen.

- **Security:** z.B. Firewall, Verschlüsselung, Datensicherheit
- **Performanz:** z.B. Latenzzeiten, Skalierungsmöglichkeiten
- **Verfügbarkeit:** z.B. Backup, Hochverfügbarkeit
- **Funktionalität:** z.B. Kundenanpassungen, Mandantentrennung, Kombinierbarkeit
- **Wartbarkeit:** z.B. Testumgebungen, Fehlerbehebung, Support
- **Compliance:** z.B. Datenschutz (BDSG), SLA, Serverstandort
- **Vertrag:** z.B. Vertragslaufzeit, Haftung, vertragliche Regelungen
- **Kosten:** z.B. Abrechnungsmodelle, Limitierung, Zusatzkosten

Kriterienkatalog	*Ja*	*Nein*	*Bemerkungen*
Security			
Verfügt der Provider über ein ausgereiftes IT-Sicherheitskonzept? (z.B. Schutz vor Malware, Abwehr von DDoS-Angriffen)	X		
Existiert ein Intrusion Detection System - IDS (Angrifferkennungssystem) zur Überwachung der IT-Infrastruktur?	X		
Werden interne Angriffe (d.h. von Kunden auf Kunden) verhindert bzw. entdeckt und effektiv untersucht und unterbunden?	X		
Sicherheitsmaßnahmen sind up-to-date	X		
Authentifizierung ist suffizient: • autorisierte Personen haben Zugang • unautorisierte Personen haben keinen Zugang	X		

Abbildung 3.1.: Auszug aus dem Kriterienkatalog

3.2. Aufbau des Katalogs

Die Sicherheit im Cloud Computing ist ein wichtiges und umfangreiches Themengebiet, aus diesem Grund wurde der Kriterienkatalog in 5 Unterkategorien aufgeteilt um einen besseren Überblick zu haben. Hier werden die einzelnen Kategorien näher erläutert und deren Auswahl gerechtfertigt.

3.2.1. Security

Die Kategorie Security des Katalogs stellt in dieser Diplomarbeit die wichtigste Kategorie von allen dar. In welcher Hinsicht auch immer, die Sicherheit in der IT, insbesondere im Datenschutz, sollte immer eine große Rolle spielen. Denn wenn sensible Daten nicht vor Angriffen geschützt sind und bzw. in fremde Hände geraten, ergeben sich für die betroffenen Firmen oft existenzielle Probleme. Um dieses vorzubeugen sollte bei der Wahl des CSP auf folgendes geachtet werden: Es sollte sichergestellt sein, dass der CSP umfangreiche Maßnahmen gegen Malware, Viren und Trojaner ergriffen hat und diese auch aktuell hält. Ebenso ist eine verschlüsselte Kommunikation via SSL (Secure Sockets Layer)/ TLS (Transport Layer Security) oder VPN unerlässlich. Im Kriterienkatalog sind im Bereich Security 30 Unterpunkte aufgelistet anhand denen die Cloud Service Nutzer erkennen können ob ein CSP den empfohlenen Sicherheitsaspekten entspricht. Diese Punkte könnten bzw. bei einem Beratungsgespräch zwischen Nutzer und Provider angesprochen werden.

3.2.2. Verfügbarkeit

Die Kategorie Verfügbarkeit beinhaltet die verschiedenen Möglichkeiten die ein CSP anbietet um den angebotenen Service resistent gegen Ausfälle zu machen. In der heutigen Zeit ist es sehr wichtig das Informationen schnell und effizient nutzbar sind. Die Hochverfügbarkeit ist in der IT- Branche, sowie auch im Cloud Computing, ein bedeutender Aspekt. Denn wenn z.B. ein Onlineshop wie Amazon nur für kurze Zeit nicht erreichbar ist, bedeutet dies für den Onlinehändler einen immensen Umsatzverlust. Somit ist es sinnvoll, sich als Nutzer vom CSP diverse Maßnahmen bestätigen zulassen, die die Verfügbarkeit des Services unterstützen.

3.2.3. Funktionalität

Die Kategorie Funktionalität bezieht sich auf die vorhandenen Funktionen und Anpassungsmöglichkeiten des Service. Man sollte als Nutzer darauf achten, dass die angebotenen Services vom CSP, sich auch an die eigenen Wünsche und Anforderungen anpassen lassen, damit ein stabiler und effizienter Betriebsablauf möglich ist. Ebenso ist es wichtig, dass der CSP eine strikte Mandantentrennung in der Cloud durchführt, um sicherzustellen, dass nur autorisierte Personen an die eigenen Firmendaten gelangen.

3.2.4. Compliance

Die Kategorie Compliance beinhaltet Einhaltung von Gesetzen und Richtlinien auf der Seite des CSP. Es ist unerlässlich, dass der CSP sich an den Datenschutz des Bundesdatenschutzgesetzes hält, insbesondere hinsichtlich auf personenbezogene Daten.[3] Ebenso sollte der CSP eine verbindliche Auskunft über den Serverstandort bzw. das Land in dem die Kundendaten gespeichert werden, geben, da außerhalb der EU andere Datenschutzgesetze gelten (siehe auch Kapitel 5). Vorteilhaft wäre es, wenn die Inhalte bezüglich der Compliance in Service Level Agreements (SLA) schriftlich festgehalten und in den Vertrag zwischen Nutzer und CSP aufgenommen werden.

3.2.5. Vertrag

Die Kategorie Vertrag bezieht sich hauptsächlich auf die Gestaltung und die Inhalte des Vertrages. Als Nutzer sollte man darauf achten, dass der Vertrag eindeutig formuliert ist, d.h. das z.B. der Serverstandort genau angegeben ist. Ebenfalls sollte klar geregelt sein, wie mit den Firmendaten nach Vertragsende umgegangen wird. Es ist wichtig, dass diese nach Ende des Vertrages vom CSP vollständig gelöscht werden. Auch die Kündigungsrechte bzw. die Mindestlaufzeit und die Haftung sollten vorher mit dem CSP besprochen und vertraglich festgehalten werden, damit z.B. bei einem Anbieterwechsel keine Probleme mit dem vorherigen CSP auftreten. Ebenso sollten die Kosten vertraglich geregelt sein, es ist wichtig, dass der Nutzer sich vor Vertragsabschluss informiert welche Bezahlungsmodelle der CSP anbietet, z.B. Pay-Per-Use d.h. der Nutzer bezahlt genau das was er auch verbraucht. Ebenfalls sollte man mit dem CSP abklären ob zusätzliche Kosten für bestimmte Services entstehen können (z.B. für Datenlöschung)

3.2.6. Gesamtstruktur

In der Gesamtheit soll der Kriterienkatalog die Sicherheitsrisiken beim Cloud Computing aufführen bzw. minimieren und die Funktionalitäten die ein Cloud Service zur Verfügung stellen sollte, der als sicher eingestuft werden kann, auflisten. Es soll eine Checkliste entstehen, die es dem Cloud Service Nutzer ermöglicht zu entscheiden, welchen Cloud Service Provider er für seine Firmendaten auswählt.

[3] http://www.gesetze-im-internet.de/bdsg_1990/__4b.html

3.3. Umfrage

3.3.1. Erhebungsmethoden

Zur Datenerhebung wurde zwischen dem 05.02.2015 und dem 07.04.2015 eine Online-Umfrage durchgeführt. Die potentiellen Teilnehmer wurden per Email, durch Forenbeiträgen in verschiedenen Fachgruppen (bzw. auf Xing[4]) und persönlich auf Messen (bzw. Cebit[5]) auf die Befragung aufmerksam gemacht bzw. kontaktiert. Insgesamt wurden 41 Unternehmen per Email angeschrieben. Die Zielgruppe bestand in erster Linie aus Unternehmen die BPM in der Cloud (z.B. BPMaaS) in ihrem Portfolio hatten. Der Zweck dieser Umfrage bestand darin, herauszufinden, wie hoch der Datenschutz und die Funktionalität der Software einzuschätzen ist. Es wurden jeweils 5-8 Fragen zu Themen wie Security, Compliance, Funktionalität, Verfügbarkeit und Vertrag gestellt. Diese Themen wurden aus dem erstellten Kriterienkatalog entnommen und bilden eine Untersektion des Kataloges.

3.3.2. Technik

Die Datenerhebung wurde zumeist anhand einer Nominalskala[6] durchgeführt, bei einigen Fragen waren neben den Einzel- auch Mehrfachantworten gestattet. Da die Umfrage nur an Unternehmen im BPM-Umfeld verteilt wurde, wurde davon ausgegangen, dass die Probanden sich mit dem Thema BPM auskennen und deswegen wurden auch allen Teilnehmern die gleichen Fragen angezeigt.

3.3.3. Literaturrecherche

Für die Planung der Befragung wurde in einem ersten Schritt eine umfassende Literaturrecherche durchgeführt. Schon hierbei und der Erarbeitung der Umfrage wurde versucht, die verschiedenen Themen wie Datenschutz und Funktionalität von BPM in der Cloud, zu erörtern. Als Quellen dienten diverse Studien[7] zu Cloud Computing im Allgemeinen, sowie generelle Fachliteratur, die insbesondere Cloud Computing und BPM als Schwerpunkt hatten.

[4]http://www.xing.com
[5]http://www.cebit.de
[6]http://de.statista.com/statistik/lexikon/definition/94/nominalskala/
[7]https://www.kpmg.com/DE/de/Documents/Cloud-Monitor-2013-KPMG-version-2.pdf

3.3.4. Verifikation

Die Umfrage wurde mit Soscisurvey[8] erstellt und bearbeitet. Sie wurde vollständig anonym durchgeführt, d.h. es wurden keine personalisierten Links benutzt oder die IP-Adressen der Teilnehmer abgefragt.

3.3.5. Statistik

Da sich die Umfrage nur auf Unternehmen bezog, die BPM in der Cloud anbieten, war der Radius der Personen/Unternehmen, die passend für die Umfrage waren, geringer (18 Teilnahmen, 8 vollständig und verwertbar) als bei diversen anderen Umfragen zum Thema Cloud Computing, da Geschäftsprozessmanagement On-Demand noch eine Thematik ist, die am Anfang ihrer Entwicklung steht. Durch diese Umfrage konnten 6 Anbieter von BPM in der Cloud und deren Softwareprodukte, ausführlich analysiert und beurteilt werden, im Hinblick auf Datensicherheit und -schutz von personenbezogenen Daten. Allerdings erweist sich die statistische Auswertung von Umfragen nur dann als sinnvoll und repräsentativ, wenn eine ausreichend große Anzahl von Personen daran teilgenommen haben (Untergrenze 30 Teilnehmer)[9]. In diesem Fall, kann man diese Umfrage eher als ein Interview sehen, bei dem die Anbieter Antworten zu ihrem Softwareprodukt abgegeben haben, da der Hauptaugenmerk der Umfrage darin bestand, möglichst viele und ausführliche Informationen zu einem Softwareprodukt zu bekommen.

3.3.6. Aktuelle Forschung

Cloud Computing hat im Allgemeinen einen schweren Stand bezüglich dem Datenschutz und dessen Einhaltung, wenn personenbezogene oder sensible Firmendaten in die Cloud ausgelagert werden sollen, wie eine Studie des Fraunhofer Instituts[10] zeigt. Die Sicherheit im Cloud Computing hat sich zwar schon verbessert, aufgrund von besseren Sicherheitsvorkehrungen und neuen Entwicklungen, aber damit die Unternehmen ihre durchaus begründete Skepsis gegenüber dem Schutz ihrer Daten in der Cloud verringern muss noch vieles getan werden.

Bezüglich Business Process Management in der Cloud zeigt eine Umfrage der Züricher Hochschule für Angewandte Wissenschaften, dass BPM in der Cloud, vor allem BPMaaS, noch recht wenig verbreitet ist. Insbesondere Komplettsysteme sind selten in Benutzung, wenn Dienste aus der Cloud angefragt werden, so sind dies im BPM-Umfeld gemäß den befragten Personen, hauptsächlich Business Process as a Service Dienste für Teilprozesse,

[8] https://www.soscisurvey.de
[9] http://www.2ask.de/media/1/10/2/23/25/3b44548aa4f7b046/Leitfaden_Statistik.pdf
[10] http://www.cloud.fraunhofer.de/content/dam/allianzcloud/de/documents/Cloud_Security_-IAOFoliendokumentationtcm421-101225.pdf

welche nicht oder nur sehr wenig mit den bestehenden On-Premise Lösungen verknüpft werden müssen.[11]

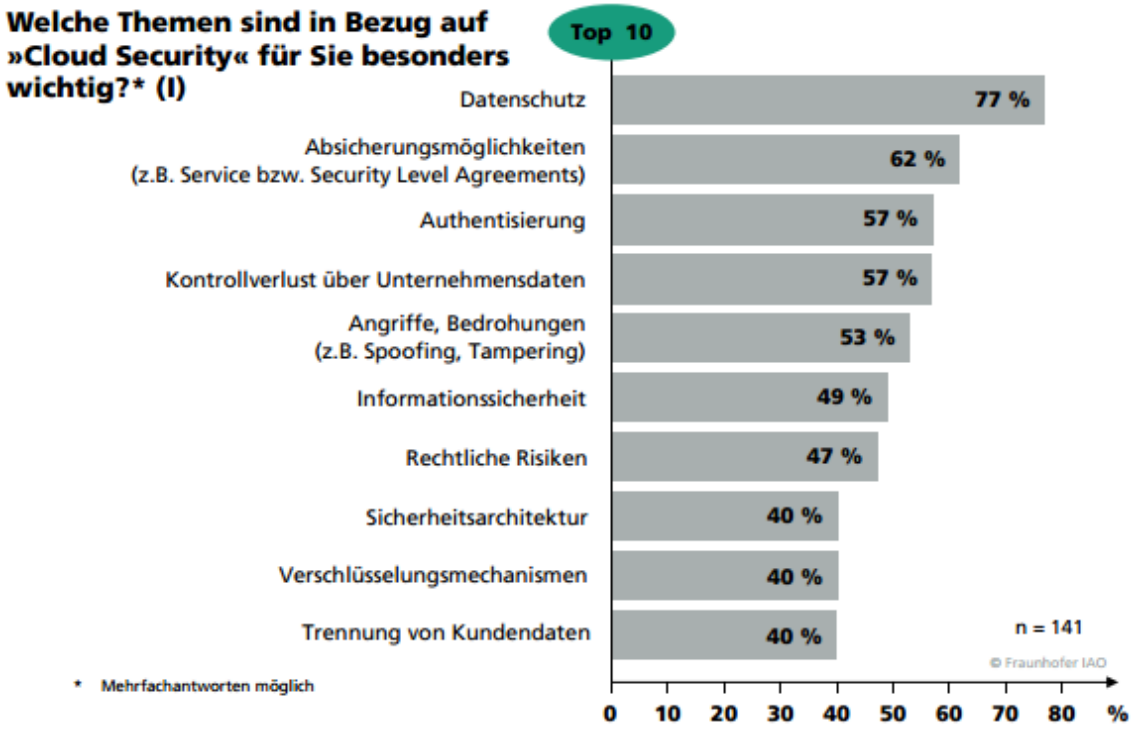


Abbildung 3.2.: Auszug aus der Umfrage des Fraunhofer Instituts

[11]http://www.vdf.ethz.ch/service/3584/3584_BPM-Loesungen-aus-der-Cloud_Leseprobe.pdf

Kapitel 4.

Umfrageauswertung

In diesem Abschnitt wird ein Ausschnitt des Kriterienkatalog auf verschiedene Produkte von Unternehmen angewendet die BPM (Business Process Management) in der Cloud anbieten (BPaaS, BPMaaS), dies basiert auf der auf der Auswertung der Umfrage.

Die Umfrage zu dieser Diplomarbeit lief vom 05.02.2015 bis 07.04.2015. In diesem Zeitraum haben sich 18 Personen an der Umfrage beteiligt, 8 davon haben den Fragenkatalog vollständig ausgefüllt. Es wurden 6 verschiedene Clouddienste angegeben die BPM in der Cloud ermöglichen. Auf dieser Grundlage werden in diesem Kapitel diese Dienste anhand der Fragen aus der Umfrage, die eine Untersektion des Kriterienkataloges darstellen, ausgewertet und analysiert.

Die Auswertung bezieht sich nur auf die Auslagerung von personenbezogenen Daten in eine Public Cloud, d.h. Daten die gesetzlichen Bestimmungen unterliegen (BDSG). Anderweitige Daten, die ohne Konflikt mit dem deutschen Datenschutz outgesourct werden können, sind für diese Analyse nicht relevant.

Für die eigene Recherche wurden die Anbieterinformationen zu den jeweiligen Cloud Services ausführlich untersucht. Hier standen unterschiedliche Möglichkeiten zur Verfügung, unter anderem ABG, SLA, Nutzungsbedingungen, Lizenzverträge, Trust-Bedingungen und Datenschutzrichtlinien der Anbieter.

Folgende BPM-Systeme wurden in der Umfrage genannt:

- 3x Microsoft Dynamics NAV - Azure (die Antworten wurden zusammengefasst)
- IBM - Business Process Manager on Cloud
- iGrafx Cloud
- ADONIS:Cloud
- Fabasoft Cloud
- PICTURE

Im weiteren Verlauf werden die BPM-Systeme einzeln untersucht und die Ergebnisse aus der Umfrage aufgelistet. Anschließend werden die BPM-Systeme auf ihre Sicherheit und Funktionalität hin überprüft und eine Bilanz daraus gezogen, inwiefern die Systeme in Bezug auf Datenschutz und Sicherheit zu empfehlen sind.

4.1. Anwendung des Kriterienkataloges auf die BPM-Systeme

4.1.1. Fabasoft Cloud

Fabasoft ist ein europäischer Softwarehersteller und Cloud-Betreiber mit Sitz in Linz (Österreich)[1]. Die Fabasoft Cloud bietet die modellbasierte Digitalisierung von Geschäftsprozessen nach dem internationalen Standard BPMN 2.0. Sie wird als Public oder Private Cloud angeboten und verfügt über:

- ◇ einen grafischen Prozess-Editor für die einfache Gestaltung, Bearbeitung, Import und Export von kompatiblen Prozessdiagrammen
- ◇ eine integrierte Workflow-Engine zur direkten Ausführung des modellierten Prozesses
- ◇ eine zentrale Verwaltung von Geschäftsprozessen und entsprechende Zugriffsrechte

Im Folgenden werden die Antworten aus der Umfrage bezüglich der Fabasoft Cloud aufgelistet:

Frage	**Antwort**
Allgemein	
Wie lautet der Name der Firma, für die Sie arbeiten?	Keine Angabe
Wie lautet der Name des Produktes, welches Sie bewerten möchten?	Fabasoft Cloud
Wird das Produkt von Ihrer Firma hergestellt oder handelt es sich um einen Drittanbieter?	Drittanbieter
Welche Services werden angeboten?	SaaS, BPMaaS
Security	
Verfügt der Provider über ein ausgereiftes IT-Sicherheitskonzept? (Schutz vor Malware, Abwehr von DDoS-Angriffen)	Ja
Welche Vorkehrungen die ggf. Ausfallzeiten und Datenverlust vorbeugen, stehen zur Verfügung?	Backup, Redundante IT-Infrastruktur, Physikalische Sicherheit (z.B. Notstromversorgung)
Existiert ein Intrusion Detection System (Angriffserkennungssystem) zur Überwachung der IT-Infrastruktur?	Ja

[1] http://www.fabasoft.com

Frage	Antwort
Ist ein effektives Verschlüsselungs- und Schlüsselmanagement vorhanden, um die Kundendaten und den Datenaustausch sicher zu verschlüsseln?	Ja, RSA Sonstiges: Self Encrpyting Disks
Ist ein definiertes Vorgehensmodell der firmeninternen IT-Geschäftsprozesse vorhanden?	Ja, ITIL
Werden regelmäßige und unabhängige Prüfungen des IT-Sicherheitszustands, wie z.B. Penetrations-Tests und Audits, vorgenommen?	Ja, monatlich
Werden interne Angriffe (d.h. von Kunden auf Kunden) verhindert bzw. entdeckt und effektiv untersucht und unterbunden?	Ja
Compliance	
In welchem Land liegt der Serverstandort?	Deutschland Sonstiges; Österreich, Schweiz
Entspricht die Datenspeicherung von personenbezogenen Daten dem Bundesdatenschutzgesetz?	Ja
Sind Compliance-Zertifikate vorhanden? Wenn ja welche?	Ja, ISO 27001/27002 Sonstiges: TÜV Rheinland, ISO 20000-1, ISO 9001
Werden interne Bereiche an Subunternehmer ausgelagert?	Ja, Raum inkl. Kühlung, ausfallsichere Strom & Internet-Anbindungen. Für Deutschland: noris network AG
Werden für Kunden SLA (Service Level Agreements) angeboten?	Ja
Ist es möglich vorhandene SLA (Service Level Agreements) an Kundenwünsche anzupassen?	Ja
Funktionalität	
Ist eine strikte Mandantentrennung in der Cloud vorhanden?	Ja
Können kurzfristig weitere Kapazitäten hinzugefügt und wieder entfernt werden, falls nötig? (Skalierbarkeit)	Ja

Frage	Antwort
Können Daten mit geringem Aufwand exportiert und zu einem anderen Provider migriert werden?	Ja
Können offene Formate für den Datenaustausch verwendet werden?	Ja, XML
Findet dieser Datenaustausch verschlüsselt statt? Wenn ja, wo werden die Daten ver- und entschlüsselt bzw. wo liegt der Schlüssel?	Sonstiges: Secomo - Schlüssel liegt beim Kunden
Kann mittels Single Sign-On auf die Kundenserver zugegriffen werden?	Ja
Gibt es eine 2-Faktor-Authentisierung für die Kunden?	Ja
Falls der Kunde „Managed Services“ bevorzugt, existiert hierfür ein effektives Patch- und Änderungsmanagement vorhanden? (z.B. Updates)	Ja
Verfügbarkeit	
Ist für Download/Upload eine ausreichende und unterbrechungsfreie Internetverbindung gewährleistet? (z.B. geringe Latenzzeiten)	Ja
Stehen dem Kunden Alternativen zur Verfügung, falls der Cloud-Service ausfallen sollte? (z.B. redundante Notfall-Server/Komponenten)	Ja, redundante Notfallserver Sonstiges: Notstromaggregate
Kann bei einer möglichen Insolvenz des Providers der Schutz und die Verfügbarkeit der Daten gewährleistet werden?	Keine Angabe
Ist der Cloud-Service hochverfügbar? (min. 99,9%)	Ja
Existiert ein ausgeprägter und professioneller Kundensupport?	Ja
Vertrag	
Wie wird der Vertrag geschlossen?	online
Wie werden die für den Vertrag benötigten Personendaten der Kunden überprüft?	Personalausweis
Wie sehen die Laufzeiten des Vertrages aus?	Sonstiges: 1-Jahresabo
Besteht bei Vertragskündigung die Möglichkeit die Kundendaten vollständig zu löschen?	Ja
Wie erfolgt die Abrechnung der Services?	pauschal
Kann der Vertrag angepasst werden, wenn sich die Anforderungen des Kunden ändern?	Ja

Tabelle 4.1.: Auswertung der Umfrage - Fabasoft Cloud

4.1.1.1. Eigene Recherche

Die Fabasoft Cloud GmbH ist ein Cloud Service Provider mit Sitz in Österreich und ein 100% Tochterunternehmen der Fabasoft AG, welcher verschiedene Clouddienste wie z.B. SaaS anbietet. Der Serverstandort kann vom Kunden selbst gewählt werden. Es stehen Serverstandorte in Deutschland, Österreich und der Schweiz zur Verfügung (je zwei Rechenzentren mit einer geographischen Distanz von mehreren Kilometern Luftlinie), was in Bezug auf das Bundesdatenschutzgesetz und der innereuropäischen Auftragsdatenverarbeitung ein großer Vorteil ist. Fabasoft stellt die Cloud-Dienste ausnahmslos mit Fabasoft-eigener Wertschöpfung zur Verfügung und betreibt die eigene Cloud-Hardware in Hochleistungsrechenzentren und mietet sich dafür lediglich Raum inklusive Kühlung sowie ausfallsichere Strom- und Internet-Anbindungen (Cloud Lokation Deutschland: noris network AG)

Fabasoft selbst stellt viele Informationen zum Schutz von Kundendaten und Cloudsicherheit zur Verfügung. Unter anderem zu finden sind Leistungsmerkmale zum Rechenzentrumsbetrieb[2]. Der Betrieb der Fabasoft Cloud Services erfolgt je Lokation in zwei Rechenzentren (Rechenzentrum 1 und Rechenzentrum 2) mit einer geographischen Distanz von mehreren Kilometern Luftlinie und einem Backup-Rechenzentrum , welches sich am Standort des Rechenzentrums 1 befindet. Dadurch werden Konzepte ermöglicht, die einen Desastertoleranten Betrieb erlauben, beispielsweise hoher Schutz gegen Elementarereignisse. Die Rechenzentren orientieren sich an der Tier-3-Spezifikation des Uptime Institutes[3]. Die einzelnen sicherheitsrelevanten Punkte werden ausführlich aufgelistet (Mindestmaßnahmen):

- ◇ **Sicherheit:** Elektromagnetisches Zutrittsystem, Personenschleuse, Videoüberwachung, 24x7 Überwachung der Rechenzentrumsflächen
- ◇ **Brandschutz:** Flächendeckende Brandmeldeanlage, Brandfrüherkennung (RAS - Rauchansaugsystem), automatische Gaslöschanlage
- ◇ **Stromversorgung:** Redundante USV-Analgen, Dieselaggregate, Einspeisungen, Transformatoren
- ◇ **Klimatisierung:** Redundante Kälteanlagen
- ◇ **Verbindung zwischen den Rechenzentren je Lokation:** Per Ethernet Point-to-Point Strecken, die Netzwerk-Hardware ist redundant ausgelegt, die Verbindung ist wegredundant ausgeführt, die gebäudeseitigen Einspeisungen erfolgen an jeweils 2 unterschiedlichen Stellen.
- ◇ **Hard- und Software** Softwareprodukte von Dritten, zum Betrieb der Fabasoftprodukte benötigt werden, sind Open-Source-Produkte (keine Abhängigkeit), Hardware-Komponenten z.B. zur Datensicherung befinden sich in Deutschland in einem eigen Brandabschnitt in je einem der Rechenzentren

