Verwendung von AWS im Rahmen der allgemeinen Überlegungen zu Datenschutz und Datensicherung

Januar 2016

(Unter https://aws.amazon.com/compliance/aws-whitepapers/

finden Sie die neueste Version dieses Dokuments.)

Übersicht

Dieses Dokument bietet Informationen für Kunden, die AWS-Produkte dazu nutzen wollen, Inhalte mit persönlichen Daten zu speichern oder zu verarbeiten, wobei die allgemeinen Überlegungen zu Datenschutz und Datensicherung eingehalten werden sollten.

Das Dokument enthält Informationen zu folgenden Themen:

- Funktionsweise von AWS und wie Kunden die Sicherheit handhaben und ihre Inhalte verschlüsseln können
- Die geografischen Standorte, an denen Kunden ihre Inhalte speichern können, sowie andere relevante Überlegungen
- Die jeweiligen Rollen von Kunden und AWS hinsichtlich der Verwaltung und Sicherung der auf AWS-Produkten gespeicherten Inhalte

Whitepapers mit näheren Informationen zu Überlegungen bezüglich Datenschutz und Datensicherung in mehreren Ländern der Region „Asien-Pazifik“ sowie in der Europäischen Union finden Sie unter **http://aws.amazon.com/compliance/**.

Umfang

Dieses Whitepaper beschäftigt sich mit den typischen Fragen von AWS-Kunden, die Überlegungen zu Datenschutz und Datensicherung für die Nutzung von AWS zur Speicherung und Verarbeitung von Inhalten mit persönlichen Daten anstellen. Es werden auch andere, relevante Überlegungen berücksichtigt, beispielsweise, wenn ein Kunde branchenspezifische Anforderungen einhalten muss, die Gesetze der Rechtsordnungen, in denen ein Kunde Geschäfte tätigt, oder vertragliche Verpflichtungen, die ein Kunde Dritten gegenüber hat.

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt keine Rechtsberatung dar und sollte auch nicht als solche verwendet werden. Da die Anforderungen jedes Kunden unterschiedlich sind, empfiehlt AWS seinen Kunden dringend, entsprechende Beratung zur Implementierung ihrer Datenschutz- und Datensicherungsanforderungen sowie bezüglich der geltenden Gesetze und anderer für ihr Unternehmen relevanten Anforderungen einzuholen.

Wenn wir uns in diesem Dokument auf „Inhalte“ beziehen, sind damit Software (einschließlich Abbilder virtueller Maschinen), Daten, Texte, Audio, Videos, Bilder und andere Inhalte gemeint, die ein Kunde oder ein anderer Endbenutzer mit AWS speichert oder verarbeitet. Zu den Inhalten eines Kunden zählen beispielsweise Objekte, die der Kunde mit Amazon Simple Storage Service speichert, Dateien, die auf einem Amazon Elastic Block Store-Volume gespeichert sind, oder die Inhalte einer Amazon DynamoDB-Datenbanktabelle. Solche Inhalte können, aber müssen nicht notwendigerweise, persönliche Daten des Kunden, seiner Endbenutzer oder von Dritten enthalten. Die Bestimmungen der AWS-Kundenvereinbarung oder einer anderen

relevanten Vereinbarung mit uns zur Verwendung von AWS gelten auch für die Inhalte des Kunden. Zu den Inhalten des Kunden zählen keine Daten, die der Kunde uns im Zusammenhang mit der Erstellung oder Verwaltung seiner AWS-Konten zur Verfügung stellt, wie zum Beispiel der Kundenname, Telefonnummern, E-Mail-Adressen und Fakturierungsdaten – diese gelten als Kontoinformationen und unterliegen der AWS-Datenschutzrichtlinie.

Inhalte des Kunden: Überlegungen zu Datenschutz und Datensicherung

Die Speicherung von Inhalten wirft für alle Unternehmen eine Reihe allgemeiner praktischer Fragen auf, wie zum Beispiel:

- Sind die Inhalte sicher?
- Wo werden die Inhalte gespeichert?
- Wer hat Zugriff auf die Inhalte?
- Welche Gesetze und Vorschriften gelten für die Inhalte und was ist erforderlich, um diese einzuhalten?

