BROCKHAUS AG

CLOUD

Eignung hybrider Cloud-Modelle zur Verarbeitung personenbezogener Daten

WHITEPAPER

Pereira Azevedo, Lionel
Student IT-Consulting

Reher, David
IT-Consulting

KURZGEFASST

Die zunehmende Nutzung und Bereitstellung von Cloud-Services ist ein fester Bestandteil des Digitalisierungsprozesses und stellt für viele Unternehmen eine geeignete Möglichkeit dar, Verarbeitungsprozesse effizient und zugänglich zu gestalten. Cloud-Lösungen überzeugen dabei besonders in ihrer Flexibilität und Skalierbarkeit und finden durch das Angebot großer Cloud Service Provider häufig schnelle und unkomplizierte Anwendung. Eine der relevantesten Herausforderungen bei der Verwendung von Clouds ist die Gewährleistung eines angemessenen Datesicherheitsniveaus. Insbesondere Unternehmen aus stark regulierten Branchen wie dem Finanz- oder Gesundheitswesen, in denen mit hochsensiblen personenbezogenen Daten umgegangen wird, müssen besondere Vorkehrungen treffen, um die Datensicherheit garantieren zu können.

In diesem Whitepaper wird besonders auf die Eignung hybrider Cloud-Modelle für die Verarbeitung personenbezogener Daten, unter Berücksichtigung der europäischen Datenschutz-Grundverordnung (DSGVO), eingegangen. Neben den konzeptionellen Vorteilen von Hybrid Clouds, legen wird ein besonderes Augenmerk auf die wichtigsten Maßnahmen, die für eine DSGVO-konforme Zusammenarbeit von Unternehmen mit Cloud Service Providern notwendig sind. Basierend auf den Vorteilen von Hybrid Clouds und den erlangten Erkenntnissen der Datenschutzregelungen, geben wir abschließend eine Einschätzung zur Eignung von Hybrid Clouds für die Verarbeitung personenbezogener Daten ab.

1 WAS IST CLOUD COMPUTING?

Für den Begriff des Cloud Computing konnte bisher keine einheitliche Definition gefunden werden [1]. Eine weitestgehend akzeptierte Definition ist jedoch die des National Institute of Standards and Technology (NIST), herausgegeben durch das U.S. Department of Commerce [2,3,4]. Ihr zufolge beschreibt Cloud Computing ein Modell, welches einen ubiquitären und bequemen Zugriff über ein Netz auf einen geteilten Pool konfigurierbarer Ressourcen ermöglicht. Darunter fallen bspw. Netzwerke, Server, Speicher, Anwendungen und Dienste. Als weiteres Merkmal benennt die NIST-Definition die Einfachheit und Geschwindigkeit der Hinzuziehung und Abbestellung zusätzlicher Ressourcen und betont dabei insbesondere die Geringfügigkeit des dadurch anfallenden Aufwandes [4]. Konkret formuliert die NIST-Definition fünf essentielle Eigenschaften des Cloud Computing, die in Tabelle 1 aufgeführt sind. Im Rahmen dieses Papers unterscheiden wir dabei zwischen dem (Cloud Service) Provider (CSP; z.B. Microsoft Azure, der eine Menge von Ressourcen zur Verfügung stellt), dem (Cloud-)Nutzer (z.B. ein Unternehmen, das mithilfe des Providers ein Cloud-Modell integrieren will) und dem (Cloud-) Endnutzer.

Aus der NIST-Definition ergeben sich bereits allgemeine Vorteile des Cloud Computing, die sich etwa unter den Begriffen Skalierbarkeit, Verfügbarkeit, Flexibilität, Kosteneffizienz und Komfort zusammenfassen lassen. In Abschnitt 3 gehen wir noch einmal genauer auf die Aspekte der verschiedenen Cloud-Modelle (Private, Public und Hybrid Cloud) ein und decken weitere Vorteile, als auch eventuelle Nachteile, auf. Das Ziel wird dabei sein, einen Überblick über den generellen Nutzen von Hybrid Clouds zu erhalten. Da im Rahmen dieses Papers gerade die Datensicherheit eine wichtige Rolle spielt, werden in Abschnitt 3 insbesondere die Sicherheitsaspekte adressiert. Anschließend erfolgt eine Bewertung der Eignung von Hybrid Clouds zur Speicherung personenbezogener Daten unter Berücksichtigung der DSGVO. Der nachfolgende Abschnitt thematisiert jedoch zunächst die verschiedenen Service-Modelle.

All diese Aspekte sollen dazu führen, die beteiligten Teams, Tools und Infrastrukturen optimal aufeinander abzustimmen, um Anwendungen in schnelleren Zyklen und in besserer Qualität auszuliefern oder weiterzuentwickeln. Mit Hilfe des DevOps-Modells möchte man sowohl die Anzahl der Deployments durch kürzere Release-Zyklen als auch die Stabilität der jeweiligen Systeme steigern. Durch die enge Zusammenarbeit können bereits bei der Entwicklung Voraussetzungen für einen reibungslosen Betrieb geschaffen werden. So müssen nicht erst im Nachhinein vermeidbare Fehler behoben werden.

CHARAKTERISTIKA DES CLOUD COMPUTING

EIGENSCHAFT	BESCHREIBUNG
On-demand self-service	Der Cloud-Nutzer ist dazu in der Lage, eigenständig und nach Bedarf zusätzliche Ressourcen wie Rechenleistung und Speicher in Anspruch zu nehmen. Dieser Prozess geschieht weitestgehend automatisch und bedarf keiner menschlichen Interaktion mit dem Provider.
Broad network access	Cloud-Lösungen sind allgemein über das jeweilige Netzwerk verfügbar. Der Zugriff erfolgt dabei über Standardmechanismen, die eine heterogene Nutzung durch verschiedene Client-Plattformen wie Handys, Laptops, Tablets und Workstations fördern.
Resource pooling	Die Ressourcen des Providers sind gepoolt. Das bedeutet, dass die verschiedenen Ressourcen mehreren Cloud-Nutzern zur Verfügung stehen und je nach Nachfrage neu zugeteilt werden (multi-tenant model). Über den exakten Speicherort der Daten hat der Nutzer zunächst keine Kontrolle, kann diesen jedoch beispielsweise auf Land, Bundesland oder Rechenzentrum beschränken. Beispiele für gepoolte Ressourcen sind Speicher, Rechenzeit und Bandbreite.
Rapid elasticity	Die Inanspruchnahme und Wiederfreigabe von Ressourcen geschieht schnell und flexibel, sodass eine zügige Skalierung der Cloud entsprechend der Nachfrage möglich ist. Aus Nutzersicht erscheinen die Ressourcen dabei unendlich.
Measured service	Die Optimierung der Ressourcennutzung in Cloud-Systemen erfolgt automatisch und effizient. Mithilfe geeigneter Mechanismen kann die Nutzung einzelner Ressourcen überwacht, kontrolliert und gemessen werden, woraus eine allgemein hohe Transparenz für Provider und Nutzer resultiert. Gängige Bezahlmodelle bei Cloud-Systemen sind pay-per-use und charge-per-use (siehe hierzu auch Begriff operational expenditures).

Tabelle 1: Die fünf essentiellen Charakteristika des Cloud Computing nach NIST-Definition [4,2].