Folgende Service Levels sind bei Fabasoft Cloud zu finden:

[2]https://at.cloud.fabasoft.com/folio/public/26m268fc1ttsd3mdtjoxrzhm7v
[3]https://uptimeinstitute.com/TierCertification/allCertifications.php?page=1&ipp=All

- ◇ **Hochverfügbarkeit:** Rechenzentrumsbetrieb erfolgt 7x24 Stunden pro Woche, 52 Wochen pro Jahr. Pro Fabasoft Cloud Lokation und Service ist eine Verfügbarkeit von 99,9% pro Beobachtungszeitraum (Quartal) vorgesehen
- ◇ **Antwortzeitverhalten:** Das Antwortzeitverhalten wird mittels Fabasoft app.telemetry gemessen (als Anfrage gilt ein am Lastverteiler eingehender HTTP-, CalDAC- oder WebDAV-Request). Pro Fabasoft Cloud Lokation und Service ist eine durchschnittliche Antwortzeit aller Anfragen von unter 1 Sekunde pro Beobachtungszeitraum (Quartal) vorgesehen
- ◇ **Datensicherheit:** Metadaten und Inhalte werden je Fabasoft Cloud Lokation in beiden Rechenzentren gespeichert. Metadaten in einem relationalen Datenbanksystem (synchron gespiegelt in beide Rechenzentren), Inhalte im Dateisystem parallel auf mehreren Rechnern. Mindestens 1x pro Tag eine Vollsicherung der Metadaten durch Datenbank-Backups auf dedizierte Backupsysteme, 1x täglich vollständige Synchronisation der Inhalte auf Backupsysteme. Folgende Parameter sind im Rahmen der Datensicherheit vorgesehen:
  - Recovery Point Objetive (RPO): Der maximale Zeitraum, für welchen Daten im Falle einer Notfallwiederherstellung verloren gehen, beträgt 30 Minuten.
  - Recovery Time Objective (RTO): Im Falle einer Notfallwiederherstellung beträgt die Zeit für die Wiederherstellung der Services, ab Verfügbarkeit der Netzwerk-, Hardware- und Softwareinfrastruktur, maximal 48 Stunden
  - Retention Time: Jede Sicherung wird für einen Zeitraum von min. 4 bis max. 6 Monaten aufbewahrt
  - Audit Logs: Audit Log Daten werden min. 12 Monate vorgehalten
- ◇ **Support:** Fabasoft bietet einen First-level Support für die Fabasoft Cloud Nutzer. Eine Supportanfrage ist über ein Webinterface bzw. im Fabasoft Cloud Client rund um die Uhr möglich. Alternativ ist der Support via Telefon und Email in den definierten Betriebszeiten zu erreichen. Folgende Reaktionszeiten sind angegeben:
  - Professional: Betriebszeiten Mo-Fr. 8-18Uhr, Reaktionszeit je Anfrage: < 2 Stunden, Lösungszeit je Anfrage: < 8 Stunden
  - Enterprise/Superior[4]: Betriebszeiten Mo-Fr 7-19Uhr, Reaktionszeit je Anfrage: < 1 Stunde, Lösungszeit je Anfrage: < 6 Stunden
- ◇ **Auditing und Sicherheitsüberprüfungen:** Die Fabasoft Cloud wird von unabhängigen Auditoren nach internationalen Standards überprüft. Das beinhaltet:
  - ISO 9001: National und international die meist verbreitete Norm im Qualitätsmanagement (QM), legt die Mindestanforderungen an ein Qualitätsmanagementsystem fest, die von Unternehmen umzusetzen sind, um die Kundenanforderungen

[4]https://www.fabasoft.com/cloud/de-de/preise

sowie weitere Anforderungen an die Produkt- bzw. Dienstleistungsqualität zu erfüllen[5]

- ISO 20000: International anerkannter Standard für IT-Service-Management-Systeme, in dem die Anforderungen für ein professionelles IT-Service-Management dokumentiert sind. Die ISO 20000 dient als messbarer Qualitätsstandard für das IT-Service-Management (ITSM).[6]
- ISO 27001: Weltweit anerkannter Standard für die Bewertung der Sicherheit von Informationen und IT-Umgebungen. Der Standard beschreibt die Anforderungen an die Umsetzung sowie die Dokumentation eines Informationssicherheitsmanagement-Systems (ISMS)[7]
- ISAE 3402 Type 2: Der International Standard on Assurance Engagements (ISAE 3402) ist der internationale Prüfungsstandard, der die Wirksamkeit des internen Kontrollsystems (IKS) von Dienstleistungsorganisationen beurteilt. Der Standard wurde vom American Institute of Certified Public Accountants (AICPA) als Nachfolger des SAS 70 Standard geschaffen[8]
- Certified Cloud Service (Tüv Rheinland): beinhaltet Prüfungen auf sicheres Hosting von Daten, Sichere Datenübertragung, Sicherer Betrieb von unternehmenskritischen Anwendungen, Qualität und Verfügbarkeit der Serviceerbringung (hohe Service-Kontinuität und hohe On-Demand Skalierbarkeit), Sicherheit und Qualität des Datenzugriffs und der Datenspeicherung (sichere Anmeldeverfahren), Schutz vor Angriffen nach dem neuesten Stand der Technik

◇ **Data Portability:** CMIS (Content Management Interoperability Standard), WebDAV (Web-based Distributed Authoring and Versioning - offener Standard zur Bereitstellung von Dateien im Internet) und CalDAV (Standard-Protokoll, dass es ermöglicht, auf Kalenderdateien über WebDAV zuzugreifen und zu synchronisieren) für den Import und den Export von Cloud-Daten. Damit ist es beispielsweise möglich, einen Fabasoft Cloud-Dienst als Netzwerklaufwerk unter Microsoft Windows oder im Apple Macintosh Finder einzurichten und über Backup-Werkzeuge einen kontinuierlichen Delta-Datenabgleich aus der Cloud oder in die Cloud durchzuführen, auch der Import und Export von Daten im XML-Format steht zur Verfügung

◇ **Haftung:** Die Haftung von Fabasoft für Gewährleistungsansprüche, sowie die Haftung von Fabasoft für allfällige Schäden, wird auf tatsächlich verursachte positive Schäden und darüber hinaus auf solche Schäden begrenzt, die durch Vorsatz oder grobe Fahrlässigkeit herbeigeführt worden sind. Fabasoft haftet nicht für mittelbare oder indirekte Schäden

[5]http://www.tuev-sued.de/management-systeme/iso-9001
[6]http://www.iso.org/iso/catalogue_detail?csnumber=51986
[7]http://www.tuv.com/de/deutschland/gk/managementsysteme/informationstechnologie/iso_27001_informationssicherheit/iso_27001.jsp
[8]http://isae3402.com/ISAE3402_reports.html

Die Fabasoft Cloud bietet in Bezug auf die Datensicherheit folgende Maßnahmen:

- ◇ Verschlüsselte Kommunikation zwischen dem Endnutzer (Webbrowser) und der Fabasoft Cloud, die Verbindungen erfolgen auf der Basis des https (Hypertext Transfer Protocol Secure) Standards TLS (Transport Layer Security)
- ◇ Kundendaten werden auf verschlüsselten Festplatten oder verschlüsselten Partitionen von Festplatten abgelegt, in den Fabasoft Cloud-Rechenzentren erfolgt die Datenverschlüsselung über Self Encrpyting Disks
- ◇ Kunden haben die Möglichkeit, bestimmte Unterlagen mit einem ihm verfügbaren und bekannten Verschlüsselungswerkzeug zu verschlüsseln und in verschlüsselter Form am Fabasoft Schreibtisch oder in einem Fabasoft Teamroom[9] abzulegen (z.B. als passwortgeschützte ZIP-Datei)
- ◇ Neben der Authentifizierung mit Login-Namen und Passwort unterstützen die Fabasoft Cloud-Dienste Zwei-Faktor-Authentifizierung (Mobile PIN), Single-Sign-On über Client-Zertifikate (X.509 Standard[10], auch auf mobilen Devices) und die Anmeldung mit einer Digitalen Identität (Österreich: Handysignatur, Deutschland: neuer Personalausweis, Schweiz: SuisseID). Die Authentifizierung erfolgt über ein Fabasoft IDP-Service, welches die Standards SAML[11] (Security Assertion Markup Language) und OAUTH[12] implementiert
- ◇ Die Fabasoft Server zeichnen automatisch alle Anfragen auf, dies beinhaltet: IP-Adressen, Datum&Uhrzeit, Aufgerufene URL, Browsertyp, Cookie und Sprache
- ◇ Fabasoft stellt Kundendaten Dritten grundsätzlich nicht zur Verfügung, außer aus einer gesetzlichen Verpflichtung heraus oder auf Kundenwunsch
- ◇ Fabasoft unterliegt als europäisches Unternehmen den folgenden Datenschutzgesetzen:
  - Richtlinie 95/46/EG des Europäischen Parlaments zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie)
  - Richtlinie 2002/58/EG des Europäischen Parlaments über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)
  - Für Deutschland: Bundesdatenschutzgesetz (BDSG)
- ◇ Gesetzliches: Fabasoft ist verpflichtet, Daten, Informationen oder Materialien, die der Kunde im Rahmen der Nutzung der Leistungen von Fabasoft aus dem Vertrag über die Nutzung eines Servicepakets übermittelt, gemäß der Bestimmungen dieser AGB keinen anderen Personen als sich selbst zugänglich zu machen, diese Daten nicht zu

[9] https://www.fabasoft.com/cloud/de-de/feature-teamroom
[10] http://www.itwissen.info/definition/lexikon/X-509-X-509.html
[11] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
[12] http://oauth.net/

benutzen und auch nicht zu veröffentlichen. Insoweit diese Daten „personenbezogene Daten“ im Sinn des jeweilig national anzuwendenden Datenschutzgesetzes umfassen, beachtet Fabasoft entsprechend das Datengeheimnis im Sinne der nationalen materiellen datenschutzrechtlichen Vorschriften. Falls Fabasoft aufgrund einer gesetzlichen Verpflichtung oder im Zug eines rechtlichen Verfahrens vor Gericht oder einer sonstigen staatlichen Autorität verpflichtet wird, bei Fabasoft vom Kunden gespeicherte Daten dem Gericht oder der sonstigen staatlichen Autorität zugänglich zu machen, wird Fabasoft den Kunden hiervon so rasch als möglich (elektronisch) verständigen

- ◇ Secomo: hochverfügbares Serverpaar im Verbund - als Ergänzung zur normalen Cloud (Zusatzkosten)-, bietet hohe Sicherheit mit End-to-End-Verschlüsselung am Arbeitsplatz und nicht erst am Server, der Schlüssel zu den Daten verbleibt ausschließlich im Unternehmen, nur der Kunde alleine hat darauf Zugriff. (Siehe Kapitel 6)

4.1.1.2. Konklusion

Nach den Ergebnissen aus der Umfrage und der eigenen Recherche kann man festhalten, dass die Fabasoft Cloud ein sehr hohes Sicherheitsniveau besitzt. Diverse ISO-Zertifizierungen[13] (International Organization for Standardization) sind vorhanden und auch aktuell. Die Server befinden sich innerhalb Europas (z.B. Deutschland), das Unternehmen ist somit an die innereuropäischen und bei Serverstandort Deutschland - an das Bundesdatenschutzgesetz gebunden. Die Leistungsmerkmale in Bezug auf Datenschutz der Fabasoft Cloud sind für die Öffentlichkeit ohne Schwierigkeiten online einzusehen und sehr ausführlich beschrieben[14].

Die Fabasoft Cloud kann, ohne Einschränkungen und Bedenken, für die Benutzung von BPM in der Public Cloud, in Bezug auf personenbezogene Daten, eingesetzt werden.

4.1.2. PICTURE

Die PICTURE GmbH[15] ist ein Beratungs- und Softwareunternehmen mit Sitz in Münster, welches sich auf die Dokumentation und Verbesserung von Geschäftsprozessen öffentlicher Verwaltungen spezialisiert hat. Die PICTURE-Prozessplattform basiert auf der PICTURE-Modellierungsmethode, bei der es sich um eine semantische Modellierungssprache handelt, die speziell auf die öffentliche Verwaltung ausgerichtet ist.

Sie findet ihre Verbreitung derzeit im deutschsprachigen Raum in öffentlichen Verwaltungen aller Ebenen (Bundes- und Landeseinrichtungen, Kreisverwaltungen und Kommunen) sowie

[13] http://www.iso.org/iso/home.html
[14] https://www.fabasoft.com/cloud/de-de/trust
[15] http://www.picture-gmbh.de/

bei Kirchenverwaltungen, Kammern und Verbänden sowie Hochschulen. Die PICTURE-Methode wurde 2005 am Institut für Wirtschaftsinformatik der Westfälischen Wilhelms-Universität Münster und am European Research Center for Information Systems (ERCIS) entwickelt.[16]

Die PICTURE-Prozessplattform ist als SaaS-Produkt in der Cloud oder als On-Premise Lösung zum Betrieb auf den eigenen Servern erhältlich - und verfügt über:

- ◇ eine Prozesslandkarte und Prozesssteckbriefe
- ◇ einen Prozessablauf mit Teilprozessen
- ◇ ein Prozessregister
- ◇ Analysemöglichkeiten

Im Folgenden werden die Antworten aus der Umfrage bezüglich PICTURE aufgelistet:

Frage	**Antwort**
Allgemein	
Wie lautet der Name der Firma, für die Sie arbeiten?	Keine Angabe
Wie lautet der Name des Produktes, welches Sie bewerten möchten?	PICTURE
Wird das Produkt von Ihrer Firma hergestellt oder handelt es sich um einen Drittanbieter?	Hersteller
Welche Services werden angeboten?	SaaS
Security	
Verfügt der Provider über ein ausgereiftes IT-Sicherheitskonzept? (Schutz vor Malware, Abwehr von DDoS-Angriffen)	Ja
Welche Vorkehrungen die ggf. Ausfallzeiten und Datenverlust vorbeugen, stehen zur Verfügung?	Backups, Sonstiges: kurzfristige Sicherung: 2-stündlich Mo-Fr 6-20Uhr für 8 Tage vorgehalten, langfr. Sicherung: monatlich für 6 Monate vorgehalten
Existiert ein Intrusion Detection System (Angriffserkennungssystem) zur Überwachung der IT-Infrastruktur?	Sonstiges: Sicherungsvorkehrungen gemäß §9 BDSG

[16] http://www.picture-eu.org/partners/ercis.shtml

Frage	Antwort
Ist ein effektives Verschlüsselungs- und Schlüsselmanagement vorhanden, um die Kundendaten und den Datenaustausch sicher zu verschlüsseln?	Sonstiges: https
Ist ein definiertes Vorgehensmodell der firmeninternen IT-Geschäftsprozesse vorhanden?	Ja, ITIL
Werden regelmäßige und unabhängige Prüfungen des IT-Sicherheitszustands, wie z.B. Penetrations-Tests und Audits, vorgenommen?	Sonstiges: regelmäßig
Werden interne Angriffe (d.h. von Kunden auf Kunden) verhindert bzw. entdeckt und effektiv untersucht und unterbunden?	Ja
Compliance	
In welchem Land liegt der Serverstandort?	Deutschland
Entspricht die Datenspeicherung von personenbezogenen Daten dem Bundesdatenschutzgesetz?	Ja
Sind Compliance-Zertifikate vorhanden? Wenn ja welche?	Sonstiges: ISO 9001
Werden interne Bereiche an Subunternehmer ausgelagert?	Sonstiges: Gehostet von PICTURE
Werden für Kunden SLA (Service Level Agreements) angeboten?	Sonstiges: AGB
Ist es möglich vorhandene SLA (Service Level Agreements) an Kundenwünsche anzupassen?	Sonstiges: Möglichkeit einer gesondert zu schließenden Auftragsdatenverarbeitungs -Vereinbarung
Funktionalität	
Ist eine strikte Mandantentrennung in der Cloud vorhanden?	Keine Angabe
Können kurzfristig weitere Kapazitäten hinzugefügt und wieder entfernt werden, falls nötig? (Skalierbarkeit)	Ja
Können Daten mit geringem Aufwand exportiert und zu einem anderen Provider migriert werden?	Sonstiges: Kostenpflichtig, Leistung nach Aufwand

Frage	Antwort
Können offene Formate für den Datenaustausch verwendet werden?	Sonstiges: PDF/EXCEL-Export, Prozess XML-Export (BPMN 2.0, PicXML), Prozess XML-Import (PicXML)
Findet dieser Datenaustausch verschlüsselt statt? Wenn ja, wo werden die Daten ver- und entschlüsselt bzw. wo liegt der Schlüssel?	Sonstiges: https, TLS / SSL
Kann mittels Single Sign-On auf die Kundenserver zugegriffen werden?	Sonstiges: Flexible Nutzer-/Rechteverwaltung
Gibt es eine 2-Faktor-Authentisierung für die Kunden?	Keine Angabe
Falls der Kunde „Managed Services“ bevorzugt, existiert hierfür ein effektives Patch- und Änderungsmanagement vorhanden? (z.B. Updates)	Ja
Verfügbarkeit	
Ist für Download/Upload eine ausreichende und unterbrechungsfreie Internetverbindung gewährleistet? (z.B. geringe Latenzzeiten)	Ja
Stehen dem Kunden Alternativen zur Verfügung, falls der Cloud-Service ausfallen sollte? (z.B. redundante Notfall-Server/Komponenten)	Sonstiges: "Work-Arounds"
Kann bei einer möglichen Insolvenz des Providers der Schutz und die Verfügbarkeit der Daten gewährleistet werden?	Keine Angabe
Ist der Cloud-Service hochverfügbar? (min. 99,9%)	Sonstiges: 98,5% im Jahresmittel bezogen auf 6-oUhr 7 Tage die Woche
Existiert ein ausgeprägter und professioneller Kundensupport?	Ja
Vertrag	
Wie wird der Vertrag geschlossen?	online
Wie werden die für den Vertrag benötigten Personendaten der Kunden überprüft?	Sonstiges: vollständige Registrierung
Wie sehen die Laufzeiten des Vertrages aus?	Sonstiges: 12 und 3 Monate
Besteht bei Vertragskündigung die Möglichkeit die Kundendaten vollständig zu löschen?	Ja

Frage	Antwort
Wie erfolgt die Abrechnung der Services?	pauschal, Sonstiges: monatliche Miete
Kann der Vertrag angepasst werden, wenn sich die Anforderungen des Kunden ändern?	Sonstiges: Änderungen oder Ergänzungen bedürfen der Schriftform

Tabelle 4.2.: Auswertung der Umfrage - PICTURE

4.1.2.1. Eigene Recherche

Die PICTURE GmbH ist ein Cloud Service Provider mit Sitz in Münster, welcher Prozessmanagement in der Cloud anbietet (SaaS). Der Serverstandort befindet sich in Deutschland und somit unterliegt die PICTURE GmbH dem deutschen Bundesdatenschutzgesetz, was ein hohes Datenschutzniveau ermöglicht. Gehostet und gewartet wird von PICTURE selbst, ob andere Subunternehmen im Unternehmen vorkommen die mit den Cloud-Diensten zusammenhängen, konnte nicht ermittelt werden. Folgende Service Levels konnten in Erfahrung gebracht werden[17]:

- **Verfügbarkeit:** Die Verfügbarkeit beträgt 98,5% im Jahresmittel, bezogen auf 6.00 - 00.00 Uhr täglich, 7 Tage die Woche und 95% in der übrigen Zeit. Von der Berechnung der Verfügbarkeit ausgenommen sind Ausfallzeiten durch Wartung und Pflege zwischen 00.00 - 2.00 Uhr täglich, sowie im Einzelfall notwendige, im Voraus angekündigte Wartungsarbeiten außerhalb dieser Zeiten.
- **Datensicherung:** Die Nutzdaten des Kunden werden in folgenden Sicherungsmustern und -intervallen gesichert:
  - kurzfristige Sicherung: 2-stündlich, zwischen 06.00 - 20.00Uhr, montags - freitags, vorgehalten für 8 Kalendertage
  - langfristige Sicherung: monatlich, am ersten des Monats, vorgehalten für 6 Monate
- **Mängelbeseitigung:** spätestens nach Ablauf der Reaktionszeit wird mit der Analyse, Bestätigung und Beseitigung des gemeldeten Mangels begonnen. Die Reaktionszeit beträgt 6 Stunden nach Meldung des Mangels innerhalb der Betriebszeiten des Supports. Falls eine Behebung innerhalb adäquater Zeit aufgrund technischer oder organisatorischer Komplexität nicht möglich ist, werden technische oder organisatorische Umgehungen (”Work-Arounds”) entwickelt und angeboten, dass der Kunde die gestörte Funktionalität in angemessener Weise nutzen kann.

[17]http://www.picture-gmbh.de/downloads/AGB%20PICTURE%20Prozessplattform%20SaaS%20-%2001-11-2014.pdf

- ◇ **Support:** PICTURE stellt einen Software-Support per Email und/oder Telefon bereit. Die Betriebszeiten für den Support sind Mo-Fr 09.00 - 17.00Uhr, mit Ausnahme von gesetzlichen Feiertagen am Betriebssitz von PICTURE, sowie nicht am 24.12. und 31.12. Der Support übernimmt folgende Leistungen
  - Initiale Einrichtung der Mandanten und Admin-Nutzer des Kunden
  - Freischaltung von Modulen entsprechend der erworbenen Nutzungslizenzen
  - Betrieb des Mandanten
  - Erzeugungen von regelmäßigen Sicherungskopien
  - Entgegennahme und Bearbeitung von Störungsmeldungen
  - Entgegennahme und Bewertung von Feature-Wünschen
  - Beantwortung von Bedienfragen, die nicht von der aktuellen Dokumentation abgedeckt sind
- ◇ **Datensicherheit und Datenschutz:** Die Parteien werden die jeweils anwendbaren, insbesondere in Deutschland gültigen datenschutzrechtlichen Bestimmungen beachten und ihre im Zusammenhand mit dem Vertrag und dessen Durchführung eingesetzten Beschäftigten auf das Datengeheimnis nach § 5 BDSG verpflichten, soweit diese nicht bereits allgemein entsprechend verpflichtet sind. PICTURE trifft die technischen und organisatorischen Sicherheitsvorkehrungen gemäß der Anlage zu § 9 BDSG
- ◇ **Datenverarbeitung im Auftrag:** PICTURE handelt im Sinne aller datenschutzrechtlichen Regelungen nach § 11 und § 9 BDSG und aller entsprechenden, sofern anzuwenden, landesspezifischen Datenschutzgesetzen. Auf Notwendigkeit und Anforderung des Kunden kann die Auftragsdatenvereinbarung in einer gesondert zu schließenden Auftragsdatenverarbeitungs-Vereinbarung geregelt werden.
- ◇ **Laufzeit und Kündigung:** Mindestlaufzeit 3 Monate - Kündigungsfrist 4 Wochen. Mindestlaufzeit 12 Monate - Kündigungsfrist 8 Wochen. Kündigungen bedürfen der Schriftform, die elektronische Form ist ausgeschlossen. Nach Kündigung des Vertrages ist PICTURE auf Anfrage des Kunden verpflichtet, die vom Kunden gespeicherten Nutzdaten über elektronische Fernübertragung in einem XML-Format entsprechend einer Spezifikation von PICTURE zur Verfügung zu stellen. Die Anfrage muss spätestens eine Woche vor Beendigung des Vertragsverhältnisses bei PICTURE eingehen, ansonsten ist PICTURE berechtigt und aus Datenschutzgründen verpflichtet die Nutzdaten zu löschen

4.1.2.2. Konklusion

Die PICTURE GmbH bietet eine gute Möglichkeit BPM in der Cloud zu nutzen. Der Serverstandort befindet sich in Deutschland und somit entstehen auch keine Probleme mit dem BDSG, im Hinblick auf personenbezogene Daten. Laut AGB (Allgemeine Geschäftsbedingungen) der PICTURE GmbH, werden die Richtlinien des BDSG eingehalten und

liefern somit die Grundlage des Datenschutzes. Außerdem wird zusätzlich zu den AGB'S, ein gesondert zu schließender Auftragsdatenvereinbarungs-Vertrag angeboten, in welchem Richtlinien zur Verarbeitung von Auftragsdaten angeführt werden können. Allerdings gibt es keine Informationen darüber, ob und wenn ja wie, die Kundendaten auf den Servern von PICTURE zusätzlich verschlüsselt werden, es wird nur angegeben, dass die Verbindung per https verschlüsselt wird.

Ebenso ist eine ISO-Zertifizierungen zwar vorhanden (ISO 9001[18]), es wurden aber keine weiteren Angaben zu anderen Zertifizierungen gemacht, was demnach - auf Seite von PICTURE - durchaus noch ausbaufähig ist. Im Großen und Ganzen ist die PICTURE Prozesslandschaft für BPM in der Public Cloud ausreichend geeignet und für den Gebrauch der Nutzer zu empfehlen. Allerdings sollte vor Vertragsabschluss hinsichtlich der Datenverschlüsselung beim Anbieter nachgefragt werden ob die Daten auf den Providerservern zusätzlich verschlüsselt werden, um den Schutz von sensiblen Daten zu gewährleisten.

4.1.3. Microsoft Dynamics NAV - Windows Azure

Die Microsoft Corporation ist ein multinationaler Software- und Hardwarehersteller mit Hauptsitz liegt in Redmond, einem Vorort von Seattle im US-Bundesstaat Washington. Microsoft Dynamics NAV ist eine Standardsoftware für ERP-Systeme, wobei im Fokus ein effizienter betrieblicher Wertschöpfungsprozess und eine optimale Steuerung der betrieblichen Abläufe stehen. Seit 2013 ist es möglich Microsoft Dynamics NAV in der Cloud zu nutzen. Die Kunden können entscheiden ob die NAV-Umgebung im Rechenzentrum des Hosting-Partners oder in der Public Cloud auf Windows Azure betrieben werden soll[19].