Diese Überlegungen sind nicht neu und nicht Cloud-spezifisch. Sie sind für intern gehostete und betriebene Systeme sowie für herkömmliche, von Dritten gehostete Dienste relevant. Mit diesen Fragen kann auch die Speicherung von Inhalten auf Anlagen oder in Räumlichkeiten Dritter oder die Verwaltung, das Aufrufen und die Nutzung der Inhalte durch externe Mitarbeiter verbunden sein. Bei der Nutzung von AWS bleibt jeder AWS-Kunde Eigentümer seiner Inhalte und behält die Kontrolle darüber. Diese Kontrolle umfasst Folgendes:

- Welche Inhalte mit AWS gespeichert oder verarbeitet werden
- Welche AWS-Dienste Kunden für ihre Inhalte nutzen
- Die AWS-Region (oder Regionen), in der die Inhalte gespeichert werden
- Das Format, die Struktur und die Sicherheit der Kundeninhalte, einschließlich der Entscheidung bezüglich des Verbergens, Anonymisierens oder der Verschlüsselung
- Wer Zugriff auf die AWS-Konten und Inhalte hat und wie diese Berechtigungen gewährt, verwaltet und widerrufen werden

Da AWS-Kunden innerhalb der AWS-Umgebung Eigentümer ihrer Inhalte bleiben und die Kontrolle darüber behalten, obliegt ihnen gemäß dem Modell geteilter Verantwortung von AWS auch die Verantwortung bezüglich der Sicherheit dieser Inhalte. Das Modell geteilter Verantwortung ist grundlegend für das Verständnis der jeweiligen Rollen von Kunden und AWS hinsichtlich der Datenschutz- und Datensicherungsanforderungen für die Inhalte, die Kunden mit AWS speichern oder verarbeiten.

AWS-Ansatz der geteilten Verantwortung in der Verwaltung der Cloud-Sicherheit

Sind die Inhalte des Kunden sicher?

Das Auslagern der IT-Infrastruktur in AWS führt zu einem Modell geteilter Verantwortung zwischen dem Kunden und AWS, da sowohl der Kunde als auch AWS wichtige Rollen beim Betrieb und bei der Verwaltung von Sicherheitsvorkehrungen einnehmen. Alle Komponenten, von Hostbetriebssystem und Virtualisierungsebene bis hin zur physischen Sicherheit der Anlagen, in denen AWS ausgeführt wird, werden von AWS betrieben, verwaltet und gesteuert. Der Kunde ist verantwortlich für die Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheits-Patches), für weitere damit verbundene Anwendungssoftware sowie für die Konfiguration der von AWS bereitgestellten Firewall für die Sicherheitsgruppe und anderer sicherheitsrelevanter Funktionen. Der Kunde stellt im Allgemeinen über von Dritten erworbene Dienste (z. B. Internetdienstanbieter) eine Verbindung zur AWS-Umgebung her. AWS stellt diese Verbindung nicht bereit, daher unterliegt sie dem Verantwortungsbereich des Kunden. Kunden sollten die Sicherheit dieser Verbindung und die Zuständigkeit des Drittanbieters für die Sicherheit in Bezug auf ihre Systeme abwägen. Die jeweiligen Rollen von Kunden und AWS im Modell geteilter Verantwortung sind in Abbildung 1 dargestellt:

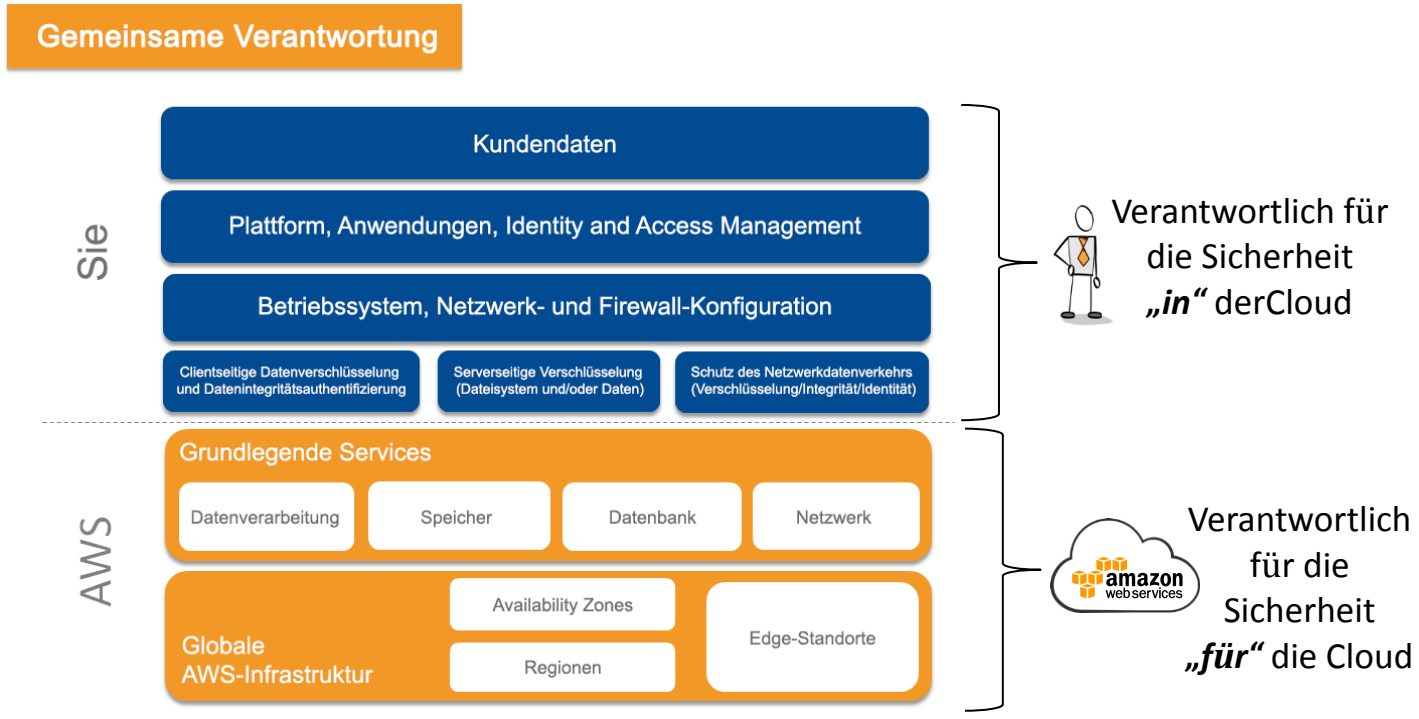

Abbildung 1 – Modell geteilter Verantwortung

Was bedeutet das Modell der geteilten Verantwortung für die Sicherheit der Inhalte des Kunden?

Der Kunde muss bei der Bewertung der Sicherheit einer Cloud-Lösung Folgendes verstehen und unterscheiden:

- Sicherheitsmaßnahmen, die der Cloud-Dienstanbieter (AWS) implementiert und betreibt – „Sicherheit ***für*** die Cloud"
- Sicherheitsmaßnahmen, die der Kunde implementiert und betreibt, und die sich auf die Sicherheit der Kundeninhalte und -anwendungen beziehen, die die AWS-Dienste nutzen – „Sicherheit ***in*** der Cloud".

Während AWS ***für*** die Sicherheit der Cloud selbst sorgt, liegt die Verantwortung für die Sicherheit ***in*** der Cloud beim Kunden. Kunden sorgen daher selbst für ausreichende Sicherheitsmaßnahmen zum Schutz ihrer eigenen Inhalte, Plattform, Anwendungen, Systeme und Netzwerke, wie dies auch in einem Rechenzentrum vor Ort der Fall wäre.

Erläuterungen zur Sicherheit *FÜR* die Cloud

AWS ist für die Verwaltung der Sicherheit der zugrunde liegenden Cloud-Umgebung verantwortlich. Die AWS-Cloud-Infrastruktur ist eine der flexibelsten und sichersten Cloud Computing-Umgebungen. Sie bietet eine optimale Verfügbarkeit bei vollständiger Kundentrennung. Außerdem stellt sie eine hochgradig skalierbare, zuverlässige Plattform zur Verfügung, in der Kunden Anwendungen und Inhalte rasch und sicher bereitstellen können – falls erforderlich, in großem Umfang und weltweit.