2 SERVICEMODELLE UND SHARED RESPONSIBILITY

Ein weiterer Teil der NIST-Definition bezüglich Cloud Computing sind die drei sogenannten Servicemodelle [4] Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Diese Modelle realisieren das Konzept Everything as a Service (XaaS), bei dem sich Nutzer nach Bedarf Infrastruktur, Entwicklungsplattformen bzw. fertige Software von einem Provider auf pay-per-use-Basis zur Verfügung stellen lassen können. Die Servicemodelle sind also das service-basierte Gegenstück des klassischen On-Premises-Nutzungsmodells. Je nach Bedarf und Anwendungsszenario kann eines dieser Modelle genutzt werden, um Kontrolle über verschiedene Bereiche der verwendeten Infrastruktur zu erhalten. Das Servicemodell entscheidet demnach darüber, ob die Verantwortung bezüglich des Risikomanagements eines Bereichs beim Cloud-Nutzer oder beim Provider liegt bzw. ob diese sich die Verantwortung teilen. Daher rührt auch der Begriff der „Shared Responsibilty". Abbildung 1 stellt die Verantwortungsbereiche bei den Servicemodellen grafisch gegenüber. Der Begriff der „Verantwortung" bezeichnet in diesem Abschnitt nicht die Verantwortung im rechtlichen Sinne. Details bezüglich rechtlicher Regelungen werden in Abschnitt 4 thematisiert.

IaaS

Bei IaaS wird die Infrastruktur des Cloud Service Provider (CSP) als solche angeboten und kann nach Bedarf vom Nutzer gemietet werden, um beliebige Software wie Applikationen und Betriebssysteme zu betreiben. Die zur Verfügung gestellten Ressourcen umfassen dabei u.a. Rechenleistung, Speicher und Netzwerke [4]. Nach NIST-Definition erhält der Nutzer so die Kontrolle über Betriebssysteme, Speicher und eingesetzte Applikationen ohne Zugriff auf die darunterliegende Infrastruktur zu erhalten. Abbildung 1 zeigt das mittels einer Shared Responsibility auf Ebene der Host-Infrastruktur. Im Vergleich zum klassischen On-Premises-Nutzungsmodell muss sich der Nutzer nicht mehr um die physische Sicherheit kümmern, da die Hardware in den Rechenzentren des CSP lokalisiert ist.

PaaS

Das Servicemodell PaaS wird genutzt, um Nutzern eine komfortable Plattform zum Entwickeln, Testen und Ausliefern von Softwareprodukten zu bieten und richtet sich daher eher an Entwickler [5,1]. Der Nutzer erhält dabei lediglich die Kontrolle über abgelegte Applikationen und möglicherweise über die Konfiguration der vom Provider unterstützten Werkzeuge, die der Schaffung einer geeigneten Entwicklungsumgebung dienen [4]. Wie Abbildung 1 zeigt, liegt das Risikomanagement konträr zu IaaS sowohl bezüglich der Infrastruktur und Netzwerkebene als auch der Host-Infrastruktur nicht mehr in der Verantwortung des Nutzers.

SaaS

SaaS abstrahiert noch eine weitere Ebene von PaaS und übergibt den Großteil der Verantwortung bezüglich des Risikomanagements an den CSP. Bei SaaS wird dem Nutzer eine Auswahl fertiger Anwendungen zur Verfügung gestellt, die nach Bedarf vom Nutzer eingesetzt werden können. Im Gegensatz zu PaaS muss sich dabei von Seiten des Nutzers neben dem Identity und Access Management, nur noch um die

Client- und Endpoint Security sowie die Datenklassifizierung und -Verantwortung gekümmert werden. Dabei hat er lediglich eingeschränkte Kontrolle über die Konfigurationsmöglichkeiten der Applikationen [4].

Ein wesentlicher Vorteil, der sich aus dem Angebot dieser Servicemodelle ergibt, ist die Vereinfachung der Umsetzung von Cloud-Lösungen. Je nach Anwendungsfall kann der Nutzer entscheiden, wie viel Kontrolle er über das System benötigt, und redundante Verwaltungsaufwände an den Provider abtreten. Darüber hinaus muss der Nutzer keine eigene Hardware beschaffen, sondern bekommt diese (ggf. eigens konfiguriert) vom Provider zur Verfügung gestellt, wodurch gerade frühe Entwicklungsprozesse enorm beschleunigt werden. Die flexiblen Konfigurationsmöglichkeiten sorgen dabei - insbesondere unter Berücksichtigung des pay-per-use Kostenmodells - zusätzlich für erhebliche Kostenersparnisse [1].

Das Shared-Responsibility-Prinzip basiert auf der Unterteilung der Verantwortungbereiche und erzeugt somit ein Vertrauensverhältnis zwischen Cloud-Nutzer und Provider.

Je nach Servicemodell übernimmt der CSP zwar weite Teile des nötigen Verwaltungsaufwands, allerdings gibt der Nutzer mit steigendem Komfort auch zunehmend die Kontrolle über gespeicherte Daten ab. Während er bei IaaS die größte Kontrolle über die Datensicherheit besitzt, teilt er sich diese bei PaaS mit dem Provider und gibt sie bei SaaS sogar beinahe vollständig ab. Gegebenenfalls ist die Speicherung der Daten in der Cloud jedoch sogar sicherer als die Speicherung auf firmeninternen Speichermedien. Viele Cloud Service Provider lassen sich nachweislich zertifizieren (bspw. bzgl. physischer Datensicherheit) und unterliegen Auditing-Prozessen, die sie zur Einhaltung gesetzlicher Vorschriften bewegt [1]. Nichtsdestotrotz ist ein reines Vertrauensverhältnis vor allem im Kontext der Speicherung personenbezogener Daten, mit Vorsicht zu genießen. Welche Maßnahmen für eine angemessene Datenverarbeitung unter Berücksichtigung der Vorschriften der DSGVO - speziell in der EU - notwendig sind, wird in Abschnitt 4 behandelt. Zunächst werden jedoch die für dieses Paper relevantesten Cloud-Typen erläutert.

Abbildung 1: Gegenüberstellung der Verantwortungsbereiche bei den verschiedenen Servicemodellen; Grafik entnommen aus https://www.netzwoche.ch/

3 CLOUD-LIEFERMODELLE

Drei der gängigsten Cloud-Typen (auch Liefermodelle oder deployment models genannt) sind die Public Cloud, die Private Cloud und die Kombination dieser beiden, die Hybrid Cloud. Um die Funktionsweise und den Mehrwert einer hybriden Cloud besser verstehen können, muss zunächst über die Eigenschaften ihrer Bestandteile aufgeklärt werden. Dazu werden in den folgenden Unterabschnitten grundlegende Vor- und Nachteile von Private und Public Clouds, bezüglich zuvor genannter Cloud-Merkmale wie beispielsweise Flexibilität, Skalierbarkeit, Kosten und kennzeichnende Sicherheitsaspekte, gegenübergestellt.

3.1 Public Clouds

Die prägende Eigenschaft von Public Clouds ist ihre öffentliche Zugänglichkeit über das Internet. Anders als bei Private Clouds, die nur einer ausgewählten Anzahl von Personen zur Verfügung stehen, bieten Public Clouds jedem, der ein kompatibles Gerät besitzt, Zugriff auf den bereitgestellten Dienst [1,4]. Per NIST-Definition befindet sich dabei die verwendete Infrastruktur – und somit auch jegliche gespeicherten Daten – in den Räumlichkeiten des Providers [4].

Zu den wesentlichen Vorteilen von Public Clouds zählen Skalierbarkeit, Verfügbarkeit, Zuverlässigkeit, Flexibilität und Kosteneffizienz. Basierend auf dem pay-per-use Kostenmodell, werden vom Nutzer immer nur die Ressourcen bezahlt, die auch genutzt werden. Dadurch wird Kosten durch ungenutzte Ressourcen entgegengewirkt und ein hoher Effizienzgrad erreicht [4]. Des Weiteren können, bei überdurchschnittlicher Nutzung eines Public-Cloud-Dienstes, zusätzliche Ressourcen hinzugezogen und anschließend wieder freigegeben werden, was sie beispielsweise von Private Clouds unterscheidet. Ein zusätzlicher Vorteil von Public Clouds ist die Verfügbarkeit in Bezug auf Zuverlässigkeit. Viele CSP verfügen über eine genügend große Redundanz an Ressourcen, die es ihnen ermöglicht, Notfälle entsprechend zu behandeln. Zur Prävention gegen Datenverlust legt Microsoft Azure beispielsweise lokale, zonale und regionale Datenkopien an, die zur Wiederherstellung der Originaldaten dienen [6]. Während der Wartung oder etwaiger Ausfälle werden die entsprechenden Ressourcen durch andere Rechner im selben oder in anderen Rechenzentren zur Verfügung gestellt. Ein weiterer Vorteil von Public Clouds ist der bereits erwähnte Komfort. So müssen sich Nutzer beispielsweise nicht um die physische Sicherheit der Daten, die Investition in eigene Hardware und deren Wartung oder den Erwerb etwaiger Sicherheitszertifikate kümmern, wodurch zusätzlich anfallende Kosten – beispielsweise durch dediziertes Sicherheitspersonal in monetärer Form oder auch in Form von Zeitverlust – vermieden werden können.