Microsoft Dynamics NAV wird besonders von kleinen und mittleren Unternehmen eingesetzt und wird exklusiv über ein Netz zertifizierter Microsoft-Partner vertrieben und verfügt im Starter Pack über folgende Funktionalitäten[20]:

- ◇ Finanzmanagement
- ◇ Customer Relationship Management
- ◇ Projektmanagement
- ◇ Supply Chain Management
- ◇ Personalverwaltung

Im Folgenden werden die Antworten aus der Umfrage bezüglich Microsoft Dynamics NAV - Windows Azure aufgelistet:

[18] http://www.picture-gmbh.de/pdf/generated/e6420eabe7b5be1de2bd5de62fb6da05.pdf
[19] http://blogs.technet.com/b/microsoft_presse/archive/2013/06/20/erp-goes-cloud-microsoft-dynamics-nav-jetzt-auf-windows-azure-verf-252-gbar.aspx
[20] http://download.microsoft.com/download/E/6/2/E626FB36-36B9-4A73-9268-C133F0B4C672/Microsoft_Dynamics_NAV_2015_Produkt-und_Funktions%C3%BCberblick_DE_Feb2015.pdf

Frage	Antwort
Allgemein	
Wie lautet der Name der Firma, für die Sie arbeiten?	Keine Angabe
Wie lautet der Name des Produktes, welches Sie bewerten möchten?	Microsoft Dynamics NAV
Wird das Produkt von Ihrer Firma hergestellt oder handelt es sich um einen Drittanbieter?	Drittanbieter
Welche Services werden angeboten?	SaaS
Security	
Verfügt der Provider über ein ausgereiftes IT-Sicherheitskonzept? (Schutz vor Malware, Abwehr von DDoS-Angriffen)	Ja
Welche Vorkehrungen die ggf. Ausfallzeiten und Datenverlust vorbeugen, stehen zur Verfügung?	Backups, Redundante IT-Infrastruktur Physikalische Sicherheit Sonstiges: Netzwerkisolierung, Protokollierung
Existiert ein Intrusion Detection System (Angriffserkennungssystem) zur Überwachung der IT-Infrastruktur?	Ja
Ist ein effektives Verschlüsselungs- und Schlüsselmanagement vorhanden, um die Kundendaten und den Datenaustausch sicher zu verschlüsseln?	Ja, AES-256 Sonstiges: und andere
Ist ein definiertes Vorgehensmodell der firmeninternen IT-Geschäftsprozesse vorhanden?	Ja, ITIL
Werden regelmäßige und unabhängige Prüfungen des IT-Sicherheitszustands, wie z.B. Penetrations-Tests und Audits, vorgenommen?	Sonstiges: ja, regelmäßig
Werden interne Angriffe (d.h. von Kunden auf Kunden) verhindert bzw. entdeckt und effektiv untersucht und unterbunden?	Ja
Compliance	
In welchem Land liegt der Serverstandort?	Deutschland, Europa, EWR, USA Sonstiges: Kunde kann auswählen
Entspricht die Datenspeicherung von personenbezogenen Daten dem Bundesdatenschutzgesetz?	Keine Angabe

Frage	Antwort
Sind Compliance-Zertifikate vorhanden? Wenn ja welche?	Ja, ISO 27001/27002 Ja, SSAE 16 / ISAE 3402 Sonstiges: Cloud Controls Matrix der CSA, Safe Harbor, u.a.
Werden interne Bereiche an Subunternehmer ausgelagert?	Ja, z.B. Kundensupport
Werden für Kunden SLA (Service Level Agreements) angeboten?	Ja
Ist es möglich vorhandene SLA (Service Level Agreements) an Kundenwünsche anzupassen?	Keine Angabe
Funktionalität	
Ist eine strikte Mandantentrennung in der Cloud vorhanden?	Ja
Können kurzfristig weitere Kapazitäten hinzugefügt und wieder entfernt werden, falls nötig? (Skalierbarkeit)	Ja
Können Daten mit geringem Aufwand exportiert und zu einem anderen Provider migriert werden?	Sonstiges: Migration Accelerator tool
Können offene Formate für den Datenaustausch verwendet werden?	Ja, Java, .NET, node.js, PHP, Python, Ruby
Findet dieser Datenaustausch verschlüsselt statt? Wenn ja, wo werden die Daten ver- und entschlüsselt bzw. wo liegt der Schlüssel?	Sonstiges: Private Verbindung
Kann mittels Single Sign-On auf die Kundenserver zugegriffen werden?	Sonstiges: ja, Azure Active Directory
Gibt es eine 2-Faktor-Authentisierung für die Kunden?	Ja
Falls der Kunde „Managed Services“ bevorzugt, existiert hierfür ein effektives Patch- und Änderungsmanagement vorhanden? (z.B. Updates)	Ja
Verfügbarkeit	
Ist für Download/Upload eine ausreichende und unterbrechungsfreie Internetverbindung gewährleistet? (z.B. geringe Latenzzeiten)	Ja
Stehen dem Kunden Alternativen zur Verfügung, falls der Cloud-Service ausfallen sollte? (z.B. redundante Notfall-Server/Komponenten)	Ja, mehrere Serverstandorte

Frage	Antwort
Kann bei einer möglichen Insolvenz des Providers der Schutz und die Verfügbarkeit der Daten gewährleistet werden?	Ja
Ist der Cloud-Service hochverfügbar? (min. 99,9%)	Ja
Existiert ein ausgeprägter und professioneller Kundensupport?	Ja
Vertrag	
Wie wird der Vertrag geschlossen?	online
Wie werden die für den Vertrag benötigten Personendaten der Kunden überprüft?	Keine Angabe
Wie sehen die Laufzeiten des Vertrages aus?	monatlich kündbar
Besteht bei Vertragskündigung die Möglichkeit die Kundendaten vollständig zu löschen?	Ja
Wie erfolgt die Abrechnung der Services?	pay-per-use
Kann der Vertrag angepasst werden, wenn sich die Anforderungen des Kunden ändern?	Ja

Tabelle 4.3.: Auswertung der Umfrage - Microsoft Dynamics/Windows Azure

4.1.3.1. Eigene Recherche

Die Microsoft Corporation ist ein weltweiter Soft- und Hardware Hersteller mit Hauptsitz in Redmond in den Vereinigten Staaten von Amerika. Zwar bietet Microsoft mit Microsoft Azure auch Serverplattformen in Europa an z.B. Irland, aber es kann nicht ausgeschlossen werden, dass Kundendaten, die auf europäischen Servern gespeichert werden, auf außereuropäische Zonen wie die USA ausgelagert werden und von Dritten eingesehen werden können (z.B. US-Patriot Act). Dies wiederum kann zu Problemen mit dem BDSG führen, wenn personenbezogene Daten in die Cloud von Microsoft ausgelagert werden (siehe auch Kapitel 5). Folgende Service Levels[21] konnten in Erfahrung gebracht werden:

- **Verfügbarkeit[22]:** Falls Microsoft die festgelegten Verfügbarkeiten nicht einhalten kann, werden Dienstgutschriften eingesetzt. Diese Dienstgutschriften gelten nur für Gebühren, die für den Dienst, die Dienstressource oder die Dienststufe gezahlt wurden, für den bzw. die eine Vereinbarung zum Servicelevel nicht eingehalten wurde (Umsatzausfälle des Kunden sind nicht Teil der Dienstgutschriften)

[21] http://go.microsoft.com/fwlink/?linkid=392408&clcid=0x407
[22] http://azure.microsoft.com/de-de/support/legal/sla/

- Für Cloud-Dienste wird für die Rollen mit Internetzugriff in mindestens 99.95% der Zeit externe Konnektivität garantiert, wenn der Kunde zwei oder mehr Rolleninstanzen in unterschiedlichen Fehler- und Upgradedomänen bereitstellt
- Für alle virtuellen Computer mit Internetzugriff, die mindestens zwei bereitgestellte Instanzen in derselben Verfügbarkeitsgruppe aufweisen, wird eine externe Konnektivität von mindestens 99.95% der Zeit garantiert
- Für das virtuelle Netzwerk wird eine Gatewayverfügbarkeit von 99.9% garantiert
- Prozent der monatlichen Betriebszeit: < 99.9% Dienstgutschrift: 10% - < 99.5% Dienstgutschrift 25%

◇ **Infrastruktur:**

- Physische Sicherheit: geographisch getrennte Rechenzentren, ausgestattet für 24x7x365 Betrieb, gesichert gegen Stromausfall, physikalischen Einbruch und Netzwerkausfälle, entspricht den Industriestandards (z.B. ISO 27001) für physische Sicherheit und Verfügbarkeit, 24x7 Personal, Zäune, Barrieren, Alarme, Erdbebenschutz, Kameras, 2-Faktor-Zutrittskontrolle (biometrisch und Kartenleser), Notstromversorgung
- Monitoring und Logging: zentralisiertes Monitoring und Analysesysteme überwachen die großen Mengen an Informationen die generiert werden.
- Update Management: Azure integriert ein Deployment-System für die Verteilung und Installation der Sicherheitsupdates, benutzt wird eine Kombination von Microsoft und Drittanbieter Scanningtools für das Betriebssystem, Webanwendungen und Datenbankscanner für die Azure-Umgebung
- Virenschutz: Alle Azure Software Komponenten durchlaufen einen Virenscan, zusätzlich bietet Microsoft Antimalware-Produkte auf allen Azure VM's. Es wird empfohlen, dass der Kunde ebenfalls Antivirenschutz Software verwendet (z.B. Microsoft Antimalware for Cloud Services and Virtual Machines)
- Penetrationstests: Microsoft für regelmäßig Penetrationstest in den Rechenzentren durch, ebenso ist es für Kunden möglich eigene autorisierte Penetrationstests der gehosteten Applikationen durchzuführen (nicht der Rechenzentren)
- DDoS Protection: Azure besitzt ein Defense-System gegen DDoS-Angriffe auf die Azure Services, benutzt werden Standardtechniken für Detection und Mitigation (Schadensminderung), das System widersteht Angriffen von innerhalb und außerhalb der Plattform

◇ **Netzwerksicherheit:**

- Netzwerkisolation: Azure benutzt logische Isolation um die verschiedenen Kundendaten voneinander zu trennen (Multimandantenfähigkeit), um zu verhindern, dass Kunden auf andere Kundendaten zugreifen können

  - Virtuelle Netzwerke: Kunden können ein virtuelles Netzwerk in der Cloud beantragen (kostenpflichtig: Statisches/dynamisches Routing bei einem VPN-Gateway 0,0269 Euro pro Gatewaystunde (ca. 21 Euro pro Monat)), jedes VPN ist isoliert von den anderen VPN's. Ebenso bietet Microsoft Side-to-Side und Point-to-Side VPN Verbindungen an
  - Verschlüsselte Kommunikation: Für Datenübertragung zwischen Kunde und Microsoft Datenzentren und innerhalb der Datenzentren verwendet Microsoft standardisierte Transportprotokolle, Kunden können zusätzlich (Azure Key Vault kostenpflichtig: geheime Schlüssel und softwaregeschützte Schlüssel 0,0112 Euro / 10.000 Vorgänge) eine Datenverschlüsselung mit eigenem Key-Management beantragen

- ◇ **Datensicherheit:**
  - Datenisolation: Multimandantenfähigkeit, mehrere Kundendaten und virtuelle Maschinen sind auf derselben Hardware gespeichert
  - Sicherheit von gespeicherten Daten: Microsoft bietet viele Verschlüsselungsmethoden an (z.B. Azure Key Vault (kostenpflichtig))
  - Datenübermittlung: Azure benutzt zur Datenübermittlung von Kunde zu Microsoft und innerhalb der Microsoft Datenzentren industrielle Standards wie z.B. TLS
  - Datenredundanz: Es bestehen Wahlmöglichkeiten zwischen in-Country und out-Country Speicherung, d.h. die Daten können entweder nur in dem ausgewählten geographischen Ort gespeichert werden oder außerhalb dieses Ortes (mit Ausnahmen, siehe Kapitel 5)
  - Datenlöschung: bei Datenlöschung oder Vertragskündigung, verfolgt Microsoft strikte Standards für das Überschreiben von Datenspeichern bevor sie wieder in Benutzung genommen werden, ebenso stimmt Microsoft vertraglich spezifischen Prozessen zur Datenlöschung zu

- ◇ **Identität und Zugriff:**
  - Enterprise Cloud Directory: Microsoft bietet mit Azure Active Directory einen Dienst für die Identitäts- und Zugriffsverwaltung an (Kostenlos oder kostenpflichtig: Preis für Premiumdienst 4,4682 Euro Benutzer/Monat)
  - Multi-Faktor-Authentisierung: Die mehrstufige Authentifizierung von Azure trägt zur Sicherung des Zugriffs auf Daten und Anwendungen bei, Verifizierungsoptionen – Telefonanruf, SMS oder Benachrichtigung in einer mobilen App (kostenpflichtig: Pro Benutzer 1,0426 Euro pro Monat (unbegrenzte Authentifizierungen) oder pro Authentifizierung 1,0426 Euro pro 10 Authentifizierungen)

- Monitoring und Logging der Zugriffe: Sicherheitsreports werden benutzt um Zugriffpatterns zu überwachen und um potentielle Gefahren zu identifizieren. Kunden können zusätzliche Monitoringfunktionen wie z.B. Drittanbieter-Monitoring-Tools (kostenpflichtig) beziehen um zusätzlichen Gefahren vorzubeugen. Kunden können Reports bei Microsoft beantragen, die Informationen über die Zugriffe der Kunden enthalten.
- Beschränkter Zugriff von Microsoftpersonal: beschränkter Zugriff, erfolgt nur wenn nötig, z.B. bei Troubleshooting oder Behandeln von Gefahren wie Malware. Wenn Zugriff zu Kundendaten gewährt wird, wird dieser kontrolliert und gespeichert, erfolgt mit Multi-Faktor-Authentisierung, Zugriff nur solange wie nötig.
- Gesetzliche Informationsanfrage: Microsoft legt Kundendaten nicht gegenüber dritten Parteien offen (u. a. Personen des Gesetzesvollzugs, anderen Regierungsautoritäten oder Zivilprozessführern), außer dies wird vom Kunden angewiesen oder ist aufgrund von gesetzlichen Bestimmungen erforderlich. Sollte Microsoft von einer dritten Partei um die Herausgabe von Kundendaten gebeten werden, wird versucht, die jeweilige dritte Partei bezüglich der Herausgabe der Kundendaten direkt an den Kunden zu verweisen. Als Teil eines solchen Vorgangs ist Microsoft berechtigt, der dritten Partei grundlegende Kontaktinformationen des Kunden zur Verfügung zu stellen. Falls Microsoft zur Offenlegung von Kundendaten an eine dritte Partei verpflichtet ist, werden die betroffenen Kunden sofort darüber informiert und bekommen eine Kopie der Anforderung, wenn Microsoft dies nicht aufgrund von gesetzlichen Bestimmungen untersagt ist
- Datenzugehörigkeit: Kunden von Microsoft Azure behalten das exklusive Eigentumsrecht der Daten. Microsoft verwendet keine Kundendaten oder daraus abgeleitete Informationen zu Werbe- oder anderen kommerziellen Zwecken. Microsoft verwendet Kundendaten ausschließlich zu Zwecken, die mit der Bereitstellung der Dienste kompatibel sind. Neben den alltäglichen Operationen können die Kundendaten zum Beispiel aus den folgenden Anlässen verwendet werden:
  - Fehlerbehebung zur Verhinderung, Erkennung und Lösung von Problemen, die den Betrieb der Dienste beeinträchtigen
  - Fortlaufende Verbesserung von Features wie z. B. der Erkennung möglicher Bedrohungen und den Schutz der Dienste und Benutzer vor neuen und aufkommenden Bedrohungen (beispielsweise Schadsoftware oder Spam)
  - Personalisierte oder rückschlussbasierte Dienstfunktionen
- Kontrolle des Speicherortes: Microsoft bietet ein globales Netzwerk von Datenzentren an, für Europa z.B. Irland. Daten werden nur innerhalb des ausgewählten geographischen Ortes gespeichert und repliziert (Redundanz), aber nicht außerhalb dieser Zone (Anmerkung: außer es liegen rechtliche Bestimmungen vor z.B. US-Patriot Act))

◇ **Compliance[23]:** Microsoft bietet eine Menge an Zertifikaten an, hier werden die wichtigsten für Deutschland und Europa aufgelistet:

- Audit und Zertifizierung nach ISO 27001/27002[24]: Azure strebt die jährliche ISO/IEC 27001/27002:2013-Zertifizierung an, einen internationalen Standard zur Informationssicherheit. Mit dem ISO/IEC 27001/27002:2013-Zertifikat wird validiert, dass Microsoft die in diesem Standard definierten, international anerkannten Informationssicherheitskontrollen implementiert hat, einschließlich Richtlinien und allgemeine Grundsätze für das Initiieren, Implementieren, Verwalten und Optimieren des Informationssicherheitsmanagements innerhalb einer Organisation.
- SOC 1/SSAE 16/ISAE 3402 und SOC 2-Nachweise[25]: Azure wurde vom Service Organization Control (SOC)-Berichterstellungsframework auf SOC 1-Typ 2 und SOC 2-Typ 2 überprüft. Der SOC 1 Typ 2-Prüfbericht bestätigt die Entwurfs- und Betriebseffektivität der Azure-Kontrollen. Die SOC 2 Typ 2-Prüfung enthält eine weitere Prüfung der Azure-Kontrollen im Hinblick auf Sicherheit, Verfügbarkeit und Zuverlässigkeit. Azure wird jährlich geprüft, um zu gewährleisten, dass die Sicherheitskontrollen aufrechterhalten werden.
- Cloud Controls Matrix (CCM) der Cloud Security Alliance (CSA[26]): Die CCM der CSA soll grundlegende Sicherheitsprinzipien bereitstellen, um Cloudanbieter anzuleiten und potenzielle Kunden bei der Bewertung des gesamten Sicherheitsrisikos eines Cloudanbieters zu unterstützen.
- Federal Risk and Authorization Management Program (FedRAMP[27]): FedRAMP ist ein obligatorisches Programm der US-Regierung, das einen standardisierten Ansatz zur Bewertung der Sicherheit, Autorisierung und kontinuierlichen Überwachung für Clouddienste bietet
- Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS[28]): Microsoft hat die Azure Government-Richtlinien und -Prozeduren überprüft, um sicherzustellen, dass es die erforderlichen Anforderungen für staatliche US-Behörden und lokale Behörden für das Verwenden von darin enthaltenen Diensten zur Erfassung und Verarbeitung von Strafverfolgungsdaten erfüllt
- Payment Card Industry (PCI) Data Security Standards (DSS) Level 1[29]: Bei PCI DSS handelt es sich um einen Informationssicherheitsstandard, der durch vermehrte Kontrollen von Kreditkartendaten Betrugsfälle verhindern soll. Die PCI-Zertifizierung ist für alle Organisationen erforderlich, die Zahlungsdaten von Karteninhabern speichern, verarbeiten oder übertragen

[23] http://azure.microsoft.com/de-de/support/trust-center/compliance
[24] http://www.bsigroup.com/en-US/ISO-IEC-27001-Information-Security/ISOIEC-270012013
[25] http://www.aicpa.org/soc
[26] https://cloudsecurityalliance.org
[27] http://www.gsa.gov/portal/category/102371
[28] http://www.fbi.gov/about-us/cjis
[29] https://www.pcisecuritystandards.org/security_standards/

  - OFFICIAL-Akkreditierung gemäß G-Cloud im Vereinigten Königreich[30]: Azure hat die OFFICIAL-Akkreditierung des Pan Government Accreditor der britischen Regierung erhalten und ist somit im G-Cloud-Framework enthalten
  - EU-Modellklauseln: Microsoft bietet seinen Kunden außerdem Modellklauseln für EU-Verträge, die zusätzliche vertragliche Garantien im Zusammenhang mit der Übertragung persönlicher Daten für In-Scope-Dienste enthalten. Microsofts Umsetzung dieser EU-Modellklauseln wurde durch die Datenschutzbehörden der Europäischen Union als übereinstimmend mit den strengen Datenschutznormen zertifiziert, die internationale Datenübertragungen durch die Firmen in ihren Mitgliedstaaten regeln. Microsoft ist das einzige Unternehmen, das für seine strengen vertraglichen Verpflichtungen zur Einhaltung von Datenschutzgesetzen, unabhängig davon, wo sich die Daten befinden, die gemeinsame Genehmigung der EU-Datenschutzgruppe für Artikel 29 erhalten hat
  - Federal Information Processing Standard (FIPS[31]): Die FIPS Publikation 140-2 ist ein Sicherheitsstandard der US-Regierung, das die Sicherheitsanforderungen für kryptographische Module zum Schutz von vertraulichen Informationen festlegt. Das National Institute of Standards and Technology (NIST) veröffentlicht eine Liste von Anbietern, die anhand der kryptographischen Module FIPS 140-1 und 140-2 zertifiziert wurden. Azure verwendet kryptografische Module von Microsoft aus der vom NIST veröffentlichten Prüfliste. Kunden können auf diese Weise ihre Azure Virtual Network-Dienste so konfigurieren, dass ihre Anforderungen an die Informationsverschlüsselung erfüllt werden
  - US–EU Safe Harbor Framework[32]: Microsoft hält sich an die Bedingungen des Frameworks, welches Richtlinien bezüglich der Sammlung, Benutzung und Speicherung von Daten aus Europa und dem EWR enthält

◇ Subunternehmer: Microsoft beauftragt unter Umständen andere Unternehmen, eingeschränkte Dienstleistungen wie das Bereitstellen von Kundensupport durchzuführen. Microsoft legt Kundendaten gegenüber Unterauftragnehmern nur in dem Maße offen, dass diese die vereinbarten Dienstleistungen erbringen können. Unterauftragnehmer dürfen Kundendaten für keine anderen Zwecke verwenden und müssen die Vertraulichkeit dieser Daten wahren. Unterauftragnehmer, die in Einrichtungen oder mit Geräten arbeiten, die von Microsoft kontrolliert werden, müssen die Datenschutzstandards von Microsoft einhalten. Alle anderen Unterauftragnehmer sind per Vertrag verpflichtet, Datenschutzstandards einzuhalten, die denen von Microsoft entsprechen. Eine Liste der Subunternehmer kann unter 'Subcontractors Microsoft[33]' abgerufen werden

[30] https://www.digitalmarketplace.service.gov.uk
[31] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[32] http://www.export.gov/safeharbor
[33] http://download.microsoft.com/download/6/C/C/6CC00FFF-0C43-4C0C-890B-2DF944CBEA69/Windows%20Azure%20Subcontractors.pdf

4.1.3.2. Konklusion

Microsoft ist hinsichtlich des Datenschutzes und der Datensicherheit sehr bemüht, diverse Zertifikate sind vorhanden, SLA und Security Regelungen findet man online (teils auf Deutsch/Englisch). Das Sicherheitsniveau ist im Allgemeinen sehr hoch, allerdings fallen für gewisse Zusatzleistungen wie z.B. Multi-Faktor-Autorisierung gesonderte Kosten an. Das größte Problem bezüglich des Datenschutzes von personenbezogenen Daten liegt allerdings daran, dass Microsoft ein US-Unternehmen ist. Zwar bietet Microsoft EU-Standardklauseln und das Safe Harbor Framework an, welche aber hinfällig werden, sobald gesetzliche Bestimmungen z.B. von der amerikanischen Regierung oder dem FBI (US Patriot Act) vorliegen, da US-Unternehmen dazu verpflichtet sind, die angefragten Daten den Behörden offenzulegen (siehe Kapitel 5.1.1).

Gordon Frazer, Managing Director bei Microsoft Großbritannien, hatte im Sommer 2011 erklärt, dass Cloud-Daten auch außerhalb der USA nicht vor dem Zugriff über den US Patriot Act sicher seien. Auf die Frage, ob Microsoft garantieren könne, dass europäische Daten, die in Datenzentren in der EU abgespeichert seien, auch unter dem Patriot Act nicht aus Europa geholt werden können, sagte Frazer: *"Microsoft kann diese Garantie nicht gewährleisten. Das kann auch kein anderes Unternehmen."* Weil der Softwarekonzern seinen Hauptsitz in den USA habe, unterliege Microsoft den US-Gesetzen[34].

Für sensible Firmendaten oder personenbezogene Daten, die in die Cloud ausgelagert werden sollen, kann Microsoft Dynamics NAV mit Microsoft Azure nicht uneingeschränkt vorgeschlagen werden. Wie bereits weiter oben erwähnt, ist durch die Möglichkeit, dass US-Behörden uneingeschränkten Zugriff auf Kundendaten haben können - selbst auf europäischen Microsoft Servern -, ein Konflikt mit dem BDSG unausweichlich. Somit ist diese Cloudlösung von Microsoft für deutsche Unternehmen, die personenbezogene Daten in die Public Cloud auslagern wollen, aus datenschutzrechtlichen Gründen, zum jetzigen Zeitpunkt, nicht zu empfehlen.