AWS ist inhaltsunabhängig, d. h. dasselbe hohe Sicherheitsniveau wird allen Kunden geboten, unabhängig von der Art der gespeicherten Inhalte oder der geografischen Region, in der sie ihre Inhalte speichern. Die erstklassigen, hochsicheren Rechenzentren von AWS wenden modernste elektronische Überwachung und Multi-Faktor-Zugriffskontrollsysteme an. Die Rechenzentren sind rund um die Uhr mit erfahrenen Support-Technikern besetzt und der Zugang wird streng auf Basis der geringsten Berechtigung erteilt. Eine ausführliche Liste aller Sicherheitsmaßnahmen, die in unserer grundlegenden AWS-Cloud-Infrastruktur, den Plattformen und Diensten integriert sind, finden Sie im Whitepaper Übersicht über die Sicherheitsmaßnahmen[1].

[1] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Wir sind um den Datenschutz unserer Kunden sehr bemüht und haben leistungsstarke technische und physische Maßnahmen gegen nicht autorisierten Zugriff implementiert. Kunden können die in der AWS-Umgebung vorhandenen Sicherheitskontrollen anhand von AWS-Zertifizierungen und -Berichten überprüfen, einschließlich der Berichte zur AWS Service Organization Control (SOC) 1, 2[2] und 3[3], der ISO 27001[4]-, 27017[5]- und 27018[6]-Zertifizierungen und der PCI-DSS[7]-Compliance-Berichte. Unsere 27018-Zertifizierung zeigt, dass AWS über ein System von Steuerungsmechanismen verfügt, die speziell auf den Datenschutz der Inhalte des Kunden ausgerichtet sind. Diese Berichte und Zertifizierungen werden von unabhängigen Auditoren erstellt und bezeugen die Effektivität des Konzepts und Betriebs der AWS-Sicherheitskontrollumgebungen. Die AWS-Compliance-Zertifizierungen und -Berichte können unter https://aws.amazon.com/compliance/contact angefordert werden. Weitere Informationen zu AWS-Compliance-Zertifizierungen, -Berichten und der Anpassung an bewährte Verfahren und Standards finden Sie auf der Compliance-Website von AWS.

Erläuterungen zur Sicherheit *IN* der Cloud

Kunden bleiben bei der Nutzung von AWS Eigentümer ihrer Inhalte und behalten die Kontrolle darüber. Nicht AWS, sondern die Kunden bestimmen, welche Inhalte sie auf AWS speichern oder verarbeiten. Da der Kunde entscheidet, welche Inhalte in die AWS Cloud hochgeladen werden, kann auch nur der Kunde bestimmen, welche Sicherheitsebene für die auf AWS gespeicherten und verarbeiteten Inhalte angemessen ist. Kunden haben ebenfalls die volle Kontrolle darüber, welche Dienste sie nutzen, wem sie Zugriff auf ihre Inhalte und Dienste gewähren und welche Anmeldeinformationen erforderlich sind. Kunden haben die Kontrolle über die Konfiguration ihrer Umgebungen, über die Sicherung und die Verschlüsselung ihrer Inhalte (im Ruhezustand und bei der Übertragung) sowie darüber, welche anderen Sicherheitsfunktionen und -tools sie einsetzen möchten und wie dies geschehen soll. AWS ändert keine Konfigurationseinstellungen des Kunden, da diese Einstellungen vom Kunden festgelegt und gesteuert werden. AWS-Kunden haben bei der Konzipierung einer Sicherheitsarchitektur, die ihren Compliance-Anforderungen entspricht, vollständige Freiheit. Dies ist ein Hauptunterschied zu herkömmlichen Hosting-Lösungen, in denen der Anbieter die Entscheidungen über die Architektur trifft. AWS gibt dem Kunden die Möglichkeit, selbst zu entscheiden, wann und wie Sicherheitsmaßnahmen in der Cloud implementiert werden. So wird gewährleistet, dass diese den Unternehmensanforderungen des einzelnen Kunden entsprechen. Wenn beispielsweise eine Architektur mit höherer Verfügbarkeit zum Schutz der Inhalte des Kunden erforderlich ist, kann der Kunde redundante Systeme, Sicherungen, Standorte, Netzwerk-Uplinks usw. hinzufügen, um eine stabilere, hoch verfügbare Architektur zu erstellen. Wenn der