Aufgrund der Tatsache, dass sich Infrastruktur und die Gesamtheit aller Daten auf den Rechenzentren des CSP befinden, begeben sich Nutzer von Public Clouds in direkte Abhängigkeit vom jeweiligen Provider. Der daraus resultierende Kontrollverlust (loss of control) über gespeicherte Daten ist gerade für Unternehmen in stark regulierten Branchen wie im Finanz- und Gesundheitswesen besonders kritisch, da die Datenverwaltung und Zugriffskontrolle allein durch den CSP erfolgt und lediglich auf gegenseitigem Vertrauen basiert. Bei Änderungen rechtlicher Gesetzeslagen müssen sich Nutzer darauf verlassen, dass die jeweiligen Anbieter diese schnellstmöglich implementieren.

Geschieht dies nicht, kann es zu Problemen bei der Aufrechterhaltung bzw. der laufenden Migration bestehender Cloud-Dienste kommen.

Charakteristisch für die Datenspeicherung in Public Clouds ist die heterogene Speicherumgebung. Das bedeutet, dass der exakte Speicherort bestimmter Daten im Normalfall unbekannt ist und die Daten verschiedener Nutzer möglicherweise auf derselben Speicherressource liegen. Diese Heterogenität resultiert daraus, dass sich mehrere Public-Cloud-Dienste den Speicherplatz teilen. Eine unklare Trennung der Daten in den Rechenzentren ist das Ergebnis (multi-tenant model).

Aufgrund des Mangels an Kontrolle über die Datenspeicherung, der heterogenen Speicherumgebung und des öffentlichen Zugangs über das Internet, werden Public Clouds häufig gerade in Bezug auf die DSGVO als zu unsicher angesehen. Hinzu kommt die erhöhte Anfälligkeit für Sicherheitslecks. Die Public Cloud eignen sie sich daher nur bedingt zur Verarbeitung personenbezogener Daten [7], da die DSGVO strenge Richtlinien bezüglich des Speicherorts der Daten formuliert. Dennoch kann ein Großteil der aufgeführten Vorteile der Public Cloud im Hybrid-Modell genutzt werden.

Der zweite Bestandteil einer Hybrid Cloud ist die Private Cloud. Durch welche Eigenschaften sie sich auszeichnet und in welchen Aspekten sie sich von der Public Cloud unterscheidet, erläutern wir im folgenden Unterabschnitt genauer.

3.2 Private Clouds

Die Definition von Private Cloud unterscheidet sich je nach Quelle oft leicht. Dennoch gibt es in allen Quellen gemeinsame Merkmale, über die sich Private Clouds definieren lassen. Wie ihr Name vermuten lässt, sind Private Clouds – konträr zur Public Cloud – nicht über das öffentliche Internet erreichbar, sondern stehen häufig nur einer eingeschränkten Anzahl von Person zur Verfügung. Diese Personen können beispielsweise einer oder mehrerer Organisationen, Bildungs- oder Regierungsinstitutionen angehören. Auch Kombinationen sind möglich [4]. Insgesamt wird zwischen vier Typen unterschieden, die u.a. über die Art der Speicherung der Daten und den Bezug der Ressourcen bestimmen [8]:

- Internal Private Cloud:
Hierbei betreibt das Unternehmen selbst die notwendige IT-Infrastruktur im eigenen Gebäude. Diese Form der Private Cloud entspricht dem klassischen On-Premises-Nutzungsmodell.
- Managed Private Cloud:
Auch hier verbleibt die Infrastruktur im Unternehmen, wird aber durch einen externen Anbieter gemanagt bzw. gewartet.
- Hosted Private Cloud:
Ein Cloud-Services-Anbieter betreibt die Cloud im Auftrag des Unternehmens in einem Rechenzentrum.
- Community Private Cloud:
Hier greifen mehrere Unternehmen – etwa einer Branche oder eines Konzerns – auf die gleiche Cloud zu.

Ein wesentlicher Vorteil von Private Clouds gegenüber Public Clouds ist die mögliche Unabhängigkeit von externen CSP beispielsweise durch Nutzung einer Internal Private Cloud. Auf diese Weise behält der Cloudbetreiber (nicht der CSP!) die volle Kontrolle über Speicherung und Zugriffsberechtigungen und kann so eine höhere Datensicherheit gewährleisten. Sicherheitsrisiken, die bei der Verwendung von Public Clouds bestehen, treten so nicht auf und individuelle Sicherheitsanforderungen von Kunden können leicht implementiert

Public Cloud vereinigen und so einen Einsatz im Finanz- und Gesundheitswesen ermöglichen. Im folgenden Abschnitt wird der Einsatz von Hybrid Clouds insbesondere unter Berücksichtigung deutscher Datenschutzgesetze beleuchtet und auf mögliche Sicherheitsrisiken aufmerksam gemacht.

3.3 Hybrid Clouds

Hybrid Clouds sind eine Kombination aus je mindestens einer Private und Public Cloud und beziehen ihre Motivation aus der effektiven Nutzung aller Vorteile dieser beiden Grundbausteine. Die Idee hinter einer Hybrid Cloud in Bezug auf Datensicherheit ist dabei die Trennung datenschutzkritischer und -unkritischer Verarbeitungsprozesse, wobei erstere in der stark regulierten Umgebung der Private Cloud und letztere in der flexiblen, frei zugänglichen Public Cloud ablaufen. Durch die Kommunikation zwischen Public und Private Cloud werden so die Sicherheitsrisiken der beiden elementaren Cloudtypen minimiert und dadurch die Sicherheit der Daten und ihrer Verarbeitung maximiert.

Vor dem Hintergrund der Datensicherheit profitiert das Hybrid-Cloud-Modell im Wesentlichen von zwei Merkmalen: der Sicherheit der Private Cloud und der Rechenkapazität der Public Cloud. Datenunkritische Prozesse können dabei auf die skalierbare und flexible Public Cloud ausgelagert werden, um Abläufe zu optimieren und Kosten (die etwa bei einem rein privaten Modell anfallen würden) zu minimieren, während datenkritische Verarbeitungsprozesse in der isolierten Private Cloud ablaufen. Da gerade in stark regulierten Branchen häufig lokale Datenschutzrichtlinien vorliegen, die möglicherweise nicht durch einen CSP gewährleistet sind, ermöglicht die Private-Cloud-Komponente eine schnelle Implementierung solcher Richtlinien. Einher mit den Vorteilen der Hybrid Cloud gehen einige administrative Zusatzaufgaben, wie beispielsweise die Identifikation und Trennung kritischer bzw. unkritischer Vorgänge und die Regulierung der Kommunikation zwischen Private- und Public-Cloud-Komponenten.

Im Allgemeinen besitzen Hybrid Clouds also ein großes Potential hinsichtlich des Umgangs mit sensiblen Daten, da sie die Sicherheit und Kontrolle der Private Cloud mit der Flexibilität und Skalierbarkeit der Public Cloud vereinigen und so einen Einsatz im Finanz- und Gesundheitswesen ermöglichen. Im folgenden Abschnitt wird der Einsatz von Hybrid Clouds insbesondere unter Berücksichtigung deutscher Datenschutzgesetze beleuchtet und auf mögliche Sicherheitsrisiken aufmerksam gemacht.