4.1.4. IBM - Business Process Manager on Cloud

Die International Business Machines Corporation (IBM[35]) ist ein US-amerikanisches IT- und Beratungsunternehmen mit Sitz in Armonk im US-Bundesstaat New York. IBM Business Process Manager on Cloud[36] ist ein abonnementbasierter Cloud-Service für das Geschäftsprozessmanagement (BPM). Dieses Produkt ist eine hochverfügbare und skalierbare Umgebung für die Prozessanwendungsimplementierung, die von IBM gesichert und verwaltet wird (auf Infrastruktur der IBM SoftLayer-Cloud[37] gehostet). Folgende Funktionalitäten sind vorhanden:

[34]http://www.golem.de/1110/87232.html
[35]https://www.ibm.com
[36]http://www-03.ibm.com/software/products/de/business-process-manager-cloud
[37]http://www.ibm.com/cloud-computing/de/de/softlayer.html

- ◇ BPM Lebenszyklus einschließlich Entwicklung, Test und Produktion
- ◇ Tools für Prozessdesign, -ausführung, -überwachung und -optimierung

Im Folgenden werden die Antworten aus der Umfrage bezüglich der IBM - Business Process Manager on Cloud aufgelistet:

Frage	**Antwort**
Allgemein	
Wie lautet der Name der Firma, für die Sie arbeiten?	Keine Angabe
Wie lautet der Name des Produktes, welches Sie bewerten möchten?	IBM / Business Process Manager on Cloud
Wird das Produkt von Ihrer Firma hergestellt oder handelt es sich um einen Drittanbieter?	Drittanbieter
Welche Services werden angeboten?	SaaS, PaaS, IaaS, BPMaaS
Security	
Verfügt der Provider über ein ausgereiftes IT-Sicherheitskonzept? (Schutz vor Malware, Abwehr von DDoS-Angriffen)	Ja
Welche Vorkehrungen die ggf. Ausfallzeiten und Datenverlust vorbeugen, stehen zur Verfügung?	Backup, Disaster Recovery, Redundante IT-Infrastruktur, Physikalische Sicherheit
Existiert ein Intrusion Detection System (Angriffserkennungssystem) zur Überwachung der IT-Infrastruktur?	Ja
Ist ein effektives Verschlüsselungs- und Schlüsselmanagement vorhanden, um die Kundendaten und den Datenaustausch sicher zu verschlüsseln?	Ja
Ist ein definiertes Vorgehensmodell der firmeninternen IT-Geschäftsprozesse vorhanden?	Ja, ITIL
Werden regelmäßige und unabhängige Prüfungen des IT-Sicherheitszustands, wie z.B. Penetrations-Tests und Audits, vorgenommen?	Ja, halbjährlich
Werden interne Angriffe (d.h. von Kunden auf Kunden) verhindert bzw. entdeckt und effektiv untersucht und unterbunden?	Ja
Compliance	
In welchem Land liegt der Serverstandort?	Deutschland, Europa, EWR, USA
Entspricht die Datenspeicherung von personenbezogenen Daten dem Bundesdatenschutzgesetz?	Ja

Frage	Antwort
Sind Compliance-Zertifikate vorhanden? Wenn ja welche?	Ja, ISO 27001/27002 Sonstiges: ISO 9001, ISO 20000 und CMMI
Werden interne Bereiche an Subunternehmer ausgelagert?	Keine Angabe
Werden für Kunden SLA (Service Level Agreements) angeboten?	Ja
Ist es möglich vorhandene SLA (Service Level Agreements) an Kundenwünsche anzupassen?	Nein
Funktionalität	
Ist eine strikte Mandantentrennung in der Cloud vorhanden?	Ja
Können kurzfristig weitere Kapazitäten hinzugefügt und wieder entfernt werden, falls nötig? (Skalierbarkeit)	Ja
Können Daten mit geringem Aufwand exportiert und zu einem anderen Provider migriert werden?	Sonstiges: Cloud Migration Rapid Assessment
Können offene Formate für den Datenaustausch verwendet werden?	Keine Angabe
Findet dieser Datenaustausch verschlüsselt statt? Wenn ja, wo werden die Daten ver- und entschlüsselt bzw. wo liegt der Schlüssel?	Ja, VPN
Kann mittels Single Sign-On auf die Kundenserver zugegriffen werden?	Ja
Gibt es eine 2-Faktor-Authentisierung für die Kunden?	Zugriffskontrolle
Falls der Kunde „Managed Services“ bevorzugt, existiert hierfür ein effektives Patch- und Änderungsmanagement vorhanden? (z.B. Updates)	Ja
Verfügbarkeit	
Ist für Download/Upload eine ausreichende und unterbrechungsfreie Internetverbindung gewährleistet? (z.B. geringe Latenzzeiten)	Ja
Stehen dem Kunden Alternativen zur Verfügung, falls der Cloud-Service ausfallen sollte? (z.B. redundante Notfall-Server/Komponenten)	Ja

Frage	Antwort
Kann bei einer möglichen Insolvenz des Providers der Schutz und die Verfügbarkeit der Daten gewährleistet werden?	Ja
Ist der Cloud-Service hochverfügbar? (min. 99,9%)	Ja
Existiert ein ausgeprägter und professioneller Kundensupport?	Ja
Vertrag	
Wie wird der Vertrag geschlossen?	online, schriftlich
Wie werden die für den Vertrag benötigten Personendaten der Kunden überprüft?	Keine Angabe
Wie sehen die Laufzeiten des Vertrages aus?	Sonstiges: unterschiedlich
Besteht bei Vertragskündigung die Möglichkeit die Kundendaten vollständig zu löschen?	Ja
Wie erfolgt die Abrechnung der Services?	Sonstiges: monatlich
Kann der Vertrag angepasst werden, wenn sich die Anforderungen des Kunden ändern?	Ja

Tabelle 4.4.: Auswertung der Umfrage - IBM - Business Process Manager on Cloud

4.1.4.1. Eigene Recherche

IBM ist eines der weltweit führenden Unternehmen für Hardware, Software und Dienstleistungen im IT-Bereich sowie eines der größten Beratungsunternehmen. Gemessen am Umsatz ist das Unternehmen der weltweit drittgrößte Softwarehersteller (Stand 2014)[38]. IBM ist, wie Microsoft zuvor, ein US-Unternehmen und somit kann es wieder zu Problemen mit personenbezogenen Daten kommen, falls diese in die IBM Cloud ausgelagert werden sollen. Seit letztem Jahr bietet IBM auch ein Rechenzentrum in Deutschland (Frankfurt) an, hier muss allerdings auch wieder darauf geachtet werden, dass es möglich wäre, dass US-Behörden dennoch auf diese Daten Zugriff erhalten könnten. IBM stellt die eigenen Service Level Agreements[39] und Nutzerbedingungen[40] online zur Verfügung. Die wichtigsten Punkte der Service Levels sind hier aufgelistet:

- **Serviceerbringung:** Der Kunde darf von jedem beliebigen Standort aus über eine Netzverbindung auf den Cloud-Service zugreifen. Cloud-Services sind bei entsprechender

[38]https://www.gartner.com/newsroom/id/2696317
[39]http://www-03.ibm.com/software/sla/sladb.nsf/pdf/5985-01/$file/i126-5985-01_06-2013_de_DE.pdf
[40]https://www-05.ibm.com/support/operations/files/pdf/csa_de.pdf

Wartung für ständige Verfügbarkeit 24x7 ausgelegt, der Kunde wird über planmäßige Wartungen informiert

◇ **Integrations-, Konfigurations- und Anpassungsservices:** IBM kann zusätzliche Standardanpassungs- und -konfigurationsservices anbieten. Diese Services werden in einer zusätzlichen Servicebeschreibung ausführlich erläutert und können bestellt werden. Auf Anforderung des Kunden kann IBM weitere Anpassungsservices ausführen, die in einer gemeinsam vereinbarten Leistungsbeschreibung enthalten sind

◇ **Vertraulichkeit und Datenschutz:**

– Jeder Cloud Service und die zugehörigen Verfahren und Vorgehensweisen sind dazu ausgelegt, den unternehmenseigenen Inhalt, den der Kunde in den Cloud Service einstellt, zu schützen und den Zugriff auf diesen Inhalt sowie dessen Nutzung nur gemäß den für den Cloud Service geltenden Bestimmungen zu ermöglichen. Sofern nicht anders festgelegt, ist der Zugriff auf die Kundendaten und deren Nutzung innerhalb des Cloud Services durch IBM Mitarbeiter und Auftragnehmer auf das zur Bereitstellung des Services erforderliche Maß beschränkt.

– IBM wird die Kundendaten nicht offenlegen und den Inhalt (einschließlich aller personenbezogener Daten) bei Ablauf oder Kündigung des Cloud Services oder, auf Anforderung des Kunden, zu einem früheren Zeitpunkt zurückgeben oder löschen (bestimmte Maßnahmen können kostenpflichtig sein, z.B. die Bereitstellung des Inhalts in einem speziellen Format)

– IBM informiert den Kunden über unbefugte Zugriffe durch Dritte und behebt mit angemessenem Aufwand die festgestellten Sicherheitslücken. Wenn Kundendaten verloren gehen oder beschädigt werden, unterstützt IBM den Kunden dabei, den Inhalt im Cloud Service von der zuletzt verfügbaren Sicherungskopie des Kunden in einem kompatiblen Format wiederherzustellen

– *Sofern in der Servicebeschreibung nicht ausdrücklich angegeben, ist der Cloud Service* ***nicht*** *für Inhalt ausgelegt, der gesetzlichen Bestimmungen unterliegt oder Sicherheitsmaßnahmen erfordert, die über das in der Servicebeschreibung angegebene Maß hinausgehen. Hierzu gehören sensible personenbezogene Daten und sonstige Daten, deren Verlust die Pflicht zur Anzeige eines Verstoßes gegen die Datensicherheit zur Folge hätte.* Der Kunde erklärt sich damit einverstanden, solchen Inhalt nicht in die Cloud Services einzustellen. Es liegt in der Verantwortung des Kunden, alle erforderlichen Zustimmungen für die Aufnahme des Inhaltes (einschließlich aller personenbezogen Daten) in den Cloud Service einzuholen, und der Kunde erteilt IBM die Genehmigung zur Nutzung, Speicherung und Verarbeitung des Inhalts im Rahmen der Bereitstellung des Cloud Services

– IBM Cloud Services entsprechen dem zwischen den USA und der EU bzw. Schweiz, bestehendem Safe Harbor Abkommen, soweit nichts anderes angegeben. Falls gesetzlich vorgeschrieben werden weitere Vereinbarungen zum Schutz personenbezogener Daten geschlossen. Wenn der Kunde personenbezogene Daten

im Cloud Service und für IBM verfügbar macht, ist der Kunde der alleinige Verantwortliche für diese Daten und beauftragt IBM mit der Verarbeitung dieser Daten (gemäß den Bedingungen der EU Richtlinie 95/46/EG).

- IBM wird personenbezogene Daten nur in dem Umfang verarbeiten, der zur Bereitstellung des Cloud Service erforderlich ist und der Kunde stimmt zu, dass eine solche Verarbeitung seinen Anweisungen entspricht
- Der Kunde erklärt sich damit einverstanden, dass IBM für die Bereitstellung der Cloud-Services Unterauftragsnehmer weltweit, einsetzen kann
- Soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet, kommen die "Ergänzenden Bedingungen für die Verarbeitung von Kundendaten im Auftrag gemäß § 11 BDSG zur Anwendung"

◇ **Haftung:** IBM haftet für Schäden, die durch Verletzung einer in Verbindung mit einem Geschäftsvorgang unter dieser Vereinbarung übernommenen Garantie entstanden sind. Bei leicht fahrlässiger Schadensverursachung haftet IBM, gleich aus welchem Rechtsgrund (einschließlich Ansprüchen aus Vertragsverletzungen sowie unerlaubter Handlung) pro Schadensfall bis zu einem Betrag von 500.000 Euro, oder wenn der Wert des schadensverursachenden Cloud Service höher ist, bis zur Höhe des Preises des schadensverursachenden Cloud Service

◇ **Gewährleistung:** IBM gewährleistet, dass der Cloud Service mit wirtschaftlich angemessener Sorgfalt und Fachkenntnis gemäß der Servicebeschreibung bereitgestellt wird. IBM übernimmt **keine** Gewähr für den unterbrechungs- oder fehlerfreien Betrieb eines Cloud Services

◇ **Gebühren:** Der für IBM SaaS (Business Process Manager on Cloud) zu bezahlende Betrag ist in einem Auftragsdokument angegeben. Folgende Abrechnungsoptionen stehen zur Auswahl: Vorauszahlung der gesamten Gebühr, Monatlich (nachträglich zahlbar), Vierteljährlich (Vorauszahlung), Jährlich (Vorauszahlung)

◇ **Einhaltung von Gesetzen:** Jede Partei bleibt für die Einhaltung von Gesetzen und Verordnungen, die sich auf die Geschäftstätigkeit, die Nutzung eines Cloud Services und den Inhalt beziehen, einschließlich der geltenden Export- und Importgesetze, selbst verantwortlich. Ein Cloud Service wird in dem Land und der auf der Grundlage des dort geltenden Rechtes und des zuständigen Gerichtsstands (unter Ausschluss des Kollisionsrechts) bereitgestellt in dem der Kunde den Cloud Service bestellt hat *(Anmerkung: Bei Abschluss eines Vertrages mit der IBM Deutschland sehen die Vertragsbedingungen die Anwendung des deutschen Rechts vor, allerdings muss beachtet werden das IBM Deutschland trotzdem ein US-Unternehmen ist)*

◇ **Virtual Privat Network (VPN):** Der Kunde kann VPN-Software für eine sichere Verbindung zum IBM SaaS oder für eine in der IBM SaaS-Betriebsumgebung ausgeführte Prozessanwendung verwenden, damit diese mit Systemen im Netz des Kunden kommunizieren kann. Informationen zu VPN werden dem Kunden auf schriftliche Anfrage hin bereitgestellt

- ◇ **Zugriff:** Single-Sign-On mit Security Assertion Markup Language (SAML)
- ◇ **Accountadministrator:** Im Rahmen des IBM SaaS-Angebots wird eine Benutzer-ID einschließlich Kennwort für die Anmeldung bei der Betriebsumgebung als Accountadministrator bereitgestellt. Der Accountadministrator kann den Zugriff der IBM SaaS-Benutzer auf die Betriebsumgebung steuern sowie IBM SaaS-Benutzerrollen zuweisen und löschen. Er kann außerdem weiteren IBM SaaS-Benutzern Administratorrechte erteilen
- ◇ **Sicherung:** Tägliche automatische Onlinesicherungen, IBM SaaS führt eine tägliche Sicherung durch, die im Bedarfsfall zur automatisierten Wiederherstellung von IBM SaaS dient
- ◇ **Export:** Export des kundeneigenen Inhalts Der Kunde kann den in IBM SaaS befindlichen Inhalt zu Speicherzwecken exportieren. Die Speicherposition für den exportierten Inhalt ist frei wählbar und die Speicherkosten trägt der Kunde
- ◇ **Automatisierte Wiederherstellung und Überwachung:** IBM SaaS überwacht die Verfügbarkeit des Service und führt eine Wiederherstellung durch, falls der Service nicht mehr reagiert oder nicht mehr erreichbar ist
- ◇ **Zertifikate:** Folgende Zertifikate hat IBM erhalten[41]:
  - ISO 9001: Qualitätsmanagement
  - ISO 14001[42] & ISO 50001[43]: Umweltmanagementsystem
  - ISO 20000: IT-Service-Management
  - ISO 27001: Informationssicherheits-Managementsystem
  - OHSAS 18001[44]: Arbeitsschutzmanagementsystem

4.1.4.2. Konklusion

Der IBM Business Process Manager on Cloud, bietet viele gute Funktionalitäten Geschäftsprozesse in der Cloud zu evaluieren. Die Sicherheitsstandards sind hoch, diverse ISO-Zertifikate sind vorhanden, Kunden können zusätzliche Sicherheitsprogramme erwerben (kostenpflichtig: z.B. IBM Security Access Manager for Enterprise Single Sign-On). In Bezug auf die Auslagerung von personenbezogenen Daten in die Cloud und den damit zusammenhängenden Gesetzen in Deutschland (BDSG), besteht hier wieder das Problem, dass IBM seinen Hauptsitz in den USA hat, was wie zuvor bereits erwähnt, zu Problemen mit dem deutschen Datenschutz führen könnte. Zwar bietet IBM inzwischen auch Speicherstandorte in Deutschland (Frankfurt) und erklärt, dass ein Cloud Service, in dem Land und zu dessen geltenden

[41] http://www-935.ibm.com/services/us/en/it-services/iso-management-system-certifications.html
[42] http://www.tuev-sued.de/management_systeme/umwelt/iso_140012004
[43] http://www.tuev-sued.de/management-systeme/energiemanagementsysteme/iso-50001
[44] http://www.tuev-sued.de/management_systeme/arbeitsschutz/ohsas_18001

Recht, in dem der Kunde diesen bestellt hat, bereitgestellt wird. Dennoch kann zum heutigen Standpunkt nicht ausgeschlossen werden, dass die Möglichkeit besteht, dass US-Behörden Zugriff auf diese Daten bekommen. Interessant ist hierbei, dass IBM eigenhändig in den AGB für die Cloud Services angibt, dass diese Cloud Services **nicht** für die Verarbeitung von personenbezogenen Daten ausgelegt sind. Falls der Kunde dies dennoch tun möchte, liegt die Verantwortung bei ihm, alle erforderlichen Zustimmungen für die Aufnahme dieser Daten in den Cloud Service, einzuholen. Ebenso muss der Kunde für alle Kosten aufkommen, die IBM entstehen, wenn solche Informationen vom Kunden in die Cloud gestellt werden, einschließlich der Kosten, die sich aus Ansprüchen Dritter ergeben. Aus diesem Grund und auf Basis des Bundesdatenschutzgesetzes zur Verarbeitung von personenbezogenen Daten, kann der IBM Business Process Manager on Cloud (in der Public Cloud) für diese Art von sensiblen Daten, falls z.B. Kundendaten in den Geschäftsprozessen vorkommen, nicht empfohlen werden.

4.1.5. iGrafx Cloud

Die iGrafx GmbH[45] ist Anbieter von Software für Geschäftsprozessmodellierung, -analyse, -simulation und -optimierung, der Hauptsitz für Europa, den Nahen Osten und Afrika befindet sich in Karlsfeld bei München, das amerikanische Headquarter in Portland/USA und der Stammsitz für Asien in Tokio. Die iGrafx Cloud[46] bietet folgende Varianten an:

- ◇ Prozessleser
- ◇ Prozessmodellierer
- ◇ Prozessanalyst
- ◇ Six Sigma- und Lean-Experte
- ◇ Enterprise Modeling-Experte

Alle Produkte der iGrafx Produktsuite sind in der iGrafx Cloud erhältlich:

- ◇ iGrafx for SAP
- ◇ iGrafx for Enterprise Modeling
- ◇ iGrafx Process for Six Sigma
- ◇ iGrafx Process
- ◇ iGrafx Flowcharter

Im Folgenden werden die Antworten aus der Umfrage bezüglich der iGrafx Cloud aufgelistet:

[45]http://www.igrafx.com/de
[46]http://www.igrafx.com/de/products/igrafx-cloud

Frage	Antwort
Allgemein	
Wie lautet der Name der Firma, für die Sie arbeiten?	Keine Angabe
Wie lautet der Name des Produktes, welches Sie bewerten möchten?	iGrafx Cloud
Wird das Produkt von Ihrer Firma hergestellt oder handelt es sich um einen Drittanbieter?	Drittanbieter
Welche Services werden angeboten?	BPMaaS
Security	
Verfügt der Provider über ein ausgereiftes IT-Sicherheitskonzept? (Schutz vor Malware, Abwehr von DDoS-Angriffen)	Ja
Welche Vorkehrungen die ggf. Ausfallzeiten und Datenverlust vorbeugen, stehen zur Verfügung?	Backup, Disaster Recovery, Physikalische Sicherheit
Existiert ein Intrusion Detection System (Angriffserkennungssystem) zur Überwachung der IT-Infrastruktur?	Ja
Ist ein effektives Verschlüsselungs- und Schlüsselmanagement vorhanden, um die Kundendaten und den Datenaustausch sicher zu verschlüsseln?	Ja, AES-256
Ist ein definiertes Vorgehensmodell der firmeninternen IT-Geschäftsprozesse vorhanden?	Ja, ITIL
Werden regelmäßige und unabhängige Prüfungen des IT-Sicherheitszustands, wie z.B. Penetrations-Tests und Audits, vorgenommen?	Sonstiges: Ja
Werden interne Angriffe (d.h. von Kunden auf Kunden) verhindert bzw. entdeckt und effektiv untersucht und unterbunden?	Ja
Compliance	
In welchem Land liegt der Serverstandort?	Keine Angabe
Entspricht die Datenspeicherung von personenbezogenen Daten dem Bundesdatenschutzgesetz?	Keine Angabe
Sind Compliance-Zertifikate vorhanden? Wenn ja welche?	Ja, ISO 27001/27002, SSAE 16 / ISAE 3402
Werden interne Bereiche an Subunternehmer ausgelagert?	Keine Angabe
Werden für Kunden SLA (Service Level Agreements) angeboten?	Ja

Frage	Antwort
Ist es möglich vorhandene SLA (Service Level Agreements) an Kundenwünsche anzupassen?	Ja
Funktionalität	
Ist eine strikte Mandantentrennung in der Cloud vorhanden?	Keine Angabe
Können kurzfristig weitere Kapazitäten hinzugefügt und wieder entfernt werden, falls nötig? (Skalierbarkeit)	Ja
Können Daten mit geringem Aufwand exportiert und zu einem anderen Provider migriert werden?	Keine Angabe
Können offene Formate für den Datenaustausch verwendet werden?	Ja
Findet dieser Datenaustausch verschlüsselt statt? Wenn ja, wo werden die Daten ver- und entschlüsselt bzw. wo liegt der Schlüssel?	Ja
Kann mittels Single Sign-On auf die Kundenserver zugegriffen werden?	Ja
Gibt es eine 2-Faktor-Authentisierung für die Kunden?	Ja
Falls der Kunde „Managed Services“ bevorzugt, existiert hierfür ein effektives Patch- und Änderungsmanagement vorhanden? (z.B. Updates)	Ja
Verfügbarkeit	
Ist für Download/Upload eine ausreichende und unterbrechungsfreie Internetverbindung gewährleistet? (z.B. geringe Latenzzeiten)	Ja
Stehen dem Kunden Alternativen zur Verfügung, falls der Cloud-Service ausfallen sollte? (z.B. redundante Notfall-Server/Komponenten)	Ja
Kann bei einer möglichen Insolvenz des Providers der Schutz und die Verfügbarkeit der Daten gewährleistet werden?	Keine Angabe
Ist der Cloud-Service hochverfügbar? (min. 99,9%)	Ja
Existiert ein ausgeprägter und professioneller Kundensupport?	Ja
Vertrag	
Wie wird der Vertrag geschlossen?	online, schriftlich

Frage	Antwort
Wie werden die für den Vertrag benötigten Personendaten der Kunden überprüft?	Keine Angabe
Wie sehen die Laufzeiten des Vertrages aus?	Sonstiges: verschieden
Besteht bei Vertragskündigung die Möglichkeit die Kundendaten vollständig zu löschen?	Ja
Wie erfolgt die Abrechnung der Services?	Sonstiges: angepasste Abo-Gebühr
Kann der Vertrag angepasst werden, wenn sich die Anforderungen des Kunden ändern?	Ja

Tabelle 4.5.: Auswertung der Umfrage - iGrafx Cloud

4.1.5.1. Eigene Recherche

Die iGrafx GmbH, ist zwar ein in Deutschland angesiedeltes Unternehmen aber laut der Allgemeinen Lizenzvereinbarung[47] ist das anwendbare Recht das Recht des Staates Oregon, wobei die Anwendung kollisionsrechtlicher Vorschriften ausgeschlossen ist. Was bedeutet, dass US-amerikanisches Recht angewandt wird und nicht deutsches oder europäisches, was wiederum zu Problemen mit dem BDSG führen könnte. Des Weiteren bietet iGrafx noch diverse rechtliche Bedingungen[48] an (hauptsächlich auf Englisch). Folgende relevanten Service Levels konnten dementsprechend in Erfahrung gebracht werden:

- **Sicherheit:**
  - 2-Faktor-Authentifizierung
  - 256-bit Datenverschlüsselung
  - SAS 70 und SSAE-16 konform
  - Tägliche Daten-Backups
  - Kostenfreie Software Updates: Keine zusätzlichen Maintenance oder Update-Kosten, alle iGrafx Updates sind inklusive, zudem übernimmt iGrafx auf Wunsch die Konfiguration und Einführung neuer Versionen
- **Support:** 24x7 Support, Den Nutzern der iGrafx Cloud steht ein umfassender IT Support des Cloud Hosting Providers zur Verfügung: 24h Stunden am Tag, 7 Tage die Woche. Das iGrafx Support Team steht Ihnen zudem während der Standard Support Zeiten zur Verfügung

[47] http://www.igrafx.com/assets/pdf/eula/2015_German_iGrafx_LLC_EULA.pdf
[48] http://www.igrafx.com/de/company/legal

- ◇ **Abrechnung:** rollenspezifisch zugeschnittene Werkzeuge für Mitarbeiter, die an Prozessoptimierungs-Initiativen beteiligt sind, Unternehmen können jedem Nutzer Zugriff auf genau die Funktionalität geben die er für seine Aufgabenstellung benötigt, Abonnement kann aus den relevanten Nutzungsszenarien der iGrafx Suite zusammengestellt werden
- ◇ **Weitergabe von Daten an Dritte:** Es ist möglich, dass Kundeninformationen mit Tochtergesellschaften o.ä. von iGrafx weitergegeben werden, diese Gesellschaften unterliegen ebenfalls den Bedingungen der iGrafx Richtlinien. Es werden keine persönlichen Daten an Dritte weitergegeben, ohne die Einwilligung des Kunden
- ◇ **gesetzliche Auskunft:** Auch wenn die Sicherheit der Daten des Kunden einen hohen Stellenwert einnimmt, kann es möglich sein, dass iGrafx persönliche Kundendaten herausgeben muss, Aufgrund von gesetzlichen Bestimmungen. Wobei hier wahrscheinlich ein juristischer Prozess oder eine richterliche Anordnung von Nöten sein wird, um dies zu erreichen
- ◇ **Verschlüsselung:** Datenübertragung z.B. im iGrafx eStore, werden mit SSL/TLS Verschlüsselt, welches eine 128-bit Verschlüsselung unterstützt. Diese Technologie stellt sicher, dass Kundeninformationen sicher über das Internet auf die iGrafx Server gelangen
- ◇ **Datenlöschung:** Wenn Daten nicht mehr benötigt werden, stellt iGrafx sicher, dass die Daten von den Servern gelöscht werden
- ◇ **Haftung:** iGrafx oder seine Lizenzgeber haften in keinem Fall gegenüber dem Kunden für indirekte Schäden, Schadenersatz, besondere Begleit- oder Folgeschäden oder jegliche Schäden durch Nutzungsausfall, Datenverlust oder entgangen Gewinn, die aus oder in Verbindung mit der Lizenzvereinbarung oder der Nutzung oder Ausführung von iGrafx, der Software, Wartung, Datenträgern, Dokumentation oder anderen von iGrafx gelieferten Materialien entstehen, weder vertraglich noch deliktisch (einschließlich, doch nicht begrenzt auf Fahrlässigkeit) und unabhängig davon ob iGrafx über die Möglichkeit solcher Schäden informiert war und gleichgültig, ob diese Schäden vorhersehbar waren oder nicht (iGrafx EULA)

4.1.5.2. Konklusion

Die iGrafx Cloud bietet viele verschiedene Funktionalitäten an (Process Suite) um ein effizientes Geschäftsprozessmanagement in der Cloud zu betreiben. Es sind einige Sicherheitsvorkehrungen vorhanden wie 2-Faktor-Authentifizierung oder 256-bit-Verschlüsselung, die Cloud soll SAS 70 und SSAE-16 konform betrieben werden und tägliche Backups sind vorhanden.

Allerdings wären weitere ISO-Zertifikate von Vorteil und es konnte nicht in Erfahrung gebracht werden, wo sich der Serverstandort befindet, auf dem Kundendaten von Kunden aus Deutschland gespeichert werden. Es gibt zwar einen Sitz der Firma in München, aber ob die Daten auch dort gespeichert werden ist unklar. Da in den Lizenzbedingungen von

iGrafx folgendes angegeben wurde:*"Anwendbares Recht ist das Recht des Staates Oregon, wobei die Anwendung kollisionsrechtlicher Vorschriften ausgeschlossen ist"*, lässt sich folgern, dass auch dieses Unternehmen an US-Amerikanisches Recht gebunden ist und es nicht ausgeschlossen werden kann, dass auch Kundendaten innerhalb Europas von US-Behörden angefordert werden können.

Somit ist die iGrafx Cloud für deutsche Firmen die sensible personenbezogene Daten in die Public Cloud auslagern wollen, vom jetzigen Standpunkt aus, nicht zu empfehlen.

4.1.6. ADONIS:Cloud

Die BOC Information Technologies Consulting GmbH[49] wurde 1995 von o. Univ. Prof. Dr. Dimitris Karagiannis in Wien als Spin-Off der BPMS- (Business Process Management Systems) Gruppe der Abteilung Knowledge Engineering der Universität Wien gegründet. Sie ist im Bereich IT-gestützter Managementwerkzeuge tätig und bietet Beratungsservices in den Bereichen Strategie-, Geschäftsprozess- und IT-Management an. Ausgehend von dem Hauptsitz in Wien und weiteren Gesellschaften in Deutschland, Griechenland, Irland, Österreich, Polen, Spanien und der Schweiz ist die BOC Gruppe weltweit tätig. Die Produkte aus dem BOC Management Office, hier insbesondere das Geschäftsprozessmanagement Toolkit ADONIS und das IT-Architektur- und Servicemanagement Toolkit ADOit, sind unter anderem in Großkonzernen und KMUs zu finden.

Die ADONIS:cloud steht als Software as a Service (SaaS) in einer Public Cloud zur Verfügung und bietet folgende Funktionalitäten für Geschäftsprozesse:

- ◇ Modellierung
- ◇ Analyse
- ◇ Publikation

Im Folgenden werden die Antworten aus der Umfrage bezüglich der ADONIS:Cloud aufgelistet:

Frage	**Antwort**
Allgemein	
Wie lautet der Name der Firma, für die Sie arbeiten?	Keine Angabe
Wie lautet der Name des Produktes, welches Sie bewerten möchten?	Cloud BPM Adonis
Wird das Produkt von Ihrer Firma hergestellt oder handelt es sich um einen Drittanbieter?	Drittanbieter
Welche Services werden angeboten?	SaaS und BPMaaS

[49]http://www.boc-group.com/de/gruppe/

Frage	Antwort
Security	
Verfügt der Provider über ein ausgereiftes IT-Sicherheitskonzept? (Schutz vor Malware, Abwehr von DDoS-Angriffen)	Ja
Welche Vorkehrungen die ggf. Ausfallzeiten und Datenverlust vorbeugen, stehen zur Verfügung?	Backup, Physikalische Sicherheit
Existiert ein Intrusion Detection System (Angriffserkennungssystem) zur Überwachung der IT-Infrastruktur?	Ja
Ist ein effektives Verschlüsselungs- und Schlüsselmanagement vorhanden, um die Kundendaten und den Datenaustausch sicher zu verschlüsseln?	Sonstiges: Ja
Ist ein definiertes Vorgehensmodell der firmeninternen IT-Geschäftsprozesse vorhanden?	Keine Angabe
Werden regelmäßige und unabhängige Prüfungen des IT-Sicherheitszustands, wie z.B. Penetrations-Tests und Audits, vorgenommen?	Sonstiges: Ja, regelmäßig
Werden interne Angriffe (d.h. von Kunden auf Kunden) verhindert bzw. entdeckt und effektiv untersucht und unterbunden?	Ja
Compliance	
In welchem Land liegt der Serverstandort?	Schweiz
Entspricht die Datenspeicherung von personenbezogenen Daten dem Bundesdatenschutzgesetz?	Ja
Sind Compliance-Zertifikate vorhanden? Wenn ja welche?	Ja, ISO 27001/27002 Sonstiges: Safe Harbor
Werden interne Bereiche an Subunternehmer ausgelagert?	Ja, Iaas cloudsigma
Werden für Kunden SLA (Service Level Agreements) angeboten?	Ja
Ist es möglich vorhandene SLA (Service Level Agreements) an Kundenwünsche anzupassen?	Ja
Funktionalität	
Ist eine strikte Mandantentrennung in der Cloud vorhanden?	Ja

Frage	Antwort
Können kurzfristig weitere Kapazitäten hinzugefügt und wieder entfernt werden, falls nötig? (Skalierbarkeit)	Ja
Können Daten mit geringem Aufwand exportiert und zu einem anderen Provider migriert werden?	Keine Angabe
Können offene Formate für den Datenaustausch verwendet werden?	Sonstiges: Verlustfreier Datenaustausch zwischen unterschiedlichen GPM-Tools
Findet dieser Datenaustausch verschlüsselt statt? Wenn ja, wo werden die Daten ver- und entschlüsselt bzw. wo liegt der Schlüssel?	Ja
Kann mittels Single Sign-On auf die Kundenserver zugegriffen werden?	Ja
Gibt es eine 2-Faktor-Authentisierung für die Kunden?	Keine Angabe
Falls der Kunde „Managed Services“ bevorzugt, existiert hierfür ein effektives Patch- und Änderungsmanagement vorhanden? (z.B. Updates)	Ja
Verfügbarkeit	
Ist für Download/Upload eine ausreichende und unterbrechungsfreie Internetverbindung gewährleistet? (z.B. geringe Latenzzeiten)	Ja
Stehen dem Kunden Alternativen zur Verfügung, falls der Cloud-Service ausfallen sollte? (z.B. redundante Notfall-Server/Komponenten)	Ja
Kann bei einer möglichen Insolvenz des Providers der Schutz und die Verfügbarkeit der Daten gewährleistet werden?	Keine Angabe
Ist der Cloud-Service hochverfügbar? (min. 99,9%)	Sonstiges: 99%
Existiert ein ausgeprägter und professioneller Kundensupport?	Ja
Vertrag	
Wie wird der Vertrag geschlossen?	online
Wie werden die für den Vertrag benötigten Personendaten der Kunden überprüft?	Keine Angabe
Wie sehen die Laufzeiten des Vertrages aus?	Sonstiges: 3-Monatige Kündigungsfrist

Frage	Antwort
Besteht bei Vertragskündigung die Möglichkeit die Kundendaten vollständig zu löschen?	Sonstiges: Löschung nach 6 Monaten Aufbewahrungsfrist
Wie erfolgt die Abrechnung der Services?	pauschal
Kann der Vertrag angepasst werden, wenn sich die Anforderungen des Kunden ändern?	Ja

Tabelle 4.6.: Auswertung der Umfrage - ADONIS:Cloud

4.1.6.1. Eigene Recherche

Die BOC Gruppe mit Hauptsitz in Österreich (Wien) bietet die ADONIS:Cloud als Software as a Service in einer Public Cloud oder einer Private Cloud zur Verfügung. BOC nutzt die notwendige Infrastruktur as a Service (IaaS) vom Cloud Service Provider CloudSigma[50]. Dieser Provider hat seinen Sitz in der Schweiz.

Die Schweiz gehört momentan zu den Staaten denen die Europäische Kommission durch eine sogenannte Angemessenheitsentscheidung attestiert hat, dass die Schweiz ein angemessenes Datenschutzniveau gewährleistet (§ 4 Abs. 2 Satz 2 BDSG), somit entstehen keine Probleme mit der Auslagerung von personenbezogenen Daten in die Cloud. Folgende Service Levels konnten ermittelt werden (SLA[51] und AGB[52]) und die wichtigsten werden hier aufgelistet:

- ◇ **Serverstandort:** IaaS-Provider: Cloudsigma AG, Glattbrugg, (Kanton Zürich, Schweiz), ISO27001-zertifiziertes Datenzentrum, Serverstandort: Schweiz
- ◇ **Lizenzierung:** ADONIS:cloud wird mit Designer-Lizenzen für Modellierer und Leser-Lizenzen angeboten. Es wird jeweils pro Benutzer lizenziert (Named Use). Die Cloud wird aktuell in zwei Editionen angeboten: Stratus Edition und Cirrus Edition. Diese Editionen unterstützen unterschiedliche Szenarien und beinhalten unterschiedliche Funktionen. Die Cirrus Edition beinhaltet die Szenarien und Funktionen der Stratus Edition und mehr
- ◇ **Kosten:** ADONIS:cloud wird vierteljährlich basierend auf einer monatlichen Nutzungsgebühr verrechnet. Designer-Lizenzen werden ab 69,00 EUR (pro Monat und Benutzer, Stratus) und Leser-Lizenz-Pakete ab 40,00 EUR (pro Monat und 25 Benutzer, Stratus) angeboten
- ◇ **Kündigung:** ADONIS:cloud kann mit Wirksamkeit zum Ende jedes Quartals gekündigt werden. Die Kündigungsfrist beträgt 3 Monate. Nach Beendigung des Service werden alle modellierten Daten exportiert und für eine maximale Dauer von 6 Monaten

[50]https://www.cloudsigma.com
[51]http://www.boc-group.com/fileadmin/cloud/Nutzungsbedingungen_ADONIScloud_(01.08.2014).pdf
[52]http://www.boc-group.com/fileadmin/media/downloads_free/de/AGB%20der%20BOC%20Gruppe%20(01.01.2014).pdf

aufbewahrt. Innerhalb dieser Frist werden diese Daten dem Kunden auf Anfrage zum Download zur Verfügung gestellt. Sollte der Kunde seinen ADONIS:cloud-Zugang innerhalb dieser Frist reaktivieren, so können die modellierten Daten auf Wunsch wieder importiert werden. Nach Ablauf dieser Frist werden alle modellierten Daten unwiderruflich gelöscht.

- ◇ **Sicherung:** Es werden von den ADONIS:cloud Datenbanken tägliche Sicherungskopien (Backups) angelegt. Die Aufbewahrungsdauer der täglichen Sicherungskopien ist 14 Tage, Lokation der Backup-Daten: Deutschland/Europäische Union
- ◇ **Verfügbarkeit:** Generell: 24/7/365, erwartete Service Verfügbarkeit: 99% Verfügbarkeit innerhalb der definierten Service-Verfügbarkeit: Montag – Freitag, 08.00-18.00 CET (ausgenommen angekündigte Wartungsfenster und österreichische Feiertage)
- ◇ **Support:** Es steht ein Hotline-Support von Montag – Freitag, 08.00-18.00 CET (ausgenommen österreichische Feiertage) zur Verfügung
- ◇ **Reaktionszeit:** Für Incidents und Service-Anfragen:
  - Betriebsverhindernde Incidents - hohe Priorität: 2 Stunden
  - Betriebsbehindernde Incidents - mittlere Priorität: 4 Stunden
  - Geringe Störungen - niedrige Priorität: 8 Stunden
  - Für alle gilt: innerhalb der Hotline-Verfügbarkeit
- ◇ **Lösungszeiten:** Für Incidents:
  - Betriebsverhindernde Incidents: 1 Arbeitstag
  - Betriebsbehindernde Incidents: 2 Arbeitstage
  - Geringe Störungen: 4 Arbeitstage
  - Für alle gilt: innerhalb der Hotline-Verfügbarkeit
- ◇ **Bearbeitungszeiten:** Für Service-Anfragen:
  - Hohe Priorität: 1 Arbeitstag
  - Mittlere Priorität: 2 Arbeitstage
  - Niedrige Priorität: 4 Arbeitstage
  - Für alle gilt: innerhalb der Hotline-Verfügbarkeit
- ◇ **Datenschutz und Geheimhaltung:**

- Allgemein: Es besteht wechselseitiges Einvernehmen darüber, dass alle ausgetauschten Informationen streng vertraulich sind und nur jenen Personen zugänglich gemacht werden dürfen, welche im Rahmen der Umsetzung dieses Vertrags Zugang haben müssen. Diese Mitarbeiter werden über die Vertraulichkeit der Informationen unterrichtet. Die Weitergabe von vertraulichen Informationen an externe Berater und sonstige Personen ist der jeweils anderen Seite im Vorhinein schriftlich mitzuteilen
- Erhebung und Verarbeitung kundenbezogener Daten: Alle von BOC verwendeten personenbezogenen Daten werden nur im gesetzlichen Rahmen erhoben, verarbeitet und genutzt. *Sollte BOC dazu Software oder Services von Drittanbietern nutzen, die nicht europäischem Recht unterliegen, so achtet BOC grundsätzlich darauf, dass die Bestimmungen der Safe Harbor Vereinbarung eingehalten werden.* BOC verwendet ausschließlich personenbezogene Daten, die uns vom Kunden aktiv mitgeteilt werden, oder sich aus der Kundenbetreuung heraus ergeben. Diese Daten verwendet BOC für:
  - Vertragsabwicklung
  - Zahlungsabwicklung
  - Bearbeitung von Kundenanfragen
  - Übermittlung von Produkt-, Service-, Veranstaltungsinformationen
- Zur Leistungserbringung sowie Zahlungsabwicklung setzt BOC fallweise Dienstleister ein, denen unbedingt erforderliche personenbezogene Daten zur Verfügung gestellt werden. Diese Dienstleister haben sich vertraglich dazu verpflichtet, diese Daten ausschließlich
  - ausschließlich zur Auftragserfüllung zu nutzen,
  - insbesondere nicht zu eigenen Zwecken zu nutzen,
  - nach erfolgter Auftragserfüllung zu löschen sowie nicht an Dritte weiterzugeben

◇ **Datensicherheit:**

- BOC trifft angemessene organisatorische und technische Maßnahmen, um die BOCWebseite und sonstige Systeme gegen Verlust, Zerstörung, Zugriff, Veränderung oder Verbreitung von Daten durch unbefugte Personen zu schützen. Personenbezogene Daten werden über eine sichere Verbindung über das Internet übertragen
- Für die zweckmäßige Absicherung anwendungsbezogener Daten sowie die Durchführung adäquater Datensicherungen und Updates ist der Kunde verantwortlich, sofern die Datensicherung nicht Gegenstand einer Betriebsservicevereinbarung ist. Eine Haftung seitens BOC für Datenverluste ist, sofern diese nicht in einer Betriebsservicevereinbarung ausdrücklich schriftlich unter Regelung der beide

Seiten treffenden Mitwirkungspflichten und Definition einer Haftungsobergrenze vereinbart wird, in jedem Fall ausgeschlossen

- BOC stellt dem Kunden Installationshinweise sowie erweiterte Softwaredokumentationen zur Verfügung. Dies bedeutet jedoch keine Haftungsübernahme durch BOC für Schäden durch Datenverlust oder Sicherheitslücken

◇ **Haftung:**

- Beide Vertragsparteien haften nicht für reine Vermögensschäden, Verlust oder Beschädigung aufgezeichneter Daten, entgangenen Gewinn, erwartete aber nicht eingetretene Ersparnisse sowie Schäden aus Ansprüchen Dritter gegenüber dem Kunden
- Beide Vertragsparteien haften wechselseitig unbeschränkt bei Vorsatz oder grober Fahrlässigkeit sowie bei leichter Fahrlässigkeit im Fall der Verletzung des Lebens, des Körpers oder der Gesundheit
- Darüber hinaus haften die Vertragsparteien nur, sofern ein Verstoß gegen eine wesentliche Bestimmung des gegenständlichen Vertrags vorliegt. Die Höhe der Haftung ist für jedes schadensverursachende Ereignis insgesamt auf den Auftragswert begrenzt

◇ **Vertrag:** Jeder Vertrag zwischen den Vertragsparteien bedarf zu seiner Wirksamkeit der Schriftform, sowie der schriftlichen Unterfertigung durch beide Vertragsparteien. Auch ein Abgehen von diesem Formerfordernis unterliegt denselben Formerfordernissen

◇ **Anwendbares Recht und Gerichtsstand:**

- Auf die gesamte Vertragsbeziehung zwischen dem Kunden und BOC einschließlich dieser AGB findet das Recht des Sitzstaates der BOC Gesellschaft Anwendung, mit der der Kunde in Vertragsbeziehung steht. Die Anwendung des UN-Kaufrechtes und der Kollisionsregeln nach dem internationalen Privatrechtsgesetz des jeweiligen Landes wird ausgeschlossen
- Für Streitigkeiten aus oder im Zusammenhang mit der Geschäftsbeziehung zwischen dem Kunden und BOC wird die Zuständigkeit des sachlich für Handelsgerichtsbarkeit zuständigen Gerichtes am Sitz der BOC-Gesellschaft vereinbart, mit der der Kunde in Vertragsbeziehung steht

Da die ADONIS:Cloud bei einem externen Provider gehostet wird (CloudSigma[53]), wird dieser hier ebenfalls analysiert. Betrachtet wird der Hauptstandort des Providers, der sich in Zürich (Schweiz) befindet (Rechenzentrum ZH4 IBX/ZH5). Alle Rechenzentren von CloudSigma erfüllen mindestens ein Tier III[54] oder eine vergleichbare Rechenzentrumseinstufung. Die wichtigsten Daten werden hier aufgelistet:

Hauptstandort der Schweizer Cloud ZH4 IBX:

[53]https://www.cloudsigma.com/de/infrastrukturstandorte
[54]http://uptimeinstitute.com/TierCertification/allCertifications.php?page=1&ipp=All

- ◇ **Strom:** Elektrische Kapazität: 1.0kVA/m^2, Anzahl der Versorgungszulieferer: 2, Anzahl der Netztransformatoren: Zwei Netztransformatoren bei 2,5 MVA, Versorgungsspannung: Zwei 11 kV (seit Ende 2011). Zwei 22 kV (nach dem Upgrade), Stand-by-Leistungskonfiguration: Drei Dieselmotorgeneratoren von 1.600 kVA
- ◇ **Gebäude:** Gebäudeart: Beton- und Stahlrahmenkonstruktion, Bodenbelastungsfähigkeit: 32 psf (1.5 kN/m^2), Bodenart: Antistatische Stahlfliesen, 600 x 600 mm, und ein Doppelboden von 400 mm/4,5 kN, Platte/Höhe zur Decke: 2600 mm
- ◇ **Zertifikate:** Kopien aller Zertifikate sind auf Anfrage erhältlich: ISO 9001, ISO 27001, SSAE16 / ISAE 3402 (überprüft), PCI DSS-zertifiziert[55]
- ◇ **Sicherheit:** Physisch: Proximity-Lesegeräte für Kartenzugang, Personen: 24-Stunden-Sicherheitspersonal an 7 Tagen die Woche, Elektronik: Biometrische Lesegeräte an kritischen Zugängen, 24-Stunden-Überwachung an sieben Tagen die Woche, digitale Videoüberwachung
- ◇ **Brandschutz:** Brandunterdrückung: Digital adressierbare Punkterkennung, automatisches High Fog-System

Zweiter Standort in Zürich ZH5, der für hohe Verfügbarkeit genutzt wird. Die ZH5-Infrastruktur ist mit unbeschalteten 10-Gbit/s-Doppelglasfasern verbunden (unabhängig geroutet) und befindet sich in einem separaten Versicherungsbereich von ZH4 und bietet eine leistungsstarke Disaster-Recovery oder ein Setup mit hoher Verfügbarkeit

- ◇ **Strom:** Elektrische Kapazität: bis zu 12 kVA pro Schrank, Anzahl der Versorgungszulieferer: Zwei eingehende Feeds, Netztransformatoren: Sieben Transformatoren bei Fertigstellung, Versorgungsspannung: 20MV, Stand-by-Leistungskonfiguration: Generatoren, mit 36-Stunden-Brennstoffautonomie vor Ort, während des Einsatzes nachfüllbar und durch einen 24-Stunden-Vertrag unterstützt
- ◇ **Gebäude:** Gebäudeart: Verstärkte Betonstruktur mit externer Verkleidung, Bodenbelastungsfähigkeit: 12.5kN/m^2, Bodenart: Fliesen, 600 x 600 mm, mit einer Punktbelastbarkeit von 4,5 kN und strapazierfähige 800-mm-Doppelbodensysteme, Platte/Höhe zur Decke: Phase 1: Platte zur Decke: 3,7 m (Platte zum Doppelboden: 0,8 m und Doppelboden zur Decke: 2,9 m) Phase 2: Platte zur Decke: 5 m (Platte zum Doppelboden: 0,8 m und Doppelboden zur Decke: 4,2 m)
- ◇ **Zertifikate:** Kopien aller Zertifikate sind auf Anfrage erhältlich: ISO 9001, ISO 27001, SSAE16 / ISAE 3402 (überprüft), PCI DSS-zertifiziert
- ◇ **Sicherheit:** Physisch: Empfang aus ballistischem Glas, Schleuse und mannshohe Drehkreuze am Ein- und Ausgang, Personen: 24-Stunden-Sicherheitspersonal an 7 Tagen die Woche, Elektronik: 24-Stunden-Überwachung an sieben Tagen die Woche, digitale Videoüberwachung, biometrischer Handflächenscanner, Zugang mit Lichtbildausweis und Einbruchmeldeanlage

[55]https://de.pcisecuritystandards.org/minisite/en/

- ◇ **Brandschutz:** Brandunterdrückung: Ansaugsystem mit mehreren Zonen, adressierbares analoges Punkterkennungssystem, hochdichter Wassernebel mit lokalisiertem Betrieb.
- ◇ **Datenschutz:** Gespeicherte Daten werden mit 256bit AES-TLX verschlüsselt, alle Daten verbleiben auf den CloudSigma Servern und unterliegen den Schweizer Gesetzen

4.1.6.2. Konklusion

Die ADONIS:Cloud bietet einen guten und effizienten Weg BPM in der Public Cloud zu betreiben, zudem besitzt sie einen hohen Sicherheitsstandard, inklusive des Providers CloudSigma aus der Schweiz. Die Informationen zu diversen Zertifikaten und Sicherheitsbestimmungen auf Providerseite sind öffentlich zugänglich und detailliert.

Da der Serverstandort in der Schweiz liegt und diese von der EU Kommission als Staat mit ausreichendem Datenschutzniveau angesehen wird, können auch personenbezogene Daten in diese Cloud ausgelagert werden, ohne in Konflikt mit dem BDGS - in Bezug auf Auftragsdatenverwaltung im außereuropäischen Raum - zu kommen.

Allerdings erwähnt die BOC Gruppe in den AGB, dass die Möglichkeit besteht, dass Software oder Services von Drittanbietern genutzt werden, die nicht dem europäischen Recht unterliegen. Zwar gibt BOC an, dass wenn dies der Fall ist, diese Drittanbieter sich an die Bestimmungen der Safe Harbor Vereinbarung halten werden. Die Tatsache, dass Drittanbieter, die nicht an Europäisches Recht gebunden sind, möglicherweise Zugriff auf sensible Kundendaten haben, mindert das hohe Datenschutzniveau der ADONIS:Cloud, denn es kann somit nicht ausgeschlossen werden, dass personenbezogene Daten außerhalb der EU/EWR bearbeitet werden.

Aus diesem Grund kann die ADONIS:Cloud (Public Cloud) zur Bearbeitung von sensiblen Daten in Geschäftsprozessen nicht uneingeschränkt empfohlen werden. Sollten die vorher erwähnten Drittanbieter ausschließlich dem europäischen Recht unterliegen, wäre die ADONIS:Cloud durchaus sehr gut für die Auftragsdatenverarbeitung von personenbezogenen Daten geeignet.

Kapitel 5.

Sicherheit und Datenschutz

In diesem Abschnitt wird auf die Regelungen des deutschen Datenschutzgesetzes im Inland und außereuropäischen Regionen, in Bezug auf die Speicherung von personenbezogenen Daten in der Cloud, eingegangen und erläutert.

5.1. Sicherheit und Datenschutz bei Geschäftsprozessen

Wo werden Kundendaten gespeichert? Wer hat Zugriff auf diese Daten? Sind sie sicher vor Missbrauch? Eines der großen Probleme beim Cloud Computing besteht darin, die Integrität und Vertraulichkeit der Datenverarbeitung des Cloud-Nutzers zu gewährleisten. Aus Sicht des Bundesdatenschutzgesetzes sind dessen Regelungen im Zusammenhang mit dem Cloud Computing nur dann anwendbar, wenn personenbezogene Daten, d.h. wenn die verarbeiteten Einzelangaben einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, im Inland (Ort der Datenverarbeitung) erhoben, verarbeitet oder genutzt werden (§1, 3 BDSG). Betroffene können Mitarbeiter, Kunden oder Lieferanten des Cloud-Nutzers sein, deren personenbezogene Daten an den Cloud-Anbieter übermittelt werden.