4 EINHALTUNG DER DSGVO IN HOSTED-CLOUD-MODELLEN

Wie in den vorigen Abschnitten bereits erläutert, bringt die Inanspruchnahme der Services von Cloud Service Providern viele Vorteile mit sich, da im Falle der Hosted Private Cloud Server-Wartungen und die physische Datensicherheit nicht mehr in den direkten Verantwortungsbereich des Nutzers fallen. Neben der Entlastung des Cloud-Nutzers bedeutet die Zusammenarbeit der beiden Parteien allerdings auch einen aus rechtlicher Sicht komplexen Anwendungsfall. Ziel dieses Abschnitts ist die Beleuchtung der europäischen Datenschutzrichtlinien bezüglich der Verarbeitung personenbezogener Daten unter Betrachtung der im Mai 2018 in Kraft getretenen Datenschutz-Grundverordnung (DSGVO).

In Abschnitt 4.1 erläutern wir zunächst die wichtigsten im Kontext der DSGVO verwendeten Begriffe und stellen einen Bezug zu den Begriffen des Cloud Computing her, um Sachverhalte möglichst nah an den gegebenen Richtlinien erörtern zu können. Anschließend werden in Abschnitt 4.2 die wichtigsten Maßnahmen erläutert, die für eine DSGVO-konforme Zusammenarbeit notwendig sind. Darüber hinaus gehen wir auf die Verantwortlichkeitsbereiche von Cloud-Provider und Nutzer und die damit einhergehenden Pflichten ein. Der Fokus liegt dabei speziell auf den für die Zusammenarbeit von Cloud-Nutzer und Cloud-Provider formulierten Regelungen. In Abschnitt 4.3 wird danach grob auf die Haftbarkeit von Provider und Nutzer eingegangen. Abschnitte 4.4 und 4.5 thematisieren jeweils die Regelungen bezüglich der Übermittlung personenbezogener Daten und die Existenz von Zertifizierungen, die die Beurteilung geeigneter Provider seitens des Nutzers erleichtern sollen. Abschließend wird in Abschnitt 4.6 ein kurzes Fallbeispiel besprochen. Sofern nicht anders gekennzeichnet, verweisen Angaben zu Artikeln und Absätzen immer auf die der DSGVO [9].

4.1 Terminologie

Das Konzept von Hosted-Cloud-Modellen fällt im Rahmen der DSGVO unter die sogenannte Auftragsverarbeitung, deren zugehörige Richtlinien in Kapitel 4 Art. 24-43 DSGVO zu finden sind. Diese beschreibt allgemein ein Arbeitsverhältnis zwischen Verantwortlichen und Auftragsverarbeitern, bei dem Letzterer für die Verarbeitung von Daten durch den Verantwortlichen beauftragt wird. Im Kontext des Cloud Computing fällt dementsprechend der Nutzer in die Rolle des Verantwortlichen und der CSP in die des Auftragsverarbeiters, weshalb diese in den kommenden Abschnitten auch synonym verwendet werden. Die folgenden Absätze dienen noch einmal der förmlichen Definition dieser beiden Parteien sowie des Begriffs der personenbezogenen Daten gemäß Art. 4 der DSGVO.

Als Verantwortlicher wird im Rahmen der DSGVO diejenige „[...] natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle [bezeichnet], die allein oder gemeinsam mit anderen über die Zwecke und Mittel zur Verarbeitung personenbezogener Daten entscheidet“ [9].

Der Auftragsverarbeiter bezeichnet „[...] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“ [9].

Als personenbezogene Daten werden alle Informationen bezeichnet, „[...] die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“ [9].

Basierend auf den hier genannten Begrifflichkeiten wird im nachfolgenden Abschnitt auf die wichtigsten Maßnahmen eingegangen, die für eine datenschutzrechtlich angemessene Verarbeitung der Daten notwendig sind.

4.2 Maßnahmen für DSGVO-konforme Zusammenarbeit

Damit eine Auftragsverarbeitung nach der DSGVO vorliegt, muss gemäß Art. 28 Abs. 3 zwischen Cloud-Nutzer und Provider ein Vertrag über die weisungsgebundenen Tätigkeiten geschlossen werden [9,10,11]. Dieser Vertrag kann nach Art. 28 Abs. 9 in Papierform oder elektronisch geschlossen werden und legt sowohl organisatorische als auch technische Maßnahmen fest, die von den jeweiligen Parteien zu ergreifen sind, um die Sicherheit der Datenverarbeitung gemäß der DSGVO zu gewährleisten. Des Weiteren garantiert der Vertrag die Einhaltung der in der DSGVO beschriebenen Grundsätze (Art. 5 - 11) und Pflichten zum Schutz personenbezogener Daten, die gespeichert und verarbeitet werden. Die DSGVO ist dabei so ausgelegt, dass sowohl Verantwortlicher als auch Auftragsverarbeiter ein Interesse daran haben, den Vertrag sorgfältig auszuarbeiten. Ein unzureichend ausgestalteter Vertrag führt dazu, dass keine Auftragsverarbeitung im Sinne der DSGVO vorliegt und die Übertragung von Daten an einen Provider vor diesem Hintergrund als unberechtigte Datenübergabe an Dritte behandelt wird [11]. Der folgende Abschnitt soll einen Überblick über die zu beachtenden Aspekte und Pflichten von Cloud-Nutzern und Providern geben.