5.1.1. Auftragsdatenverarbeitung

Beim Cloud Computing handelt es sich, nach allgemeiner Auffassung, als eine Form des Outsourcings und um sog. Auftragsdatenverarbeitung (§ 11 BDSG). Der Auftragnehmer (Provider) trägt somit keine eigene Verantwortung für die Verarbeitung der Daten, der Auftraggeber (Cloud-Nutzer) bleibt datenschutzrechtlich verantwortlich für die Daten, solange die Datenspeicherung innerhalb der EU bzw. des EWR stattfindet. Keine Auftragsdatenverarbeitung ist gegeben, wenn ein Empfänger ein Dritter ist. Dies ist nach § 3 Abs. 8 S. 2 BDSG jede Stelle außerhalb des Inlands bzw. außerhalb eines Mitgliedstaates der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes (EWR). In diesem Fall kann die Privilegierung der Datenverarbeitung nach § 11 BDSG nicht in Anspruch genommen werden.[1] Eine solche Übermittlung von Daten ist aber nur dann zulässig, wenn es dafür eine

[1] https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html

Rechtsgrundlage gibt. Eine zulässige Datenübermittlung ins Dritt(aus)land außerhalb des EWR an einen Cloud-Anbieter ist aber eventuell möglich wenn folgende Punkte eingehalten werden:

- ◇ wenn in den Drittstaaten ein angemessenes Datenschutzniveau besteht (§ 4b Abs. 2, 3 BDSG). Dies wurde für bestimmte Staaten durch die EU-Kommission festgestellt, z.B. für die Schweiz, Kanada oder Argentinien.
- ◇ wenn die von der Europäischen Kommission zur Verfügung gestellten „Standardvertragsklauseln für die Übermittlung von Daten in Drittländer" vereinbart werden
- ◇ wenn der Cloud-Anbieter in den USA seinen Sitz hat und sich den sog. „Safe Harbor Principles", einschließlich den sog. „Frequently Asked Questions", verpflichtet hat
- ◇ wenn eine verbindliche Unternehmensregelung nach § 4 c Abs. 2 S. 1 BDSG zwischen den an der Cloud beteiligten Unternehmen getroffen wird (sog. Corporate Binding Rules) und diese durch die zuständige Datenschutzbehörden genehmigt wurde[2]

Diese Unzulässigkeit der Übermittlung von personenbezogenen Daten in Drittländer hat dazu geführt, dass einzelne Cloud-Anbieter den Nutzern die Möglichkeit einräumen, eine Datenverarbeitung ausschließlich innerhalb des EWR durchführen zu lassen. Einige große Cloud-Anbieter wie z.B. Microsoft[3] bieten Serverstandorte in verschiedenen Regionen an, wie z.B. Nord- und Westeuropa (Irland und Niederlande). Allerdings schließt Microsoft in seiner Policy nicht vollständig aus, dass Kundendaten außerhalb Europas gespeichert werden. Hier ein Auszug aus den Datenschutzrichtlinien von Microsoft Azure (Stand November 2014):

Microsoft überträgt keine Kundendaten an Standorte außerhalb der geografischen Räume, die der Kunde angibt (Beispiel von Europa nach USA oder von USA nach Asien), es sei denn, dies ist für Microsoft erforderlich, um Kundensupport bereitzustellen, ein Problem mit dem Dienst zu beheben, rechtliche Bestimmungen einzuhalten oder wenn der Kunde eine derartige Übertragung von Kundendaten bei der Konfiguration des Kontos aktiviert, auch durch Verwendung von:

- ◇ *Features, die keine Auswahl des geografischen Raums ermöglichen, wie etwa das Content Delivery Network (CDN), das einen weltweiten Caching-Dienst anbietet*
- ◇ *Web- und Workerrollen, die Softwarebereitstellungspakete unabhängig vom geografischen Bereitstellungsraum in den USA sichern*
- ◇ *Vorschau-, Beta- oder andere Features vor der Veröffentlichung, die Kundendaten möglicherweise unabhängig vom geografischen Bereitstellungsraum in den USA speichern oder dorthin übertragen: Azure Active Directory (außer für Access Control) darf Active Directory-Daten für Europa in die USA übertragen und für Asien, Japan und Brasilien, außer für die USA (hier bleiben Active Directory-Daten in den USA), weltweit speichern. Bei der Multi-Factor Authentication von Azure werden die Authentifizierungsdaten in den USA gespeichert. Azure*

[2]http://www.it-recht-kanzlei.de
[3]http://azure.microsoft.com/de-de/support/trust-center/privacy/

RemoteApp darf abhängig davon, von wo der Benutzer auf den Dienst zugreift, die Namen und IP-Adressen der Endbenutzer weltweit speichern.

Existiert im Drittstaat kein angemessenes Datenschutzniveau, können die Daten unter Umständen auch dann übermittelt werden, wenn die Betroffenen der Übermittlung ausdrücklich zugestimmt haben. Wobei man in der Praxis, die Einwilligung der betroffenen Person einzuholen, schnell an Grenzen stößt. Eine solche Einwilligung ist nur dann rechtswirksam, wenn diese freiwillig und grundsätzlich schriftlich gegeben worden ist. Im Geschäftsbetrieb ist es selten möglich von jedem Betroffenen eine schriftliche Einwilligung zu erhalten, dass dieser der Speicherung seiner Daten außerhalb der EU zustimmt. Folgendes wurde im BDSG gesetzlich geregelt:

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. (§ 4 BDSG)

Für Unternehmen bedeutet dies, vor dem Abschluss genau zu prüfen, was der Vertrag dazu sagt, wo die Daten verarbeitet werden. Denn viele dieser Verträge enthalten keine ausreichenden Regelungen zu einem Verbleib der Daten innerhalb des EWR und manche lassen den Datenexport sogar ausdrücklich zu. Ein deutsches Unternehmen sollte einen solchen Vertrag nicht abschließen wenn personenbezogene Daten in die Cloud ausgelagert werden sollen, denn er führt zu einem Bußgeld, weil er eindeutig die Bestimmungen des § 11 BDSG verletzt[4].

Aktuell läuft in den USA ein Verfahren gegen Microsoft, in welchem eine US-Bundesrichterin darauf besteht, dass Microsoft E-Mail-Daten (Nutzerdaten), die auf einem ihrer Server in Irland liegen, herausgeben muss. Microsoft hat das New Yorker Urteil auch auf Drängen der Bundesregierung angefochten. Für die amerikanischen Internet-Unternehmen könnte es ein problematischer Präzedenzfall werden, falls Microsoft die in Europa gespeicherten Daten herausgeben muss[5].

5.2. Interkulturelle Unterschiede und Regelungen

Wie bereits im vorherigen Absatz erwähnt, gibt es verschiedene Möglichkeiten personenbezogene Daten in ein Drittland wie z.B. USA auszulagern, wenn bestimmte Regelungen eingehalten werden. Hier werden die wichtigsten interkulturellen Vereinbarungen aufgelistet und analysiert.

[4]http://www.rechtsanwalt.de/auftragsdatenverarbeitung
[5]http://www.heise.de/newsticker/meldung/US-Zugriff-auf-EU-Rechenzentrum-Microsoft-bekommt-Aufschub-2281428.html

5.2.1. EU-Standardvertragsklauseln für die Übermittlung von Daten in Drittländer

Zur Anpassung an neue Geschäftsmodellen und wegen der die zunehmenden Globalisierung und Auslagerung von Datenverarbeitungstätigkeiten hat die Europäische Kommission Anfang Februar 2010 die so genannten „Standardvertragsklauseln“ aktualisiert. Die EU-Standardvertragsklauseln[6] regeln die Übermittlung von personenbezogenen Daten an Auftragsverarbeiter außerhalb der Europäischen Union. Wenn ein Unternehmen mit Sitz in der EU als Exporteur von personenbezogen Daten an ein Unternehmen außerhalb der EU und des EWR übermittelt und von diesem speichern, nutzen oder verarbeiten lässt, muss der Exporteur ein “angemessenes Datenschutzniveau” beim Importeur sicherstellen. Schließen der Datenexporteur in der EU und der Datenimporteur außerhalb der EU/EWR einen Vertrag mit den Standardvertragsklauseln der EU-Kommission, so ist damit automatisch ein angemessenes Datenschutzniveau beim Importeur sichergestellt.[7] Allerdings muss hier beachtet werden, dass die Vertragsklauseln nur unverändert dieses Datenschutzniveau herstellen. Falls Klauseln abgeändert werden oder individuelle Klauseln eingesetzt werden, muss erst eine aufsichtsbehördliche Genehmigung eingeholt werden.

Eine der wichtigsten Neuregelungen für die Praxis und insbesondere für das Cloud Computing ist, die Möglichkeit, auf Seiten des Auftragnehmers, die empfangen Daten seinerseits wiederum an Subunternehmer auszulagern, sofern der Auftraggeber (Kunde) dem schriftlich eingewilligt hat und dem Unter-Auftragsdatenverarbeiter (Subunternehmer) die gleichen Pflichten auferlegt werden, die auch der originäre Auftragnehmer (Provider) erfüllen muss. Verletzt der Subunternehmer seine Datenschutzpflichten (nach EU-Standardvertragsklauseln), ist der Auftragnehmer gegenüber dem Kunden uneingeschränkt für die Erfüllung der Pflichten des Subunternehmers verantwortlich.

Auszug aus den EU-Standardvertragsklauseln von 2010:

Klausel 11 Vergabe eines Unterauftrags:

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss (1). Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

Die Klauseln sollen den Schutz persönlicher Daten auch dann sicherstellen, wenn Unternehmen personenbezogenen Daten an andere Unternehmen außerhalb der EU zur Weiterverarbeitung transferieren. Diese Standardvertragsklauseln finden allerdings nur dann

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF
[7] http://www.praxis-it-recht.de/

Anwendung wenn der Auftragnehmer (Provider) außerhalb der EU seinen Sitz hat. Wenn der Provider in der EU ansässig ist und nur der Subunternehmer (falls vorhanden) in einem Drittland ist, sind die Klauseln nicht anwendbar.

5.2.2. Safe Harbor

Bei Safe Harbor[8] (Sicherer Hafen) handelt es sich um eine zwischen der EU (Europäischen Union) und den USA (Vereinigte Staaten von Amerika) im Jahre 2000 getroffene Vereinbarung, die gewährleistet, dass personenbezogene Daten legal in die USA übermittelt werden können. Ausgangspunkt für diese Vereinbarung bilden die Vorschriften der Art. 25 und 26 der Europäischen Datenschutzrichtlinie[9], nach denen ein Datentransfer in Drittstaaten verboten ist, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da es dort keine umfassenden gesetzlichen Regelungen zum Datenschutz gibt, die dem europäischen Standard entsprechen. Allerdings sieht Art. 25 Abs. 6 der Richtlinie vor, dass die Kommission der Europäischen Gemeinschaft die Angemessenheit des Datenschutzes in einem Drittland feststellen kann, wenn dieses bestimmte Anforderungen erfüllt.[10]

Die vereinbarten Regelungen richten sich ausschließlich an Unternehmen mit Sitz in den USA. Wegen eines fehlenden Datenschutzniveaus in den USA, bestand die Gefahr, dass die Datentransfers nach Amerika zerrüttet werden könnten. Um dieses Problem zu umgehen wurde das Safe Harbor Abkommen vom amerikanischen Handelsministerium um der EU-Kommission erarbeitet. Welches ab Sommer 2000 in Kraft trat und im Laufe des Jahres auch in der Praxis angewandt wurde.

Um den Datenschutz der USA an den der Europäischen Union anzupassen, wurden im Juli 2000 vom US-Handelsministerium 7 Prinzipien[11] und Antworten auf 15 häufig gestellte Fragen[12] (FAQ) erarbeitet und veröffentlicht. Diese Prinzipien und FAQ sollen den Datenschutz in den USA soweit anheben, dass Datenübertragung gemäß den Datenschutzgesetzen der EU möglich ist. Am 26. Oktober 2000 erließ die Europäische Kommission eine Entscheidung, nach der in den USA tätige Organisationen über ein angemessenes Datenschutzniveau verfügen, wenn sie sich gegenüber der Federal Trade Commission (FTC[13]) öffentlich und unmissverständlich zur Einhaltung der Prinzipien und der in den 15 häufig gestellten Fragen enthaltenen Hinweise verpflichten.

Die Safe Harbor Vereinbarung sieht vor, dass die Unternehmen die folgenden 7 Prinzipien einhalten müssen, um ein angemessenes Datenschutzniveau vorweisen zu können:

- **1. Informationspflicht:** die Unternehmen müssen die Betroffenen darüber unterrichten, welche Daten sie für welche Zwecke erheben und welche Rechte die Betroffenen haben

[8] https://safeharbor.export.gov/list.aspx
[9] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf
[10] https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/SafeHarbor.html
[11] http://www.export.gov/safeharbor/eu/eg_main_018475.asp
[12] http://www.export.gov/safeharbor/eu/eg_main_018493.asp
[13] https://www.ftc.gov/

- ◇ **2. Wahlmöglichkeit:** die Unternehmen müssen den Betroffenen die Möglichkeit geben, der Weitergabe ihrer Daten an Dritte oder der Nutzung für andere Zwecke zu widersprechen
- ◇ **3. Weitergabe:** wenn ein Unternehmen Daten an Dritte weitergibt, muss es die Betroffenen darüber und die unter 2. aufgeführte Wahlmöglichkeit informieren
- ◇ **4. Zugangsrecht:** die Betroffenen müssen die Möglichkeit haben, die über sie gespeicherten Daten einzusehen und sie ggf. berichtigen, ergänzen oder löschen können
- ◇ **5. Sicherheit:** die Unternehmen müssen angemessene Sicherheitsvorkehrungen treffen, um die Daten vor unbefugtem Zugang oder vor Zerstörung und Missbrauch zu schützen
- ◇ **6. Datenintegrität:** die Unternehmen müssen sicherstellen, dass die von ihnen erhobenen Daten korrekt, vollständig und zweckdienlich sind
- ◇ **7. Durchsetzung:** die dem Safe Harbor beigetretenen Unternehmen verpflichten sich zudem, Streitschlichtungsmechanismen beizutreten, so dass die Betroffenen ihre Beschwerden und Klagen untersuchen lassen können und ihnen im gegebenen Fall Schadensersatz zukommt.[14]

Kritisch betrachtet werden sollte bei dieser Vereinbarung, dass Unternehmen die die Safe Harbor Vereinbarung in Anspruch nehmen wollen, lediglich zu erklären brauchen, dass sie bereit sind, die Grundsätze als verbindlich anzuerkennen.[15] Eine unabhängige Prüfung ob sie die erforderlichen Voraussetzungen dafür erfüllen, erfolgt nicht. Es reicht eine sogenannte Selbstzertifizierung.

Ende 2008 kritisierte der australische Datenschutzexperte Chris Connolly in seinem Paper "The US Safe Harbor - Fact or Fiction?"[16] einige Punkte am Safe Harbor Abkommen. Unter anderem beanstandete er, dass die Grundsätze des Abkommens von den Mitgliedsunternehmen in der Regel nicht eingehalten werden. Er gab an, dass von den 1.597 Einträgen in der Mitgliederliste[17] nur 1.109 Organisationen wirklich Mitglied des Safe Harbor Abkommens sind, da sie entweder nicht mehr existieren oder es versäumt haben ihre Zertifizierung zu erneuern. Außerdem enthielt die Liste zu diesem Zeitpunkt auch doppelte Einträge. Laut Connolly erfüllten nur 348 Organisationen die Mindestanforderungen des Safe Harbor Abkommens, unter anderem da einige keine "public privacy policy" (öffentliche Datenschutzbestimmungen) haben.

Auch als Kritikpunkt zu erwähnen, ist der USA PATRIOT Act.[18] Der USA PATRIOT Act ist ein US-amerikanisches Bundesgesetz, das im Oktober 2001 vom Kongress im Zuge des Krieges gegen den Terrorismus verabschiedet wurde. Die Bestimmungen des Gesetzes

[14] https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/SafeHarbor.html
[15] http://www.export.gov/safeharbor/eu/eg_main_018388.asp
[16] http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_-fiction.pdf
[17] https://safeharbor.export.gov/list.aspx
[18] http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:

erlauben US-Behörden wie dem FBI, der NSA oder der CIA nicht nur den Zugriff ohne richterliche Anordnung auf die Server von US-Unternehmen, sondern auch ausländische Tochterunternehmen sind nach dem US-Gesetz verpflichtet, Zugriff auf ihre Server zu gewähren, selbst dann, wenn lokale Gesetze dies untersagen. Durch diese Möglichkeit der US-Behörden, standortunabhängig uneingeschränkt Zugriff auf personenbezogene Daten zu bekommen, ist die Kritik an der Glaubwürdigkeit des Safe Harbor Abkommens durchaus berechtigt, da nicht einmal eine Einschaltung von US-Gerichten notwendig ist, sondern durch den Erlass eines "National Security Letters[19]" werden die Unternehmen unmittelbar durch die US-Behörden zur Herausgabe der Daten verpflichtet. Was natürlich im direkten Konflikt mit dem Europäischen Datenschutz steht.

Aufgrund dieser Probleme, stellten die obersten Aufsichtsbehörden für den Datenschutz im nicht- öffentlichen Bereich am 28./29. April 2010 in Hannover, mit den Beschluss des Düsseldorfer Kreises[20], verschärfte Anforderungen an die Übermittlung von personenbezogenen Daten an US-Unternehmen die Mitglieder des Safe Harbor Abkommens sind. Unter anderem heißt es dort:

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Habor Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Habor Zertifizierung des Importeurs noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor gegenüber dem von der Datenverarbeitung Betroffenen nachkommt.

Diese Mindestprüfung muss von den Unternehmen, die personenbezogene Daten in die USA auslagern wollen, dokumentiert und auf Nachfrage der Aufsichtsbehörden nachgewiesen werden können. Bei Fehlen dieser Standardvoraussetzungen empfiehlt der Düsseldorfer Kreis, die Verwendung von Standardvertragsklauseln oder bindende Unternehmensrichtlinien (Binding Corporate Rules) zur Gewährleistung eines angemessenen Datenschutzniveaus.

5.2.3. Binding Corporate Rules

Ein ausreichendes Datenschutzniveau stellen auch so genannte Binding Corporate Rules (verbindliche Unternehmensrichtlinien) sicher. Dabei legt sich eine Gruppe von Unternehmen rechtsverbindlich Regeln in Bezug auf den Umgang mit personenbezogenen Daten auf (Privacy Policy). Dadurch kann bei allen Unternehmen der Gruppe ein angemessenes

[19] http://fas.org/sgp/crs/intel/RL33332.pdf

[20] https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_-10neu.pdf

Datenschutzniveau sichergestellt werden. Somit dürfen innerhalb einer Unternehmensgruppe personenbezogene Daten auf der Grundlage verbindlicher unternehmensinterner Datenschutzregelungen (Binding Corporate Rules – BCR) aus der EU in Drittländer übermittelt werden. Die Datenschutzgruppe hat in ihren Arbeitsdokumenten WP 741 und WP 1082 Überlegungen zu den wesentlichen Bestandteilen solcher Regelungen angestellt.[21] Der Geltungsbereich dieser Richtlinien bezieht sich hauptsächlich auf Übermittlungs- und Verarbeitungsvorgänge innerhalb einer Unternehmensgruppe, wobei die Verarbeitungsvorgänge innerhalb der EU und die Datenübermittlung aus der EU in Drittländer vollzogen werden. Innerhalb der Unternehmensgruppe gelten somit standortunabhängig dieselben verbindlichen Richtlinien in Bezug auf den Datenschutz. In den Corporate Binding Rules unter anderem enthalten sind:

- ◇ **Zweckbindung:** Zweck der Verarbeitung und Übermittlung muss eindeutig und rechtmäßig sein
- ◇ **Datenqualität und -verhältnismäßigkeit** Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein
- ◇ **Rechtsgrundlage:** Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben oder - die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags u.a.
- ◇ **Transparenz:** Selbstverpflichtung, allen betroffenen Personen leichten Zugang zu den BCR zu gewähren
- ◇ **Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten:** Jede betroffene Person hat das Recht, frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten eine Kopie aller sie betreffenden Daten, die Gegenstand einer Verarbeitung sind, zu erhalten und ein Recht auf Berichtigung, Löschung oder Sperrung von Daten, insbesondere wenn diese Daten unvollständig oder unrichtig sind.
- ◇ **Automatisierte Einzelentscheidungen:** Selbstverpflichtung, dass keine Entscheidung, die die betroffene Person erheblich beeinträchtigt, ausschließlich auf eine automatisierte Verarbeitung ihrer Daten gestützt wird
- ◇ **Sicherheit und Vertraulichkeit:** Selbstverpflichtung zur Anwendung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und gegen jede andere Form der unrechtmäßigen Verarbeitung schützen
- ◇ **Verhältnis zu Datenverarbeitern, die der Unternehmensgruppe angehören:** Der für die Verarbeitung Verantwortliche muss einen Datenverarbeiter auswählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und

[21] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_de.pdf

organisatorischen Vorkehrungen eine ausreichende Gewähr bietet, und er muss für die Einhaltung dieser Maßnahmen sorgen.

- ◇ **Beschränkung des Datentransfers und der Weiterübermittlung an Datenverarbeiter und für die Verarbeitung Verantwortliche, die nicht der Unternehmensgruppe angehören:** Bei der Übermittlung von Daten an externe Verarbeiter außerhalb der EU sind zusätzlich zu den Vorschriften für den grenzüberschreitenden Datenverkehr (Artikel 25 und 26 der Richtlinie 95/46/EG) die Vorschriften für Datenverarbeiter zu beachten (Artikel 16 und 17 der Richtlinie 95/46/EG[22]).
- ◇ **Schulungsprogramm:** Selbstverpflichtung zur Bereitstellung geeigneter BCR-Schulungsmaßnahmen für Mitarbeiter, die ständigen oder regelmäßigen Zugang zu Personaldaten haben, die solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln
- ◇ **Auditprogramm:** Selbstverpflichtung, die Einhaltung der BCR innerhalb der Unternehmensgruppe einem Audit zu unterziehen
- ◇ **Einhaltung der BCR und Überwachung:** Selbstverpflichtung des Unternehmens, einen Mitarbeiterstab zu bilden (z. B. ein Netz von Datenschutzbeauftragten), der mit Unterstützung der Unternehmensspitze die Einhaltung der Vorschriften überwacht und gewährleistet
- ◇ **Vorgehen bei einzelstaatlichen Vorschriften, die der Einhaltung der BCR entgegenstehen:** Eindeutige Informationspflicht: Hat ein Unternehmen der Gruppe Anlass zu der Annahme, dass die es betreffenden Rechtsvorschriften es daran hindern, seinen Verpflichtungen im Rahmen der BCR nachzukommen, muss es unverzüglich die Hauptniederlassung der Unternehmensgruppe in der EU oder das Unternehmen, das in der EU die Haftung für den Datenschutz übernommen hat, oder den zuständigen Datenschutzbeauftragten informieren.
- ◇ **Interne Beschwerdeverfahren:** Selbstverpflichtung zur Einführung eines Beschwerdeverfahrens, das folgenden Grundsätzen genügt: - Jede betroffene Person muss Beschwerde mit der Begründung erheben können, dass ein Mitglied der Unternehmensgruppe gegen die BCR verstößt u.a.
- ◇ **Drittbegünstigung:** Eine klare Aussage dahin gehend, dass die BCR den betroffenen Personen als Drittbegünstigte Durchsetzungsrechte einräumen
- ◇ **Haftung:** Selbstverpflichtung folgenden Inhalts: Die EU-Hauptniederlassung oder das haftende Unternehmen in der EU übernimmt die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der EU, ergreift die notwendigen Maßnahmen, um Verstößen gegen die BCR abzuhelfen, und leistet Ersatz für Schäden, die aus einem Verstoß gegen die BCR durch ein Mitglied der Unternehmensgruppe entstanden sind. Die Beweislast trägt entweder die EU-Hauptniederlassung oder das haftende Unternehmen in der EU

[22]https://www.datenschutzzentrum.de/material/recht/eu-datenschutzrichlinie.htm

- ◇ **Gegenseitige Unterstützung und Zusammenarbeit mit den Datenschutzbehörden:** Selbstverpflichtung dahin gehend, dass die Mitglieder der Unternehmensgruppe bei Anfragen oder Beschwerden einer betroffenen Person oder bei Untersuchungen oder Nachforschungen der Datenschutzbehörden zusammenarbeiten und einander unterstützen die Unternehmen den Mitteilungen der Datenschutzbehörden, die die Auslegung der BCR betreffen, nachkommen
- ◇ **Aktualisierung der Vorschriften:** Selbstverpflichtung zur Meldung signifikanter Änderungen der BCR oder der Mitgliederliste gegenüber allen Mitgliedern der Unternehmensgruppe und den Datenschutzbehörden, um Änderungen der gesetzlichen Regelungen oder der Unternehmensstruktur Rechnung zu tragen
- ◇ **Verhältnis zwischen einzelstaatlichem Recht und BCR:** Erklärung, dass in Fällen, in denen das geltende Recht – z. B. EU-Recht – ein höheres Schutzniveau für personenbezogene Daten vorschreibt, dieses Recht den BCR vorgeht und die Datenverarbeitung in jedem Fall nach Maßgabe des anwendbaren Rechts im Sinne von Artikel 4 der Richtlinie 95/46/EG und der einschlägigen einzelstaatlichen Vorschriften erfolgt
- ◇ **Schlussbestimmungen:** Zeitpunkt des Inkrafttretens und Übergangszeit

5.2.4. Konklusion

Im Großen und Ganzen zeichnet sich ab, dass deutsche Unternehmen die personenbezogene Daten in die Cloud auslagern wollen, auf der sicheren Seite sind, wenn die Cloud Service Provider ihren Sitz in Deutschland oder dem Europäischen Wirtschaftsraum haben und die Daten eben dort gespeichert werden. Falls die Provider in einem Drittland ihren Sitz haben, mit geringem Datenschutzniveau, sollte vorher, anhand der vorhergegangenen Zusatzrichtlinien, genau überprüft werden welche Bedingungen die Provider erfüllen und dementsprechend entscheiden welcher als ausreichend sicher eingestuft werden kann.

Zum momentanen Zeitpunkt kann aber nicht sicher gesagt werden, ob US-Unternehmen die Safe Harbor zertifiziert sind oder andere Zertifikate besitzen, auch wirklich gewährleisten können, dass amerikanische Gerichte oder das FBI, keinen Zugriff zu sensiblen Kundendaten bekommen (selbst mit Serverstandort in Europa), da in dieser Situation, die amerikanischen Gesetze und die europäischen Datenschutzgesetze in Konflikt stehen.

Kapitel 6.

Anonymisierbarkeit

In diesem Abschnitt werden Möglichkeiten untersucht ob und wie Geschäftsprozesse und sensible Daten anonymisiert werden können, um somit den Datenschutz noch weiter auszubauen.

6.1. Anonymisierbarkeit und Schutzbedürftigkeit von sensiblen Daten in Geschäftsprozessen

Wie bereits im vorangegangenen Kapitel erwähnt, treten in Bezug auf personenbezogene Daten in der Cloud einige Hindernisse auf. Ein großes Problem ist es sicherzustellen, dass diese Daten nicht von Dritten missbraucht werden. Insbesondere wenn Geschäftsprozesse bearbeitet werden, die Kundendaten oder firmeninterne Prozesse beinhalten. Abhilfe können hier zum Beispiel die Anonymisierung oder Pseudonymisierung von diesen Daten darstellen. Das Bundesdatenschutzgesetz hat eine klar festgelegte Definition für beide Begriffe in § 3 BDSG.

6.1.1. Anonymisierung

So beschreibt der § 3 Abs. 6 BDSG die Anonymisierung wie folgt: *Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.* Es stehen unterschiedliche Methoden zur Verfügung um personenbezogene Daten zu anonymisieren:

- ◇ Löschung der Identifikationsmerkmale wie z.B. Name, Anschrift, Kontonummern usw.
- ◇ Merkmalsaggregierung, d.h. liegt eine bestimmte Merkmalsausprägung vor, wie z.B. 103 Jahre und kann diese nur jeweils einer Person in einer Personengruppe zugeordnet werden, müssen diese Angaben gelöscht oder durch allgemein gehaltene Aussagen ersetzt werden (z.B. über 80 Jahre).

- ◇ Zufallsfehler, eine weitere Methode, besteht darin, in kontrollierter Weise Zufallsfehler in den Datenbestand einzubringen.

Nach der Anonymisierung sind die Daten zwar immer noch Einzelangaben über eine bestimmte Person, allerdings können diese Daten dann keinen Personenbezug mehr herstellen und niemandem mehr zugeordnet werden. Somit lassen anonymisierte Daten folglich unter normalen Umständen keine Rückschlüsse auf Personen zu und unterfallen deshalb nicht den Einschränkungen des Bundesdatenschutzgesetzes. Anonymisierte Daten können uneingeschränkt bearbeitet, genutzt und weitergegeben werden. Allerdings muss erwähnt werden, dass alleine das Verschlüsseln von Daten nicht als deren Anonymisierung gilt, da dies hauptsächlich einen unverhältnismäßig hohen Rechenaufwand (Aufwand an Zeit und Kosten) bedeutet aber nicht den Aufwand der Arbeitskraft. Ebenfalls muss angenommen werden, dass mit fortschreitender technischer Entwicklung, es möglich sein könnte mit weniger Aufwand ebendiese Verschlüsselung zu brechen.

6.1.2. Pseudonymisierung

Und Pseudonymisierung (§ 3 Abs. 6a BDSG) wie folgt: *Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.* Bei der Pseudonymisierung werden Identifikationsmerkmale wie der Name oder Personenkennzahlen, durch ein Kennzeichen (Pseudonym) ersetzt. Es müssen alle direkten Identifikationsmerkmale ersetzt werden, bis die Zuordnung nicht mehr möglich ist. Anders als bei der Anonymisierung ist es hier möglich den Bezug zwischen den Daten und der Person wieder herzustellen. Dies ist zum Beispiel nötig, wenn einem Patienten Forschungsergebnisse mitgeteilt werden sollen. Damit schützen Pseudonyme die Identität des Betroffenen gegenüber Dritten, nicht jedoch gegenüber der verantwortlichen Stelle.[1]. Somit bedeutet Pseudonymisierung in Abgrenzung zur Anonymisierung (§ 3 Abs. 6 BDSG) nicht zwingend ein dauerhaftes Entfernen des Personenbezugs und die Daten bleiben ggf. datenschutzrelevant.

6.1.3. Heutiger Stand

Datenschützer ermuntern grundsätzlich zu Anonymisierung, Datenvermeidung und Datensparsamkeit, um die Verarbeitung personenbezogener Daten auf ein Mindestmaß zu reduzieren.[2] Allerdings wird von keinem Unternehmen verlangt, jeden Personenbezug aus den Datenbeständen zu tilgen. Beispielsweise darf der Cloud Service Provider aus Compliance-Gründen bei Systemprotokollen nicht jeden Personenbezug entfernen, denn sonst kann im konkreten Verdachtsfall der schuldige Nutzer nicht ausgemacht werden. Hierbei gilt die besondere Zweckbindung (§ 31 BDSG), werden personenbezogene Daten nur für den Erhebungszweck verarbeitet, müssen sie nicht anonymisiert werden.

[1] https://www.datenschutz.de/
[2] http://www.gesetze-im-internet.de/bdsg_1990/__3a.html

Es gibt unterschiedliche Methoden um personenbezogene Daten im Unternehmen zu anonymisieren, hier werden einige Ansätze erklärt.

6.1.4. Data Masking

6.1.4.1. Static Data Masking (SDM)

Unter Static Data Masking versteht man im Allgemeinen die Maskierung von personenbezogenen Daten in bereits vorhandenen Datensätzen. Hierbei durchsucht eine Software die Datenbanken oder auch unstrukturierte Datensätze nach personenbezogenen Daten und anonymisiert diese nach bestimmten Kriterien. Fundstellen lassen sich nach vorher definierten Regeln maskieren. Die statische (oder dauerhafte) Datenmaskierung ändert Datenwerte permanent und unwiderruflich, behält aber gleichzeitig die ursprünglichen Eigenschaften und Muster bei. Data Masking schützt vertrauliche Daten wie Kreditkartennummern, Adressen und Telefonnummern vor unbeabsichtigter Offenlegung, indem realistische, anonymisierte Daten erstellt werden, die sicher intern oder extern übermittelt werden können. Als Maskierungsmethoden können unter anderem Substitution, Zufallsauswahl, Sequenzen, Verdrehung oder Annullierung eingesetzt werden.

6.1.4.2. Dynamic Data Masking (DDM)

Dynamic Data Masking ist eine Abwandlung des Static Data Masking, anstatt die Original Datenbank persistent zu maskieren, also sensible Daten zu verschleiern, wird hier die Original Datenbank nicht geändert, sondern in Echtzeit für unautorisierte Benutzer die Daten maskiert. Das heißt die dynamische Datenmaskierung ändert den Wert, der dem Benutzer während der Anfrage angezeigt wird. Die ursprünglichen Werte bleiben dabei unverändert. Autorisierte Benutzer können so die Originaldatenbank verwenden, während nicht autorisierte Benutzer wie z.B. Techniker oder Administratoren nur die maskierte Datenbank inklusive abgeänderter Daten zu sehen bekommen.

Auch in Bezug auf die Cloud sind solche Datenmaskierungen denkbar, beispielsweise könnte der Nutzer eine, durch SDM maskierte Datenbank, in die Cloud auslagern (z.B. Kundendatenbank oder Geschäftsprozesse mit sensiblen Daten) um mit den maskierten Daten zu arbeiten aber ohne Gefahr zu laufen, dass sensible Daten missbraucht werden könnten. Auf Providerseite wäre denkbar, ein DDM-System einzubauen, damit Personen die zwar Zugang zu den Daten benötigen wie z.B. Administratoren, ihn auch gewährt bekommen, aber durch die dynamische Datenmaskierung nur in die abgewandelten Daten Einsicht bekommen.

6.1.5. Technik

Um die Daten sicher zu maskieren sind verschiedene Techniken[3] möglich. Hier werden die wichtigsten näher erläutert.

6.1.5.1. Substitution

Diese Technik basiert auf den zufälligen spaltenweisen Austausch von Daten in einer Datenbank, mit Daten die ähnlich aussehen aber keinen Bezug zu den ursprünglichen Daten haben. Beispielsweise können die original Nachnamen in einer Kundendatenbank durch Werte aus einer Liste mit zufällig (random) generierten Nachnamen ersetzt werden. Ein Nachteil hierbei wäre allerdings, dass immer große Datenlisten vorhanden sein müssen, um sensible Daten ersetzten zu können wie z.B. Namen, Adressen, Telefonnummern. Von Vorteil wäre, wenn Daten generiert werden, die den Originaldaten entsprechen aber nicht benutzbar sind, sollten sie in falsche Hände geraten. Als Beispiel zu erwähnen sind hier Kreditkartennummern die die Prüfsummenformel des Luhn-Algorithmus[4] bestehen aber nicht benutzbar sind.

6.1.5.2. Shuffling

Beim Shuffling werden die Datensätze einer Spalte zwischen den Zeilen einer Datenbank getauscht (randomisiert), dies geschieht solange, bis kein Bezug mehr zu den Originaldaten in einer Spalte hergestellt werden kann. Diese Methode birgt allerdings einige Gefahren, denn wenn die Kundennamen nicht geändert werden sondern nur getauscht, kann jemand der nach einem bestimmten Namen sucht ihn auch finden, wenn auch an anderer Stelle. Shuffling ist am effektivsten, wenn es auf große Datenmengen angewendet wird, bei relativ kleinen Datensätzen wo z.B. nur 5 Zeilen zum Vertauschen vorhanden sind, ist es nicht ratsam an dieser Stelle die Shufflingtechnik zu benutzen.

6.1.5.3. Datenstreuung

Die Methode der Datenstreuung ist eine nützliche Technik, wenn es sich um numerische Daten handelt, wie z.B. Datum oder Finanzdaten. Der Algorithmus variiert jedes Datum oder jede Zahl in einer Spalte nach einem zufälligen Prozentwert seines Originalwertes. Wenn z.B. ein Gehalt in einer Zeile mit 3.500 angegeben ist, ändert der Algorithmus den Wert um +8% ab, in diesem Beispiel wären das 3.780 als maskierter Wert. Diese Methode hat den Vorteil, dass sie die Daten angemessen verändert aber trotzdem im Range des Originalwertes bleibt.

[3] http://www.datamasker.com/DataMasking_WhatYouNeedToKnow.pdf
[4] https://de.wikipedia.org/wiki/Luhn-Algorithmus

6.1.5.4. Verschlüsselung

Beim Verschlüsseln sind die Daten in der Datenbank unverändert sichtbar für autorisierte Personen, die einen Schlüssel besitzen und nutzlos für Personen die keinen Schlüssel erhalten haben. Diese Methode hat allerdings einige Nachteile. Wird der Schlüssel einmal unautorisiert weitergegeben oder gestohlen, ist die gesamte Datenbank für denjenigen sichtbar, zwar kann der Schlüssel wieder geändert werden, aber für kurze Zeit ist die Datenbank ungeschützt. Ebenso kann man mit verschlüsselten Daten schlecht arbeiten, da sie meist unleserlich sind, also unähnlich zum Originalwert. Wichtig hierbei ist immer eine gute Verschlüsselung zu verwenden wie z.B. AES 256bit oder RSA[5], man sollte niemals nur eine einfache Austauschverschlüsselung wie die Ceasar-Verschlüsselung[6] benutzten, bei der einzelne Buchstaben durch andere ersetzt werden.

6.1.5.5. NULL

Eine weitere Möglichkeit besteht darin, sensible Daten zu löschen bzw. die Werte einer Spalte mit NULL zu ersetzen. Dies ist natürlich ein effektiver Weg, personenbezogene Daten vor unautorisierten Personen zu schützen, allerdings kein effizienter. Denn auch wie auch schon weiter oben erwähnt, lässt sich mit 'ausgenullten' Daten sehr schlecht arbeiten. Diese Methode ist nur sinnvoll wenn die expliziten Daten nicht direkt benötigt werden, z.B. für Stresstests bei denen nur viele Daten aber nicht deren eigentlicher Wert benötigt werden.

6.1.5.6. Retuschieren

Eine bekannte Methode ist das Retuschieren von bestimmten Werten innerhalb der Daten. Das heißt, es werden Teile des Originalwertes mit einem Charakter ersetzt, z.B. einem X. Dieses wird oft bei Kreditkartennummern verwendet. Das Maskieren mit Charaktern löscht effizient und schnell den sensiblen Bezug der Daten. Allerdings muss darauf geachtet werden, dass genug Daten maskiert wurden um die nötige Sicherheit herzustellen. Folgende Maskierung wäre nicht von Vorteil: 4297 8296 7496 87XX. Da bei nur 2 fehlenden Zeichen es nicht schwer wäre die Originalwerte herauszubekommen, vor allem da die realen Kreditkartennummern auch der Prüfsummenformel genügen müssen. Optimal wäre folgende Maskierung: 4297 XXXX XXXX 8724.

6.1.6. Datenbankbesonderheiten

Wenn sensible Daten in großen Datenbanken maskiert werden sollen, können einige Probleme auftreten. Zum Beispiel haben manche personenbezogene Daten Bezug zu anderen Zeilen oder Spalten oder ganzen Tabellen. Ein guter Datenmaskierungs-Algorithmus, muss eben

[5]http://cacr.uwaterloo.ca/hac/about/chap8.pdf
[6]http://www.mathe.tu-freiberg.de/ hebisch/cafe/kryptographie/caesar.html

diesen Bezug den die Daten zu anderen Daten haben, erkennen, synchronisieren und ebenfalls maskieren. Einige Besonderheiten werden hier aufgeführt.

6.1.6.1. Reihensynchronisation

In Tabelle 6.1 sieht man die Einträge einer Kundendatenbank, mit den Originalwerten 'Katja' und 'Thomas'. Es wird deutlich, dass wenn eine Maskierung der Daten z.B. durch Substitution vorgenommen wird, dass sich dann nicht nur der 'Vorname' und 'Nachname' ändern müssen sondern auch der gesamte Name in der Spalte 'Name', da diese Spalten inhaltlich zusammenhängen.

ID	VORNAME	NACHNAME	NAME
123	Katja	Meier	Katja Meier
122	Thomas	Schulz	Thomas Schulz
		↓	
123	Lisa	Müller	Lisa Müller
122	Sven	Heinz	Sven Heinz

Tabelle 6.1.: Beispiel einer Reihensynchronisation

6.1.6.2. Zeilensynchronisation

Ebenso ist es möglich, dass in verschiedenen Zeilen einer Tabelle dieselben Werte vorkommen. Dieses Szenario muss von der Maskierungssoftware ebenfalls abgedeckt werden, da sonst die Daten in der Datenbank verfälscht werden könnten. In Tabelle 6.2. ist dieses bildlich dargestellt.

ID	VORNAME	NACHNAME	NAME
123	Katja	Meier	Katja Meier
122	Thomas	Schulz	Thomas Schulz
577	Anna	Mahler	Anna Mahler
123	Katja	Meier	Katja Meier
		↓	
123	Lisa	Müller	Lisa Müller
122	Sven	Heinz	Sven Heinz
577	Ute	Schiller	Ute Schiller
123	Lisa	Müller	Lisa Müller

Tabelle 6.2.: Beispiel einer Zeilensynchronisation

6.1.7. Reversible Anonymisierung

Eine der neueren Entwicklungen ist die reversible Anonymisierung. Hier sollen schutzwürdige Daten (personenbezogene Daten) anonymisiert werden um somit dem Bundesdatenschutzgesetz zu genügen. Die Vorgehensweise ist folgende:

- ◇ Verschlüsseln der Daten mit z.B. AES 256
- ◇ Fragmentieren der Daten in mehrere Teile
- ◇ getrenntes Speichern der Fragmente

Durch die Verschlüsselung, Fragmentierung und gleichzeitiges Speichern an verschiedenen Speicherorten entsteht ein sehr hohes Datenschutzniveau. Wie schon im vorherigen Kapitel erwähnt, gelten Daten laut BDSG als anonymisiert wenn sie "nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." Der Beschaffungsaufwand von Daten die verschlüsselt, fragmentiert und an unterschiedlichen Speicherorten verteilt sind ist dementsprechend unverhältnismäßig hoch. Selbst wenn die Verschlüsselung gebrochen werden sollte, so liegen die Daten nicht vollständig vor und es müssten erst alle unterschiedlichen Speicherorte herausgefunden und dort die Fragmente abgegriffen werden. Dieser Beschaffungsaufwand wird auch nicht mit der Zeit geringer. Somit ist hier die Wiederherstellung der personenbezogenen Daten für Dritte im Hinblick auf Zeit, Kosten und Arbeitsaufwand unverhältnismäßig hoch[7]. Das heißt, dass die gesetzlichen Anforderungen laut BDSG erfüllt sind und somit gelten diese ehemals personenbezogenen Daten nicht mehr als schutzwürdig und können ohne als Auftragsdatenverarbeitung zu gelten, ausgelagert werden. Allerdings muss die Person die die Daten verwaltet, beim Cloud Computing der Cloudnutzer, die Vorschriften des BDSG jedoch weiterhin beachten. Denn die ausgelagerten Daten sind, nicht für die intern verantwortliche Stelle anonymisiert, da diese die Daten wieder entschlüsseln kann, sondern nur für die Outsourcing-Stelle in diesem Fall der Cloud Provider. Die für eine Identifizierung erforderlichen Zusatzinformationen sind separat zu speichern und dürfen in diesen Fall nicht mit den Fragmenten ausgelagert werden.

Ein Nachteil dieser Methode ist natürlich, dass ein Cloudspeicher nicht mehr ausreicht um dieses Datenschutzniveau aufrecht zu erhalten. Was wiederum mit Mehrkosten und Mehraufwand verbunden ist.

6.1.8. Verschlüsseln mit AES 256

Einer der bekanntesten und zurzeit auch sichersten Verschlüsselungsansätze ist die symmetrische Verschlüsselung mit AES-256 Bit. Der Advanced Encryption Standard (AES) ist eine Blockchiffre[8], im Oktober 2000 vom National Institute of Standards and Technology (NIST)

[7]https://www.dfn.de/fileadmin/3Beratung/DFN-Forum7/folien/9-dfn-2014-cloud-speicher-uni-freiburg.pdf
[8]http://www.itwissen.info/definition/lexikon/Blockchiffre-block-cipher.html

als Standard bekanntgegeben wurde. AES schränkt die Blocklänge auf 128 Bit und die Wahl der Schlüssellänge auf 128, 192 oder 256 Bit ein. Die Bezeichnungen der drei AES-Varianten AES-128, AES-192 und AES-256 beziehen sich jeweils auf die gewählte Schlüssellänge. Der Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren eingesetzt sowie in Soft- und Hardware implementiert werden.[9] Dem Verfahren[10] nach wird der Klartext in zehn Runden (10 Runden bei 128-Bit-Schlüssel, 11 bei 192, 13 bei 256) mit Rundenschlüssel, die aus dem geheimen Schlüssel abgeleitet werden, verschlüsselt. Zuvor wird der Klartext in Zeilen und Spalten aufgeteilt und in jeder Verschlüsselungsrunde werden die Ausgangsdaten byteweise ersetzt, die Zeilen rotieren, die Spalten werden gemischt und die Daten über eine XOR-Verknüpfung verknüpft.[11]

6.1.9. Fragmentierung

Hierbei werden die im vorhergegangen Schritt verschlüsselten Daten in mehrere Fragmente aufgeteilt. Der Zweck dieser Aufteilung besteht darin, dass die verschlüsselten Daten nicht komplett in einem Stück vorliegen. Das macht es ungemein schwerer die Daten zu entschlüsseln selbst wenn der Schlüssel offengelegt werden sollte. In Abb. 6.1. sieht man die Funktionsweise einer Fragmentierung.[12]

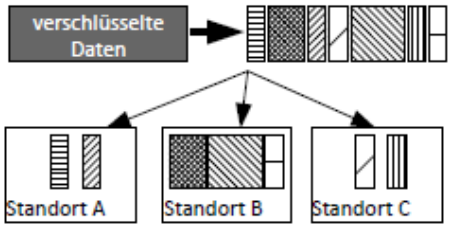


Abbildung 6.1.: Funktionsweise einer Fragmentierung

6.1.10. Föderiertes Speichersystem

Wie bereits vorab erwähnt, ist es bei der reversiblen Anonymisierung unerlässlich, dass die verschlüsselten und fragmentierten Daten auf unterschiedlichen Speichersystemen gespeichert werden. Was natürlich einige Probleme mit sich bringt, wenn man darauf angewiesen ist, seine Daten auf mehrere Cloudsysteme auszulagern. Ein Ansatz zur Verbesserung des

[9] http://csrc.nist.gov/groups/ST/toolkit/documents/aes/CNSS15FS.pdf
[10] http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
[11] http://www.itwissen.info/definition/lexikon/Rijndael-Vincent-Rijmen-and-Joan-Daemen.html
[12] https://www.dfn.de/fileadmin/3Beratung/DFN-Forum7/folien/9-dfn-2014-cloud-speicher-uni-freiburg.pdf

Problems wurde an der Albert-Ludwigs-Universität Freiburg untersucht. Hier wurde das Problem mit einem föderiertem Speichersystem angegangen. Dieses Speichermodell verbindet mehrere Cloudspeichersysteme und deren jeweilige Systeme zu einem Speicherverbund[13], damit soll es möglich sein die Speicherressourcen von mehreren unabhängigen Speicherorten im Verbund zu nutzen. In Abbildung 6.2 sieht man den Grundriss des föderierten Speichersystems.

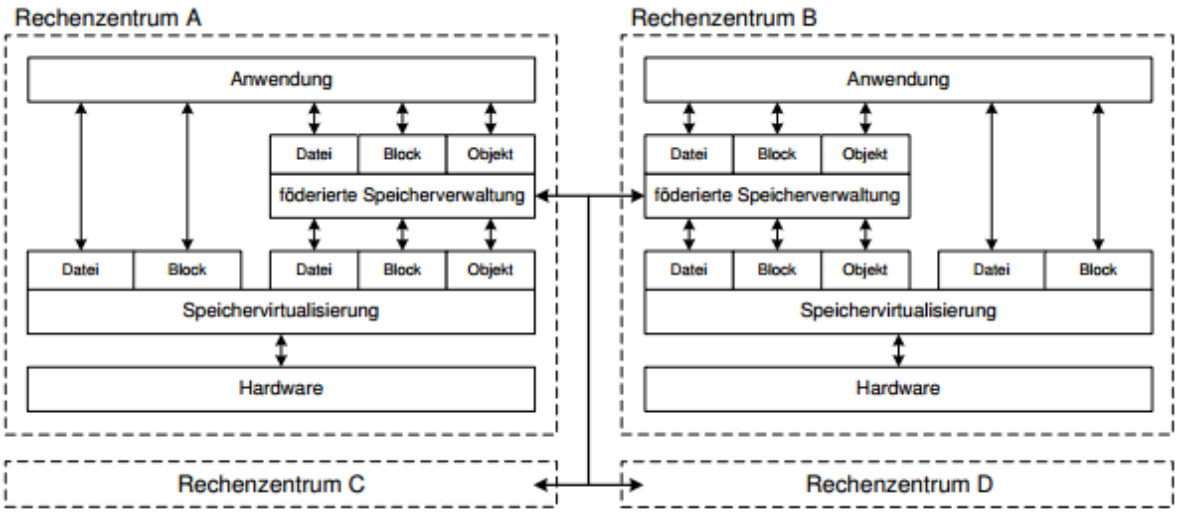


Abbildung 6.2.: Aufbau eines föderierten Speichersystems (Universität Freiburg)

Das System basiert auf dem Ansatz eines Object-Storage-Systems (hier Open Stack Swift[14]) mit frei wählbarem Datenspeicherort und wird durch eine Abstraktions- und Verwaltungsschicht über der lokalen Speicherverwaltung ermöglicht. Die verschiedenen Schichten und die Kommunikation dazwischen sind in Abb. 6.2 dargestellt. Die Kommunikation zwischen den Rechenzentren erfolgt über die Schicht der föderierten Speicherverwaltung.[15] Die unterste Schicht bildet der lokale Hardware-Speicher, welcher für die darüber liegende Schicht - die Speichervirtualisierung - den Speicher bereitstellt. Diese wiederum verwendet den zur Verfügung gestellten Speicher und stellt ihn in Speichertools über Datei- oder Blockzugriff bereit. Auch ein Object-Storage wie Open-Stack-Storage ist möglich, wobei hier die Speichervirtualisierung einen Objektzugriff bereitstellt. Beim Blockzugriff erfolgt der Zugriff auf die Daten direkt Block für Block vom Datenträger. Gesteuert wird dieses über Dateitabellen des Betriebssystems des anfragenden Rechners. Aufgrund dieses Aufbaus ist Blockzugriff schneller als andere Methoden, allerdings jeweils beschränkt auf einen Rechner. Beim Dateizugriff werden Daten nur über ihre Namen adressiert, nicht über ihren Speicherplatz.

[13]https://www.dfn.de/fileadmin/3Beratung/DFN-Forum6/2_Ein_Konzept_zum_Aufbau_eines_fo__ederierten__dezentralen_Speichersystems_im_Hochschulumfeld.pdf
[14]http://docs.openstack.org/developer/swift
[15]http://subs.emis.de/LNI/Proceedings/Proceedings231/75.pdf

Dies benötigt einen separaten Fileserver, der die Lese- und Schreibanfragen verwaltet und intern ebenfalls über Blockzugriff auf die Daten zugreift. Die beteiligten Rechner kennen den Speicherort der Daten nicht, sondern senden nur eine Namensanfrage an den Fileserver, der diese Anfragen verwaltet. Ein Vorteil hierbei ist, dass somit mehrere Systeme gleichzeitig auf die Daten zugreifen können.[16] Beim Objektspeicher wird ein Objekt abgelegt, das die Daten selbst und eine variable Menge an Metadaten und einen Key (Unique Identifier) umfasst. Die verwendete flache Hierarchie steht dabei im Gegensatz zum Dateizugriff, wo der Ablageort sowie die Hierarchie genau bestimmt werden müssen wie z.B. Ordner und Dateinamen. Die Speichertools der Speichervirtualisierung werden von der föderierten Speicherverwaltung als Object Storage angesprochen, selbst wenn die Speichervirtualisierung in Datei- oder Blockzugriff implementiert ist. In diesem Fall übernimmt die föderierte Speicherverwaltung die Übersetzung in einen Object-Storage. Der Sinn dieser Speicherverwaltung ist es, verschiedene Standorte untereinander zu verbinden. Über die Schicht der föderierten Speicherverwaltung ist es möglich, Objekte zwischen den Standorten zu verschieben oder zu kopieren.[17]

Um den Datenschutz der in diesem Speichersystem gelagerten Daten zu gewährleisten, ist es jeder Anwendung möglich, über Metadaten im Object-Storage zu definieren welche Art von Schutz die gespeicherten Daten benötigen. Es bestehen unterschiedliche Securitylevel mit denen der Grad des Schutzlevels eingerichtet werden kann.