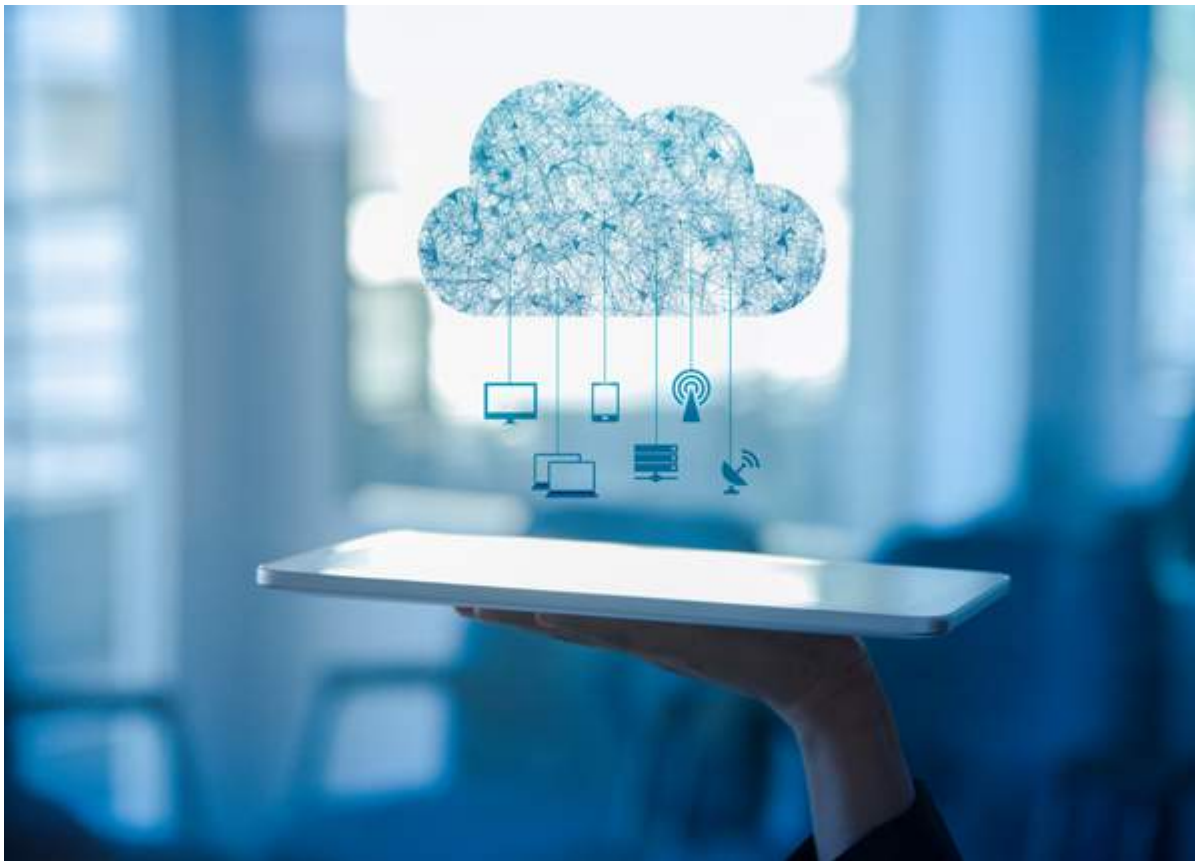
Gemäß Art. 28 Abs. 1 hat in erster Linie der Cloud-Nutzer dafür Sorge zu tragen, dass er ausschließlich mit Auftragsverarbeitern zusammenarbeitet, „[...] die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen [der DSGVO] erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“ [9]. Diese Festlegung fundiert auf dem Grundsatz, dass die Datenverarbeitung des Auftragsverarbeiters strikt weisungsgebunden durch den Verantwortlichen passieren muss. Das bedeutet, dass Cloud-Nutzer zunächst die Verantwortung für Zweck und Mittel der Verarbeitung und somit die DSGVO-Konformität der vertraglichen Rahmenbedingungen tragen. Gemäß Art. 24 Abs. 1 ist er dazu verpflichtet die Einhaltung der DSGVO unter Berücksichtigung der Art, des Umfangs und dem Zweck der Verarbeitung sowie Eintrittswahrscheinlichkeiten und Schwere von Risiken für Rechte und Freiheiten betroffener Personen nachweisen zu können [9] . Ziel eines Vertrags gemäß Art. 28 ist die Bindung des Auftragsverarbeiters an die Datenschutzstandards der DSGVO und die Festlegung der Zusammenarbeit von Verarbeiter und Verantwortlichem. Dazu werden auch dem Auftragsverarbeiter entsprechende Pflichten auferlegt, die in Art. 28 Abs. 3 genauer formuliert sind. Tabelle 2 fasst die aufgeführten Aspekte einmal zusammen.

Die Haftungsregelung bei Verstoß gegen Datenschutzrichtlinien im Bereich der Auftragsverarbeitung wird in Abschnitt 4.3 separat beleuchtet.

Die in Art. 5 Abs. 1 aufgeführten „Grundsätze für die Verarbeitung personenbezogener Daten“ umfassen mehrere Bereiche, darunter unter anderem die Datenminimierung (c), Richtigkeit (d) und Vertraulichkeit und Integrität (f) [9]. Im Kontext der Auftragsverarbeitung ist dabei insbesondere der erste der Grundsätze von Relevanz, nämlich der der Rechtmäßigkeit und Transparenz (a). Hierbei sind insbesondere die notwendigen Maßnahmen zur Gewährleistung der Transparenz von Verarbeitungsprozessen interessant, da diese für den Einhaltungsnachweis der DSGVO-Richtlinien essentiell sind.

Um die Datenverarbeitung also möglichst nachvollziehbar zu gestalten, erlegt die DSGVO sowohl Verantwortlichen als auch Auftragsverarbeitern Dokumentationspflichten auf, die nicht nur zur Selbstkontrolle, sondern auch zur Kontrolle durch berechtigte Behörden dienen. Die Inhalte dieser sog. Verarbeitungsverzeichnisse sind für Verantwortliche in Art. 30 Abs. 1 und für Auftragsverarbeiter in Abs. 2 geregelt. Tabelle 3 stellt die inhaltlichen Unterschiede grob gegenüber.

Sowohl Auftragsverarbeiter als auch Verantwortliche müssen gemäß Art. 30 Abs. 4 ihre Verarbeitungsverzeichnisse auf Anfrage der Behörde zur Verfügung stellen. Auf diese Weise wird sichergestellt, dass die technischen und organisatorischen Maßnahmen zum Schutz der Daten im Sinne der DSGVO gewährleistet sind.



PFLICHTEN DES CSPS (AUFTRAGSVERARBEITERS)

STICHWORT	BESCHREIBUNG
Weisungsgebundenheit	Der Auftragsverarbeiter (AV) verarbeitet die Daten nur so, wie es vertraglich mit dem Verantwortlichen festgelegt ist. Ist der AV nicht durch das Recht der EU bzw. ihrer Mitgliedstaaten dazu verpflichtet, muss dies dem Verantwortlichen vor der Verarbeitung mitgeteilt werden (Art. 28 Abs. 3a).
Vertraulichkeit & Verschwiegenheit	Der AV muss gewährleisten, dass sich Personen mit Befugnis zur Verarbeitung von personenbezogenen Daten als vertraulich verpflichtet haben oder einer Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3b).
Sicherheit der Verarbeitung	Der AV ergreift alle sicherheitstechnischen Maßnahmen zur Gewährleistung einer sicheren Datenverarbeitung gemäß Art. 32. Das umfasst u.a. die Berücksichtigung des Stands der Technik, Zwecke und Umstände der Verarbeitung, Pseudonomisierung und Verschlüsselung personenbezogener Daten, Vertraulichkeit und Verfügbarkeit der Dienste, Datenvernichtung und Risiko-abschätzungen (Art. 28 Abs. 3c).
Kooperation	Der AV unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht, den in Kapitel 3 der DSGVO geschilderten Rechten der betroffenen Person nachzukommen (Art. 28. Abs. 3e). Zusätzlich unterstützt er den Verantwortlichen in angemessener Weise bei der Einhaltung seiner Pflichten bezüglich der Sicherheit bei der Verarbeitung, der Folgenabschätzung und Meldung von Daten-pannen sowie der Benachrichtigung betroffener Personen bei Datenschutzverletzungen gemäß Art. 32-36 (Art. 28. Abs. 3f).
Löschung	Sobald die vereinbarten Verarbeitungsleistungen erbracht wurden, gibt der AV die Daten an den Verantwortlichen weiter und löscht jegliche angefertigte Kopien derselben - sofern nicht anders durch das EU-Recht vorgeschrieben (Art. 28. Abs. 3g).
Transparenz	Der AV informiert den Verantwortlichen, wenn er ein Subunter-nehmen in den Verarbeitungsprozess einbeziehen möchte und benötigt dafür eine schriftliche Genehmigung des Verantwort-lichen (Art. 28. Abs. 3d). Weitergehend stellt der Auftragsver-arbeiter dem Verantwortlichen alle notwendigen Informationen zur Verfügung, die als Nachweis zur Einhaltung der Pflichten notwendig sind (Art. 28. Abs. 3h).