- ◇ Level 0: Daten werden nicht verschlüsselt
- ◇ Level 1: Daten werden beim Auslagern verschlüsselt
- ◇ Level 2: Daten werden lokal und beim Auslagern verschlüsselt
- ◇ Level 9: personenbezogene Daten

Wenn personenbezogene Daten an externe Speichersysteme innerhalb der Föderation weitergegeben werden, wird das bereits erwähnte reversible Anonymisierungsverfahren angewendet. Der Ablauf des Verfahrens besteht aus:

- ◇ Verschlüsselten Datensatz lokal lesen (Metadaten)
- ◇ Verschlüsselten Datensatz fragmentieren
- ◇ Fragmente extern speichern
- ◇ Linkinformationen verschlüsseln
- ◇ Verschlüsselte Linkinformationen lokal speichern

[16] http://www.it-administrator.de/download/whitepapers/Whitepaper_Ontrack_Server-Datenrettung.pdf
[17] https://www.dfn.de/fileadmin/3Beratung/DFN-Forum6/2_Ein_Konzept_zum_Aufbau_eines_fo__ederierten__dezentralen_Speichersystems_im_Hochschulumfeld.pdf

Damit, bei Bedarf, die fragmentierten Daten wieder zusammengefügt werden können, werden Linkinformationen im lokalen Speichersystem erstellt und im Datenbereich des ursprünglichen Objektes gespeichert. Sie enthalten Metadaten (Speicherort, Container, Objektname im externen Speichersystem) die später dazu verwendet werden könnten, die getrennten Datenfragmente korrekt zusammenzusetzen.

Allerdings stellt die Anzahl der Fragmente und deren Auslagerung, bei dieser Variante ein Problem dar. Diese werden hier statisch festgelegt, d.h. genau ein Fragment (nicht redundant) wird in einem externen Speichersystem gespeichert und stehen nicht genügend dieser Speichersysteme zur Verfügung, können die fragmentierten Daten nicht ausgelagert werden. Ebenfalls müssen beim Zugriff auf die Daten (Zusammensetzung) alle externen Speichersysteme verfügbar sein.

Für die Zukunft müsste hier noch eine effizientere Fragmentierungsmethode eingebunden werden, die es ermöglicht die Fragmente optimal und redundant zu speichern um z.B. bei Ausfällen Datenverlusten vorzubeugen.

Eine detaillierte Ausführung der Funktionsweise des föderierten Speichersystems kann unter "Ein Konzept zum Aufbau eines föderierten, dezentralen Speichersystems im Hochschulumfeld"[18] nachgelesen werden.

6.1.11. End-to-End Verschlüsselung

Eine weitere Möglichkeit sensible Daten in der Cloud zu schützen, ist die End-to-End-Verschlüsselung. Bei den meisten Cloud-Anbietern werden die Daten erst über eine sichere Verbindung übertragen und dann auf den Servern des Cloud Service Providers gespeichert und verschlüsselt. Der Schlüssel hierfür liegt dann beim Provider und nicht beim Kunden. Was unter anderem zu Sicherheitsproblemen führen kann, falls der Schlüssel auf Provider-Seite in falsche Hände gerät.

Eine der aktuellen Entwicklungen zu diesem Thema hat die Firma Fabasoft[19] in Zusammenarbeit mit der TU Graz vorgestellt. Die Secomo Appliance[20] ist ein Paket bestehend aus der Secomo Software auf einem hochverfügbaren Serverpaar (mit integrierten Hardware-Sicherheitsmodulen) im Verbund. Sie kann als Private Cloud oder Public Cloud betrieben werden. Die Daten werden schon im eigenen Unternehmen verschlüsselt gespeichert und - im Falle einer Public Cloud - verschlüsselt an den Cloud Service Provider übermittelt. Mit der End-to-End Verschlüsselung nicht erst am Server, sondern direkt am Arbeitsplatz. Das Unternehmen allein behält den Schlüssel zu den Daten und der CSP kann somit keine Information aus den verschlüsselten Dokumenten entnehmen.

[18] https://www.dfn.de/fileadmin/3Beratung/DFN-Forum6/2_Ein_Konzept_zum_Aufbau_eines_fo__ederierten__dezentralen_Speichersystems_im_Hochschulumfeld.pdf
[19] https://www.fabasoft.com
[20] https://www.fabasoft.com/cloud/de-de/secomo

Abbildung 6.3.: Darstellung der Secomo Appliance (www.fabasoft.com)

6.1.12. Konklusion

Data Masking ist eine gute Möglichkeit, sensible Daten die außerhalb des Unternehmens, durch z.B. Outsourcing oder Testumgebungen, gelagert werden, vor Missbrauch zu schützen. Auch in Bezug auf sensible Geschäftsprozesse die in die Cloud ausgelagert werden sollen, bringt Data Masking einige Vorteile. Denn auch beim Cloud Service Provider haben bestimmte Personen (z.B. Administratoren) Zugang zu den Kundendaten. Wenn diese Kundendaten nun maskiert sind erhöht sich hierdurch die Sicherheit und der Schutz dieser sensiblen Daten, denn der Administrator hat zwar Zugang aber nur zu abgewandelten Daten die keinen realen Kundenbezug haben.

Die reversible Anonymisierung mit einem föderierten Speichersystem ist ein Prototyp, der durchaus Potential hat, eine gute Lösung in Bezug auf den Schutz von personenbezogenen Daten zu werden. Allerdings müssen hierbei noch Verbesserungen und Anpassungen durchgeführt werden, damit dieser Ansatz in der Zukunft eine Möglichkeit ist, die Daten ausreichend und effizient zu anonymisieren.

End-to-End Verschlüsselung ist eine gute Möglichkeit sensible Daten bereits im eigenen Unternehmen, vor dem Übertragen in die Cloud, zu verschlüsseln um somit einen höheren Sicherheitsstandard zu erreichen. Allerdings muss hier beachtet werden, dass wenn die Übertragung von verschlüsselten Daten am Sicherheitsgateway (z.B. ein virtuelles privates Netzwerk - VPN) des Providers zugelassen wird, die Filter des Gateways möglicherweise nicht mehr in der Lage sind die eingehenden Nutzerdaten auf Viren oder andere Schadprogramme zu überprüfen. Ebenfalls zählt die alleinige Verschlüsselung von Daten laut BDSG nicht als Anonymisierung (siehe Kapitel 6.1.1), dennoch ist die End-to-End Verschlüsselung eine nützliche Ergänzung zu den herkömmlichen Sicherheitsmaßnahmen, unabhängig davon ob es sich nun um personenbezogene Daten handelt oder nicht.[21]

[21] http://www.bsi.bund.de

Kapitel 7.

Zusammenfassung und Ausblick

In diesem Abschnitt werden die Ergebnisse und Rückschlüsse aus der Diplomarbeit in einem Fazit zusammengefasst und erläutert.

Ausblick

Zum momentanen Zeitpunkt ist der Markt, in Bezug auf BPM in der Cloud, noch überschaubar, da diese Kombination von Geschäftsprozessmanagement und Cloud Computing, noch am Anfang ihrer Entwicklung steht. Es gibt zwar schon einige Anbieter wie IBM oder Fabasoft, die BPM in der Cloud anbieten aber es wird noch gewisse Zeit dauern, bevor dieses ein weitverbreiteter Ansatz sein wird, um Geschäftsprozesse effizient zu optimieren. Eines der Hauptprobleme, welches das Cloud Computing im Allgemeinen hat, ist der Datenschutz. Viele Unternehmen sind sich im Unklaren ob sensible Firmendaten oder personenbezogene Kundendaten in der Cloud wirklich sicher sind, vor allem da in Deutschland eines der höchsten Sicherheitsniveaus, in Bezug auf Datenschutz, existiert (Bundesdatenschutzgesetz). Wenn personenbezogene Daten in die Cloud ausgelagert werden sollen, müssen einige gesetzliche Bestimmungen eingehalten werden, um sich als Unternehmen, welches diese sensiblen Daten outsourct, nicht strafbar zu machen.

Im Rahmen dieser Diplomarbeit wurden diverse Anbieter von BPM in der Cloud ausgewertet und hinsichtlich des Datenschutzniveaus, anhand eines dafür erstellten Kriterienkataloges, analysiert. Als Ergebnis dieser Auswertung kann gesagt werden, dass die Nutzer der Cloudservices sich sehr genau über den Cloud Service Provider informieren sollten, insbesondere wo sich der Serverstandort für die Kundendaten befindet und wo der Provider seinen Hauptfirmensitz hat, bzw. welches Recht im Falle von Problemen angewandt wird (z.B. amerikanisches oder deutsches Recht). Im Allgemeinen zeichnet sich ab, dass Unternehmen die personenbezogene Daten in die Cloud verlagern wollen, gesetzlich auf der sicheren Seite sind, wenn sie einen Provider mit Hauptsitz und Serverstandort in Deutschland/Europa auswählen, der selbst alle Cloudservices anbietet oder falls Subunternehmer vorhanden sind, diese ebenfalls aus Europa stammen und somit auch an die Bestimmungen des Europäischen Datenschutzes gebunden sind. Vorsicht geboten ist demnach bei Anbietern mit Hauptsitz in den USA, da hier ein weitaus geringeres Datenschutzniveau besteht und auch zum momentanen Zeitpunkt nicht gesagt werden kann, ob Kundendaten vor amerikanischen

Gerichten oder dem US Patriot Act sicher sind, selbst wenn sie auf europäischen Servern der US-Anbieter liegen.

Da dem Cloud Computing für die Zukunft, von diversen Studien[1] ein immer größeres Wachstum vorhergesagt wird, wird auch BPM in der Cloud weiteren Zulauf bekommen. Es wäre wünschenswert, wenn es zukünftig mehr Anbieter geben würde, die diese Cloud Services anbieten, ihren Hauptsitz vorzugsweise in Deutschland oder Europa haben und die Kundendaten ebenfalls dort gespeichert werden. Für die Cloudnutzer würde dies die Handhabe mit den personenbezogenen Daten in der Cloud wesentlich vereinfachen und das Risiko, in Konflikt mit dem Bundesdatenschutzgesetzes zu kommen, verringern.

[1] http://www.bitkom.org/de/presse/81149_80724.aspx

Akronyme und Abkürzungen

BPM Business Prozess Management

BPMN Business Process Model and Notation

EPK Ereignisgesteuerte Prozesskette

OMG Object Management Group

BPEL Business Process Execution Language

BPMaaS Business Process Management as a Service

CSP Cloud Service Provider

BPEL Business Process Execution Language

BSI Bundesamt für Sicherheit

SLA Service Level Agreement

SaaS Software as a Service

PaaS Platform as a Service

IaaS Infrastructure as a Service

SECaaS Security as a Service

BPaaS Business Process as a Service

BPMaaS Business Process Management as a Service

DDoS Distributed Denial of Service

VM Virtual Machine

VMM Virtual Machine Monitor

BIOS Basic input/output System

LAN Local Area Network

SAN Storage Area Network

OS Operating System

SSH Secure Shell

VPN Virtual Private Network

BDSG Bundesdatenschutzgesetz

EWR Europäischer Wirtschaftsraum

BCR Binding Corporate Rules

SDM Static Data Masking

DDM Dynamic Data Masking

XML Extensible Markup Language

VLAN Virtual Local Area Network

TLS Transport Layer Security

SSL Secure Sockets Layer

SAML Security Assertion Markup Language

ISO International Organization for Standardization

Anhang A.

Ein Anhang

Der Kriterienkatalog soll als Unterstützung dienen, um herauszufinden welche Punkte ein Cloud Service Provider erfüllen sollte, damit sensible Daten (z.B. personenbezogene) sicher in die Cloud ausgelagert werden können.

Die einzelnen optimalen Antworten sind mit einem grauen 'X' gekennzeichnet. Ebenso kann, die in dieser Diplomarbeit durchgeführte Anwendung des Kriterienkataloges, als Hilfestellung hinzugezogen werden.

Kriterienkatalog	*Ja*	*Nein*	*Bemerkungen*
Security			
Verfügt der Provider über ein ausgereiftes IT-Sicherheitskonzept? (z.B. Schutz vor Malware, Abwehr von DDoS-Angriffen)	X		
Existiert ein Intrusion Detection System - IDS (Angrifferkennungssystem) zur Überwachung der IT-Infrastruktur?	X		
Werden interne Angriffe (d.h. von Kunden auf Kunden) verhindert bzw. entdeckt und effektiv untersucht und unterbunden?	X		
Sicherheitsmaßnahmen sind up-to-date	X		
Authentifizierung ist suffizient: • autorisierte Personen haben Zugang • unautorisierte Personen haben keinen Zugang	X		
Auf Anbieterseite haben nur wenige Personen Zugang zu den Kundendaten (bzw. Admin)	X		
Ist ein effektives Verschlüsselungs- und Schlüsselmanagement vorhanden, um die Kundendaten und den Datenaustausch sicher zu verschlüsseln? • RSA • AES • https	X		

Kriterienkatalog	*Ja*	*Nein*	*Bemerkungen*
Sichere Schlüsselverwaltung: • geeignete Schlüsselgeneratoren • sichere Verteilung der Schlüssel • Admins haben keinen Zugriff auf Kundenschlüssel	X		
Stehen Vorkehrungen zur Verfügung die ggf. Ausfallzeiten und Datenverlust vorbeugen? • Backups • Redundante Infrastruktur • Physikalische Sicherheit (z.B. Notstrom)	X		
Ist ein definiertes Vorgehensmodell der firmeninternen IT-Geschäftsprozesse vorhanden? • ITIL • COBIT	X		
Intensives Monitoring von Cloud-Nutzeraktivitäten auf Anbieterseite	X		
Zur Datenübertragung werden ausschließlich verschlüsselte Protokolle benutzt	X		
Werden regelmäßige und unabhängige Prüfungen des IT-Sicherheitszustands, wie z.B. Penetrations-Tests und Audits, vorgenommen? • wöchentlich • monatlich • jährlich	X		
Log-Analyse der Netzwerkverbindungen zwischen Cloud Anwender und Cloud Ressourcen	X		
Ist ein geschütztes Cloudmanagementsystem (CMS) vorhanden? • IDS • Zugriffsliste	X		
Sichere Grundkonfiguration des Hostbetriebssystems • gehärtetes Betriebssystem • Sicherheitsupdates	X		
Sichere Hypervisoren • Sicherheitsupdates • zertifizierte Software (Common Criteria min. EAL 4)	X		
Daten werden nur auf Systemen des CSP gespeichert und nicht an Drittanbieter ausgelagert	X		
Protokollierung aller administrativen Zugriffe	X		

Kriterienkatalog	*Ja*	*Nein*	*Bemerkungen*
Compliance			
Wo liegt der Serverstandort? • Deutschland/Europa • EWR • Drittausland (z.B. USA)	 X X 	 X	
Entspricht die Datenspeicherung von personenbezogenen Daten dem Bundesdatenschutzgesetz?	X		
Kann der Anbieter nachweisen, dass er sich an die Datenschutzrichtlinien hält?	X		
Sind Compliance-Zertifikate vorhanden? • ISO 27001/27002 • SAS 70 Typ I / Typ II • SSAE 16 / ISAE 3402 • ISO 9001	 X 	 	
Verbindliche Auskunft über den Speicherort der Kundendaten	X		
Werden interne Bereiche an Subunternehmer ausgelagert? • europäische Subunternehmer • außereuropäische Subunternehmer	 X 	 X	
Sicherheit bezüglich der Kundendaten kann in den SLA abgeklärt werden	X		
Können dritte Parteien Zugang bekommen? (Rechtsprechung, wenn Server bzw. in den USA stehen, vgl. US Patriot Act)		X	
Verbindliche Auskunft des Providers welche Personen Zugang zu den Kundendaten haben	X		
Werden für Kunden SLA (Service Level Agreements) angeboten?	X		
Ist es möglich vorhandene SLA an Kundenwünsche anzupassen?	X		
Funktionalität			
Ist eine strikte Mandantentrennung in der Cloud vorhanden?	X		
Können kurzfristig weitere Kapazitäten hinzugefügt & wieder entfernt werden, falls nötig? (Skalierbarkeit)	X		
Repräsentative Performanztests sind möglich	X		
Können Daten mit geringem Aufwand exportiert und zu einem anderen Provider migriert werden?	X		

Kriterienkatalog	*Ja*	*Nein*	*Bemerkungen*
Entstehen für eine Datenmigration zusätzliche Kosten?		X	
Können offene Formate für den Datenaustausch verwendet werden? (z.B. XML)	X		
Findet dieser Datenaustausch verschlüsselt statt? Wenn ja, wo werden die Daten ver- und entschlüsselt bzw. wo liegt der Schlüssel? (z.B. auf Anbieter-/Kundenseite)	X		
Kann mittels Single Sign-On auf die Kundenserver zugegriffen werden?	X		
Gibt es eine 2-Faktor-Authentisierung für die Kunden?	X		
Falls der Kunde „Managed Services“ bevorzugt, existiert hierfür ein effektives Patch- und Änderungsmanagement vorhanden? (schnelles Einspielen von Patches, Updates)	X		
Qualität des Services ist hochwertig (z.B. keine Bugs)	X		
Auf Anbieterseite stehen genügend Rechen- und Speicherkapazität zur Verfügung	X		
Verfügbarkeit			
Ist für Download/Upload eine ausreichende und unterbrechungsfreie Internetverbindung gewährleistet? (gute Netzqualität, geringe Latenzzeiten)	X		
Stehen dem Kunden Alternativen zur Verfügung, falls der Cloud-Service ausfallen sollte? (z.B. redundante Notfall-Server/Komponenten)	X		
Kann bei einer möglichen Insolvenz des Providers der Schutz und die Verfügbarkeit der Daten gewährleistet werden?	X		
Ist der Cloud-Service hochverfügbar? (min. 99,9%)	X		
Existiert ein ausgeprägter und professioneller Kundensupport?	X		
Vertrag			
Wie wird der Vertrag geschlossen? • Schriftlich • Online			wahlweise
Wie werden die für den Vertrag benötigten Personendaten der Kunden überprüft? • Personalausweiskopie • Sonstiges			wahlweise

Kriterienkatalog	*Ja*	*Nein*	*Bemerkungen*
Wie sehen die Laufzeiten des Vertrages aus? • Mindestlaufzeit 24 Monate • Mindestlaufzeit 12 Monate • Monatlich kündbar • Sonstiges			wahlweise
Besteht bei Vertragskündigung die Möglichkeit die Kundendaten vollständig zu löschen?	X		
Wie erfolgt die Abrechnung der Services? • Pauschal • Pay-Per-Use			wahlweise
Kann der Vertrag angepasst werden, wenn sich die Anforderungen des Kunden ändern?	X		
Ist die Auslagerung von Bereichen an Subunternehmer auf Anbieterseite vertraglich festgehalten?	X		
Datenschutzbestimmungen sind vertraglich festgehalten	X		
Die Haftung ist vertraglich festgehalten, in Bezug auf: • Nichterreichbarkeit des Cloud Services • Datenverlusten • Weitergabe von sensiblen Firmendaten	X		

Tabelle A.1.: Kriterienkatalog

Literatur

Allweyer, Thomas (2009). *BPMN 2.0 Business Process Model and Notation - Einführung in den Standart für die Geschäftsprozessmodellierung*. Books on Demand. ISBN: 978-3-8391-2134-4.

Aschenbrenner, Michael u. a. (2010). *Informationsverarbeitung im Versicherungsunternehmen*. Springer-Verlag. ISBN: 978-3642043208.

Barton, Thomas (2014). *E-Business mit Cloud Computing*. Springer Vieweg Verlag. ISBN: 978-3-8348-2425-7 (siehe S. 12).

Baun, Christian u. a. (2010). *Cloud Computing - Web-basierte dynamische IT-Services*. Springer Verlag. ISBN: 978-3-642-01593-9 (siehe S. 11, 15, 18–20, 22).

Becker, Jörg, Martin Kugeler und Michael Rosemann (2005). *Prozessmanagement – Ein Leitfaden zur prozessorientierten Organisationsgestaltung*. Springer-Verlag. ISBN: 978-3540234937.

Becker, Jörg, Christoph Mathas und Axel Winkelmann (2009). *Geschäftsprozessmanagement*. Springer-Verlag. ISBN: 978-3-540-85153-0.

Bergsmann, Stefan (2012). *End-to-End-Geschäftsprozessmanagement - Organisationselement, Integrationsinstrument, Managementansatz*. Springer Verlag. ISBN: 978-3-7091-0839-0.

BSI (2014). URL: `https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html` (besucht am 11. 10. 2014).

Fischer, Herbert, Albert Fleischmann und Stefan Obermeier (2006). *Geschäftsprozesse realisieren*. Vieweg Verlag. ISBN: 978-3-8348-0053-4 (siehe S. 27, 30, 31).

Fischer, Peter und Peter Hofer (2008). *Lexikon der Informatik*. URL: `http://ebooks.ub.uni-muenchen.de/8098/` (besucht am 12. 05. 2012).

Funk, Burkhardt u. a. (2010). *Geschäftsprozessintegration mit SAP - Fallstudien zur Steuerung von Wertschöpfungsprozessen entlang der Supply Chain*. Springer Verlag. ISBN: 978-3-642-12720-5.

Gadatsch, Andreas (2008). *Grundkurs Geschäftsprozessmanagement*. Vieweg Verlag. ISBN: 978-3-8348-0363-4 (siehe S. 29–31).

Gorecki, Pawel und Peter Pautsch (2013). *Lean Management*. Carl Hanser Verlag. ISBN: 978-3446434523.

Hummel, Thomas (2011). *Total Quality Management: Tipps für die Einführung*. Carl Hanser Verlag. ISBN: 978-3446416093.

Jobst, Daniel (2010). *Service- und Ereignisorientierung im Contact-Center - Entwicklung eines Referenzmodells zur Prozessautomatisierung*. Springer Verlag. ISBN: 978-3-8349-2487-2.

Karl, Heiko (2011). *Zugriffskontrolle in Geschäftsprozessen*. Vieweg+Teubner Verlag. ISBN: 978-3-8348-1465-4.

Komus, Ayelt (2011). *BPM Best Practice*.

Komus, Prof. Dr. (2014). *Metastudie „BPM Quintessenz“*.
URL: http://www.bpm-quintessenz.de (besucht am 28. 05. 2014).
Kroslid, Dag u. a. (2003). *Six Sigma: Erfolg durch Breakthrough-Verbesserungen*.
Carl Hanser Verlag. ISBN: 978-3446222946.
Leiting, Andreas (2012). *Unternehmensziel ERP-Einführung - IT muss Nutzen stiften*.
Springer Verlag. ISBN: 978-3-8349-4461-0.
Lissen, Nina, Christian Brünger und Stephan Damhorst (2014).
IT-Services in der Cloud und ISAE 3402. Springer Gabler Verlag. ISBN: 978-3-662-43472-7
(siehe S. 12, 13, 15, 16).
Name, Ein (2014). *Der Superduper Titel*. 1. Ausgabe. Heimverlag.
Niermann, Peter F.-J. und Andre M. Schmutte (2014).
Exzellente Managemententscheidungen - Methoden, Handlungsempfehlungen, Best Practices.
Springer Verlag. ISBN: 978-3-658-02245-7.
Preißner, Andreas (2011).
Balanced Scorecard anwenden: Kennzahlengestützte Unternehmenssteuerung.
Carl Hanser Verlag. ISBN: 978-3446425705.
Scheer, August Wilhelm (2002). *ARIS - Vom Geschäftsprozess zum Anwendungssystem*.
Springer-Verlag. ISBN: 978-3540658238 (siehe S. 31).
Scheer, August-Wilhelm, Wolfram Jost und Karl Wagner (2005).
Von Prozessmodellen zu lauffähigen Anwendungen - Aris in der Praxis. Springer-Verlag.
ISBN: 3-540-23457-8.
Scheer, August-Wilhelm, Helmut Kruppke u. a. (2006).
Agilität durch ARIS Geschäftsprozessmanagement. Springer Verlag. ISBN: 978-3-540-33358-6.
soscisurvey (). URL: https://www.soscisurvey.de (besucht am 24. 06. 2014).
Weerawarana, Sanjiva u. a. (2005). *Web Services Platform Architecture : SOAP, WSDL,
WS-Policy, WS-Addressing, WS-BPEL, WS-Reliable Messaging, and More*. Prentice Hall PTR.
ISBN: 0131488740.
Weske, Mathias (2007). *Business Process Management – Concepts, Languages, Architectures*.
Springer-Verlag. ISBN: 978-3-642-28615-5.
Wikipedia (2014). URL: www.wikipedia.com (besucht am 24. 06. 2014).

Alle URLs wurden zuletzt am 2014-11-03 geprüft.

Erklärung

Ich versichere, diese Arbeit selbstständig verfasst zu haben. Ich habe keine anderen als die angegebenen Quellen benutzt und alle wörtlich oder sinngemäß aus anderen Werken übernommene Aussagen als solche gekennzeichnet. Weder diese Arbeit noch wesentliche Teile daraus waren bisher Gegenstand eines anderen Prüfungsverfahrens. Ich habe diese Arbeit bisher weder teilweise noch vollständig veröffentlicht. Das elektronische Exemplar stimmt mit allen eingereichten Exemplaren überein.

Ort, Datum, Unterschrift