Tabelle 2: Vertraglich festgelegte Pflichten des Auftragsverarbeiters gemäß Art. 28 [9]

INHALTE DER VERARBEITUNGSVERZEICHNISSE

NUTZER-SEITE	CSP-SEITE
■ Name und Kontaktdaten (eigene, des Vertreters und des Datenschutz-beauftragten) ■ Zwecke der Verarbeitung ■ Beschreibung der Kategorien betroffener Personen und personenbezogener Daten ■ Kategorien von Empfängern gesammelter personenbezogenen Daten ■ ggf. Übermittlung personenbezogener Daten an Drittländer unter Berücksichtigung von Art. 49 Absatz 1 ■ wenn möglich, Fristen für Löschung verschiedener Datenkategorien ■ wenn möglich, Beschreibung der organisatorischen und technischen Maßnahmen zur Sicherheit gemäß Art. 32 Abs. 1	■ Name und Kontaktdaten (eigene, des Vertreters und des Datenschutz-beauftragten) ■ Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden ■ ggf. Übermittlung personenbezogener Daten an Drittländer unter Berücksichtigung von Art. 49 Absatz 1 ■ wenn möglich, Beschreibung der organisatorischen und technischen Maßnahmen zur Sicherheit gemäß Art. 32 Abs. 1

Tabelle 3: Inhaltliche Gegenüberstellung der Verarbeitungsverzeichnisse nach Art. 30 DSGVO

4.3 Haftung

Bei Verstößen gegen die Datenschutzrichtlinien der DSGVO sieht Art. 82. Abs. 4 vor, dass Auftragsverarbeiter und Verantwortlicher zunächst gesamtschuldnerisch haften, sofern beide an der Verarbeitung beteiligt und gemäß Abs. 2-3 für „[...]einen durch die Verarbeitung verursachten Schaden verantwortlich [sind]“ (Art. 82 Abs. 4) [9,11]. Das bedeutet, dass - speziell im Bereich des Cloud Computing - sowohl der Cloud-Nutzer für Verstöße seitens des Providers als auch der Provider für Verstöße seitens des Cloud-Nutzers, strafrechtlich belangtwerden kann [11,9]. In diesem Punkt findet sich also in gewisser Weise das Prinzip der Shared Responsibility wieder. Die Haftbarkeit des Auftragsverarbeiters ist dabei direkt abhängig von den gemäß Art. 28 vertraglich festgehaltenen Vereinbarungen, Pflichten und Weisungen im Rahmen der Auftragsverarbeitung. Gemäß Art. 82 Abs. 2 kann die Haftung des Providers nämlich begrenzt werden, sofern er nachweislich im Sinne der ihm auferlegten Pflichten der DSGVO gehandelt hat und allen Anweisungen bezüglich der Verarbeitung dem Cloud-Nutzer gefolgt ist. Gemäß Art. 82. Abs. 3 ist jedoch auch der Cloud-Nutzer dazu in der Lage, sich von der Haftung zu befreien, wenn er vorlegen kann, dass er „[...] in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“ [9]. Diese Regelungen betonen noch einmal zusätzlich die

Wichtigkeit einer sorgfältigen Ausarbeitung des Vertrags zur Auftragsverarbeitung gemäß Artikel 28. Beide Seiten sollten möglichst klare und realisierbare Vereinbarungen treffen, um ihren jeweiligen Pflichten nachzukommen und etwaigen Bußgeldern entgegenzuwirken.

Die nach Art. 83 verhängten Geldbußen bei Verstoß gegen die Richtlinien der DSGVO sind gemäß Absatz 3 „[...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ [9]. Die exakten Bußgelder für Verstöße gegen die einzelnen Aspekte der DSGVO sind dabei im Wesentlichen in den Absätzen 4-6 verfasst und liegen bei bis zu 10.000.000 - 20.000.000€ bzw. bei bis zu 2-4% des weltweit erzielten Jahresumsatzes eines Unternehmens.

In Art. 83 Abs. 4a werden zunächst die Bußgelder festgelegt, die anfallen, sollten Verantwortliche bzw. Auftragsverarbeiter gegen die ihnen auferlegten Pflichten verstoßen. Dabei bezieht sich der Absatz auf die Art. 8, 11, 25-39, 42 und 43 und somit unter anderem auf die Aspekte Sicherheit der Verarbeitung, Führung von Verarbeitungsverzeichnissen, Informationspflichten, Meldepflichten bei Datenpannen, Risiko- und Folgenabschätzungen sowie Stellung und Aufgaben eines Datenschutzbeauftragten. Liegt ein Verstoß bei einem dieser Punkte vor, kann ein Bußgeld in Höhe von bis zu 10.000.000€ bzw. von bis zu 2% des weltweit erzielten Jahresumsatzes anfallen. Der fällige Betrag ist dabei der höhere der beiden.

Noch härter als die in Art. 83 Abs. 4a genannten Verletzungen von Pflichten, werden Verstöße gegen die Grundsätze der DSGVO und die Rechte der betroffenen Personen geahndet. Gemäß Art. 83 Abs. 5 werden Verstöße gegen die in Art. 5-9 aufgeführten Grundsätze, die Rechte der betroffenen Personen gemäß der Artikel 12-22 und die Datenübermittlung an Drittstaaten nach Art. 44-49, mit Bußgeldern in Höhe von bis zu 20.000.000€ bzw. von bis zu 4% des weltweit erzielten Jahresumsatzes bestraft. Der anfallende Betrag ist dabei auch hier der höhere der beiden. Ähnliche Geldbußen fallen gemäß Art. 83 Abs. 6 an, wenn Anweisungen von Aufsichtsbehörden gemäß Art. 85 Abs. 2 nicht befolgt werden.

4.4 Datenübermittlung an Drittländer

Die DSGVO trifft genaue Vorschriften bezüglich der Datenübermittlung an Drittländer. So wird in Art. 44ff eine Übermittlung von Daten an ein Unternehmen, eine Behörde o.Ä. mit Sitz außerhalb der EU nur unter bestimmten Voraussetzungen erlaubt [9]. Eine Besonderheit bilden Länder, für die die EU-Kommission gemäß Art. 45 eine Angemessenheitsentscheidung erlassen hat. Dazu prüft die Kommission die Datensicherheitsstandards eines Landes oder eines spezifischen Sektors hinsichtlich politischer, rechtlicher und organisatorischer Mechanismen, die einen Einfluss auf die Sicherheit im Umgang mit personenbezogenen Daten haben. Die in Art. 45 Abs. 2 beachteten Aspekte umfassen u.a. die Achtung von Menschenrechten und Grundfreiheiten, die öffentliche und nationale Sicherheit, allgemeine Vorschriften zum Umgang mit personenbezogenen Daten, die Existenz und Funktionsweise von Aufsichtsbehörden sowie deren Unabhängigkeit, Zugriffsmöglichkeiten von Behörden auf Daten und bereits eingegangene internationale Verpflichtungen im Kontext der Verarbeitung personenbezogener Daten [9]. Ob und welche Voraussetzungen für die Datenübermittlung an Drittländer erfüllt sein müssen, ist abhängig davon, ob ein Angemessenheitsbeschluss für das entsprechende Land vorliegt oder nicht. Dazu wird in zwei Fällen unterschieden:

Liegt ein Angemessenheitsbeschluss für ein Land vor, so ist die Datenübermittlung zunächst ohne weiteres erlaubt, solange das sog. Verbot mit Erlaubnisvorbehalt berücksichtigt wird. So ist die Erhebung, Speicherung, Verarbeitung und Übermittlung von Daten an Drittländer oder internationale Organisationen nur dann erlaubt, wenn eine ausdrückliche Einwilligung

der betroffenen Personen bezüglich der Erhebung, Verarbeitung und Speicherung der Daten vorliegt oder eine gesetzliche Regelung dies erlaubt [10,12]. Die aktuelle Liste dieser Länder veröffentlicht die EU-Kommission im Amtsblatt der Europäischen Union und auf ihrer Website [13].

Existiert für das entsprechende Land kein Angemessenheitsbeschluss, sind zusätzliche Regelungen notwendig, um ein geeignetes Datenschutzniveau gewährleisten zu können. Die zu ergreifenden Maßnahmen werden dabei in Art. 46 genau definiert. Obwohl diese hier nicht im Detail besprochen werden sollen, sind dennoch einige Möglichkeiten aufgeführt, die der Gewährleistung eines geeigneten Datenschutzniveaus dienen. Eine Möglichkeit für das EU-Ausland bieten sog. Standardvertragsklauseln. Diese werden von der EU-Kommission freigegeben und vom Datenempfänger unterschrieben [10,14]. Des Weiteren können gemäß Art. 47 durch sog. Binding Corporate Rules Vereinbarungen über angemessene Datenschutzrichtlinien getroffen werden, die auf eine konzernweite Anpassung an die Standards der DSGVO abzielen. Ein solches Regelwerk wird von einer berechtigten Aufsichtsbehörde geprüft und ggf. genehmigt [10]. Zusätzlich können gemäß Art. 46 Abs. 2e/f durch Aufsichtsbehörden genehmigte Zertifizierung und Verhaltensregeln als rechtliche Grundlage verwendet werden [10,14].

4.5 Zertifizierungen

Laut Art. 28. Abs. 1 liegt es zunächst in der Pflicht des Verantwortlichen die Eignung des Auftragsverarbeiters zu beurteilen und eine rechtmäßige Verarbeitung personenbezogener Daten zu garantieren. Da dies in der Realität jedoch häufig schwierig und zeitintensiv ist und Verantwortliche ggf. nicht das entsprechende Fachwissen besitzen, sehen Art. 44 und 45 eine allgemeine Zertifizierung vor, die es Verantwortlichen ermöglichen soll, den Entscheidungsprozess zu beschleunigen. Wie für Zertifizierungen üblich, wird sie dabei von berechtigten, unabhängigen Aufsichtsbehörden ausgestellt und kann als Rechtsgrundlage herangezogen werden [9,10,14]. Das im November 2017 gestartete Projekt AUDITOR arbeitet bis heute (Oktober 2020) an solch einer Zertifizierung [15]. Obwohl also noch keine allgemeine Zertifizierung vorhanden ist, gibt es dennoch andere Zertifizierungen, die Auskunft über das Sicherheitsniveau einzelner Aspekte der DSGVO geben. Dies decken beispielsweise Teile der Zertifikate ISO/IEC 27018, ISO/IEC 27701 und das in Deutschland vorhandene C5 ab. Dabei sei angemerkt, dass diese Zertifikate in keinem Fall einer allgemein gültigen Zertifizierung nach den Standards der DSGVO gleichzusetzen sind. Häufig stellen die einzelnen CSPs eine Liste der von ihnen erworbenen Zertifikaten in ihren Compliance Centern öffentlich zur Verfügung.

4.6 Fallbeispiel Auftragsverarbeitung USA

Zum Abschluss dieses Abschnitts betrachten wir beispielhaft die Auftragsverarbeitung in den USA, da der Großteil der Cloud Provider amerikanischen Unternehmen angehört und aufgrund ihrer Kapazitäten häufiger als Provider in Erwägung gezogen werden. Von größter Relevanz ist dabei der Serverstandort. Befindet sich der Server außerhalb der EU bzw. des Europäischen Wirtschaftsraumes (bspw. innerhalb der USA) liegt eine Übermittlung an ein Drittland vor, weshalb für eine weitestgehend unproblematische Datenübertragung ein Angemessenheitsbeschluss für die Vereinigten Staaten notwendig ist. Dieser liegt aktuell jedoch nicht vor [13]. Bis zum 16. Juli 2020 existierte ein Angemessenheitsbeschluss basierend auf dem sog. EU-US Privacy Shield, einer Absprache zwischen der EU und den USA, die ein angemessenes Sicherheitsniveau bei der Speicherung und Verarbeitung personenbezogener Daten des transatlantischen Datenverkehrs gewährleisten sollte [16]. Vor dem Hintergrund der DSGVO erklärte der Europäische Gerichtshof den Angemessenheitsbeschluss am 16. Juli 2020 jedoch für ungültig und begründete seine

Entscheidung mit unzureichenden Datenschutzsicherheitsstandards innerhalb der USA, die den Anforderungen der DSGVO nicht gerecht werden [17]. Das bedeutet, dass die Einbeziehung US-amerikanischer Cloud Provider in den Verarbeitungsprozess personenbezogener Daten, unter Verwendung von Servern innerhalb der USA, Zusatzmaßnahmen erfordert.

Zu Gunsten der europäischen Cloud-Nutzer besitzen US-amerikanische Provider mittlerweile Niederlassungen in EU-Mitgliedsstaaten, um den durch die Auflösung des EU-US Privacy Shields resultierenden Folgen entgegenzuwirken.

Der Firmensitz von Amazon befindet sich beispielsweise in Luxemburg, wodurch es als Unternehmen unmittelbar den Richtlinien der DSGVO unterliegt. Zusätzlich stehen in den europäischen Mitgliedsstaaten oft lokale Rechenzentren zur Verfügung, durch die eine Datenübermittlung an Drittländer optional wird und Daten so auch innerhalb desselben Landes gespeichert werden können. Befinden sich Serverstandort und Sitz des Nutzers in verschiedenen EU-Ländern, können zur Gewährleistung eines angemessenen Datenschutzniveaus entsprechend Standardvertragsklauseln verwendet werden [10].

Die Zuständigkeit der Aufsichtsbehörden nach Art. 55-59 ist ebenfalls ein interessanter Gesichtspunkt, den wir an dieser Stelle kurz aufgreifen. Von besonderer Relevanz sind die Regelungen der grenzüberschreitenden Datenverarbeitung [9], bei der ein Unternehmen mit Firmensitz in einem EU-Mitgliedsstaat Dienste in anderen Mitgliedsstaaten anbietet. Zunächst wird jeder Aufsichtsbehörde gemäß Art. 55 die Zuständigkeit für die Erfüllung der in Artikel 57 und 58 genannten Aufgaben und Befugnisse innerhalb ihres eigenen Mitgliedsstaates auferlegt. Im Kontext der grenzüberschreitenden Datenverarbeitung unterscheidet die DSGVO jedoch weiter zwischen der betroffenen und der federführenden Aufsichtsbehörde. Letztere ist dabei gemäß Art. 56 Abs. 1 für die grenzüberschreitende Verarbeitung aller Unternehmen zuständig, deren Sitz sich im Land der entsprechenden Aufsichtsbehörde befindet. Findet eine betroffene Aufsichtsbehörde nun bei der grenzüberschreitenden Verarbeitung einen möglichen Verstoß gegen datenschutzrechtliche Vorschriften, informiert diese die federführende Aufsichtsbehörde über den Verstoß. Diese ist gemäß Art. 55 Abs. 2 dazu verpflichtet sich mit dieser Beschwerde auseinanderzusetzen und zu entscheiden, ob sie sich mit dem Fall befasst. Je nach Beschluss hat die betroffene Aufsichtsbehörde die Möglichkeit des Einspruchs. Dieser Sachverhalt gibt einen Einblick über die Einbindung und Zusammenarbeit der verschiedenen Aufsichtsbehörden durch die DSGVO zur Schaffung eines möglichst hohes Kontrollniveaus. Die genaue Zusammenarbeit der Behörden ist dabei in den Artikeln 60-67 geregelt. Ein konkretes Negativbeispiel ist jedoch die Datenschutz-Situation hinsichtlich Facebook, welches seinen Firmensitz in Irland hat. Seit des Inkrafttretens der DSGVO im Mai 2018 hat die zuständige federführende Aufsichtsbehörde von insgesamt elf Verfahren gegen Facebook bis zum Februar 2020 keines abgeschlossen [18].

Ein weiterer relevanter Gesichtspunkt der US-amerikanischen Gesetzeslage im Bereich der Datensicherheit ist die Existenz der sog. Cloud Acts und Freedom Acts. Letzterer regelt den Zugriff amerikanischer Behörden auf die von inländischen Organisationen gespeicherten Daten. Die Behörden selbst dürfen dabei keine Daten speichern [19]. Ihre Motivation zieht diese Gesetzgebung aus Anti-Terror-Maßnahmen, die dem Schutz der US-amerikanischen Bürger zugutekommen sollen. Die Kombination mit dem Cloud Act ermöglicht zusätzlich den Zugriff auf Daten, die nicht innerhalb der Vereinigten Staaten liegen [20]. Dabei sei angemerkt, dass die gesetzliche Lage eine eigene Komplexität besitzt, deren Ausarbeitung den Rahmen dieses Dokuments sprengen würde und deshalb auch nicht weiter vertieft wird.

Es wird dennoch empfohlen, sich bei gegebenem Anlass mit der genauen Gesetzgebung auseinanderzusetzen, da die entsprechenden Regelungen ggf. nicht mit den Richtlinien der DSGVO vereinbar sind.

5 FAZIT

Basierend auf den vorhergegangen Abschnitten lässt sich abschließend ein Fazit für die Eignung von Hybrid Clouds zur DSGVO-konformen Speicherung personenbezogener Daten ziehen. Die Kombination aus Public und Private Cloud ermöglicht eine gute Trennung der Daten, wobei sensible Informationen innerhalb der Private Cloud und unkritische Daten in der Public-Cloud-Komponente verarbeitet werden können.

Um den Richtlinien der DSGVO gerecht zu werden, empfehlen wir deutschen Unternehmen hinsichtlich der Private Cloud entweder einen vollständig autonomen Ansatz in Form einer Internal Private Cloud oder eine Hosted-Variante, unter Hinzuziehung eines europäischen, wenn nicht sogar deutschen Providers, zu verwenden. Auf diese Weise kann einer möglichen Haftung durch Nichteinhaltung datenschutzrechtlicher Vorschriften vorgebeugt werden. Die Auftragsverarbeitung durch Managed bzw. Hosted Private Cloud Provider außerhalb der EU, mit Serverstandort in Deutschland, ist prinzipiell nicht ausgeschlossen, bedarf aber besonderer Vorsicht, da sich die Gesetzeslage in den jeweiligen Ländern ggf. deutlich von der der EU unterscheidet. Internationale Unternehmen befinden sich so in einer Sandwich-Position zwischen inländischer und ausländischer Gesetzgebung, die möglicherweise EU-datenschutzrechtliche Risiken mit sich bringt.

Einschränkungen bezüglich der Nutzung von Public Cloud Providern haben sich keine ergeben, solange gewährleistet werden kann, dass keinerlei personenbezogene Daten in der Public-Cloud-Komponente verarbeitet werden. Auf diese Weise können also alle Vorteile der großen Public Cloud Provider ausgeschöpft werden, wodurch die Hybrid Cloud enorm an Flexibilität gewinnt und so u.a. Kosten gespart werden können.

Allgemein sind Hybrid Clouds bei sorgfältig überlegter Anwendung also eine geeignete Möglichkeit zur Verarbeitung personenbezogener Daten unter Berücksichtigung der DSGVO. Allerdings sorgen die europäischen Datenschutzrichtlinien auch dafür, dass ein deutlicher Mehraufwand nötig ist, um ein entsprechend gültiges Auftragsverarbeitungsverhältnis herzustellen. Da die größten Cloud-Provider häufig nicht vollkommen für eine DSGVO-konforme Auftragsverarbeitung geeignet sind, verbleiben weitere Maßnahmen, wie technische und physische Sicherheit möglicherweise in die Hände der Unternehmen. In diesem Sinne ließe sich dies als Wechselwirkung zwischen Sicherheit und Aufwand bzw. Kosten interpretieren.

LITERATUR

[1] Christian Baun and Marcel Kunze.
Cloud computing Web-basierte dynamische IT-services. Springer, 2019.

[2] Bundesamt fur Sicherheit in der Informationstechnik (BSI).
Cloud Computing Grundlagen.
https://www.bsi.bund.de/
letzter Zugriff: 20.10.2020, 9:24.

[3] Yanpei Chen, Vern Paxson, and Randy H Katz.
What's new about cloud computing security. University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010):2010-5, 2010.

[4] Peter Mell and Timothy Grance.
The nist definition of cloud computing. NIST special publication, 800:1-3, 2011.

[5] 1&1 IONOS SE.
PaaS: Platform as a Service im Überblick.
https://www.ionos.de/
letzter Zugriff: 21.10.2020, 10:00.

[6] Microsoft Corporation.
Azure Storage-Redundanz.
https://docs.microsoft.com/
letzter Zugriff: 21.10.2020, 11:24.

[7] 1&1 IONOS SE.
Die Public Cloud: Mehr Rechenpower für alle!
https://www.ionos.de/
letzter Zugriff: 21.10.2020, 12:12.

[8] Klaus Foitzick (Global Access Internet Services GmbH).
Private Cloud - Vorteile und Einsatz.
https://www.global.de/
letzter Zugriff: 23.10.2020, 10:15.

[9] *Datenschutz-Grundverordnung.*
https://dsgvo-gesetz.de/
letzter Zugriff: 28.9.2020, 10:27.

[10] RA Dr. Hans M. Wulf. White Paper:
Überblick zur neuen EU-Datenschutz-Grundverordnung.
https://www.ionos.de/
SKW Schwarz Rechtsanwälte & 1&1 IONOS cloud SE
letzter Zugriff: 29.9.2020, 10:44.

[11] Jens Eckard.
GDPR Playbook - Praxistipps zur Umsetzung der DS-GVO.
https://www.eco.de/, Seite 130
letzter Zugriff: 29.9.2020 11:19.

[12] Patricia Rogosch.
2: Grundlagen der Einwilligung, pages 22-35. Die Einwilligung im Datenschutzrecht.
Nomos Verlagsgesellschaft mbH & Co. KG
Baden-Baden, 1 edition, Dec 2013.

[13] Website der EU-Kommission.
Liste der Angemessenheitsbeschlüsse.
https://ec.europa.eu/
letzter Zugriff: 9.10.2020, 15:25.

[14] RAin Doris Brandl und RA Markus Säugling.
White Paper: Die neue EU-Datenschutz-Grundverordnung - Aus BDSG wird DSGVO.
https://www.tuvsud.com/
letzter Zugriff: 29.9.2020, 10:35.

[15] Kompetenznetzwerk Trusted Cloud e. V.
Europäische Datenschutz-Grundverordnung.
https://www.trusted-cloud.de/
letzter Zugriff: 12.10.2020, 8:38.

[16] Website der EU-Kommission.
Europäische Kommission stellt EU-US-Datenschutzschild vor: verbindliche Garantien zur Wiederherstellung des Vertrauens in den transatlantischen Datenverkehr.
https://ec.europa.eu/
letzter Zugriff: 12.10.2020, 10:00.

[17] Krempl, Stefan (Heise Online).
EuGH kippt EU-US-Datenschutzvereinbarung Privacy Shield.
https://www.heise.de/
letzter Zugriff: 12.10.2020, 10:05.

[18] Benjamin Stiebel (Behörden Spiegel).
Irische Datenschutzbehorde in der Kritik.
https://www. behoerden-spiegel.de/
letzter Zugriff: 28.10.2020, 11:03.

[19] Alex Byers (Politico).
USA Freedom Act vs. USA PATRIOT Act.
https://www.politico.com/
letzter Zugriff: 12.10.2020, 10:53.

[20] Mewes, Bernd (Heise Online).
CLOUD Act - US-Gesetz für internationalen Datenzugriff und -schutz verabschiedet.
https://www.heise.de/
letzter Zugriff: 12.10.2020, 10:55.

Dieses Whitepaper stellt die Zusammenhänge da und bietet einen Überblick über rechtliche Zusammenhänge. Sie soll und kann keine Rechtsberatung im Einzelfall ersetzen. Nur Fachleute mit speziellen Kenntnissen, können Ihnen abschließende Informationen und Beurteilungen geben. Wir haben die Inhalte mit größtmöglicher Sorgfalt zusammengestellt, zielgerichtet auf den Zweck dieses Dokuments. Eine Haftung für die Richtigkeit, die Vollständigkeit und ggf. die Aktualität der Informationen müssen wir ausschließen.