[2] http://aws.amazon.com/compliance/soc-faqs/
[3] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf
[4] http://aws.amazon.com/compliance/iso-27001-faqs/
[5] http://aws.amazon.com/compliance/iso-27017-faqs/
[6] http://aws.amazon.com/compliance/iso-27018-faqs/
[7] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

Zugang auf die Inhalte des Kunden eingeschränkt werden soll, ermöglicht AWS dem Kunden die Implementierung von Kontrollen der Zugriffsberechtigungen – sowohl auf Systemebene als auch über die Verschlüsselung auf Datenebene.

AWS bietet eine große Auswahl an Sicherheitstools und -funktionen, die Kunden zur Einrichtung, Implementierung und zum Betrieb ihrer eigenen sicheren AWS-Umgebung einsetzen können. Kunden können ebenfalls ihre eigenen Sicherheitstools und -kontrollen verwenden, einschließlich einer großen Anzahl von Drittanbieter-Sicherheitslösungen. AWS lässt sich nach Wunsch konfigurieren, damit Kunden diese unterschiedlichen Sicherheitsfunktionen, Tools und Kontrollen nutzen können, um ihre Inhalte zu schützen. Dazu gehören leistungsstarke Tools zur Identitäts- und Zugriffsverwaltung, Sicherheitslösungen, die Verschlüsselung und Netzwerksicherheit. Folgende Maßnahmen können Kunden beispielsweise zum Schutz ihrer Inhalte implementieren:

- Richtlinien für sichere Passwörter, individuelle Gewährung angemessener Zugriffsrechte und zuverlässiger Schutz von Zugriffsschlüsseln
- Angemessene Firewalls und Netzwerksegmentierung, Verschlüsselung von Inhalten und durchdachte Systemarchitektur, um Datenverlust und nicht autorisierten Zugriff zu verhindern

Da Kunden und nicht AWS die Kontrolle über diese wichtigen Faktoren haben, obliegt den Kunden auch die Verantwortung für ihre Entscheidungen und für die Sicherheit der Inhalte, die sie auf AWS hochladen. Dies betrifft auch die Verbindung mit ihrer AWS-Infrastruktur, wie das Gastbetriebssystem, Anwendungen auf ihren Datenverarbeitungs-Instances und die Inhalte, die in AWS-Speichern, Plattformen, Datenbanken und anderen Diensten gespeichert und verarbeitet werden.

AWS bietet erweiterte Funktionen für den Zugriff, die Verschlüsselung und die Anmeldung, damit Kunden ihre Inhalte effektiv verwalten können. Dazu gehören beispielsweise das AWS Key Management Service und AWS CloudTrail. Damit Kunden die AWS-Sicherheitskontrollen in ihre vorhandenen Kontrollrahmen integrieren und Sicherheitsbewertungen zum Einsatz von AWS in ihren Unternehmen erstellen und durchführen können, veröffentlicht AWS verschiedene Whitepapers zu den Themen Datensicherheit, Organisation, Risiken und Compliance sowie mehrere Checklisten und bewährte Methoden. Natürlich können Kunden auch ihre eigenen Sicherheitsbewertungen erstellen und ausführen und Erlaubnis zur Durchführung eigener Scans in ihrer Cloud-Infrastruktur beantragen, solange sich diese Scans auf die Datenverarbeitungs-Instances der Kunden beschränken und nicht gegen die AWS Acceptable Use Policy verstoßen.

AWS-Regionen: Wo werden die Inhalte gespeichert?

AWS-Rechenzentren wurden in Clustern in verschiedenen Regionen weltweit errichtet. Wir bezeichnen ein Cluster von Datenzentren in einem bestimmten Land als „Region". Kunden haben weltweit Zugang zu 12 AWS-Regionen[8]. Kunden können eine Region, alle Regionen oder eine Kombination aus beliebigen Regionen auswählen. In der Abbildung 2 sind die AWS-Regionen dargestellt:

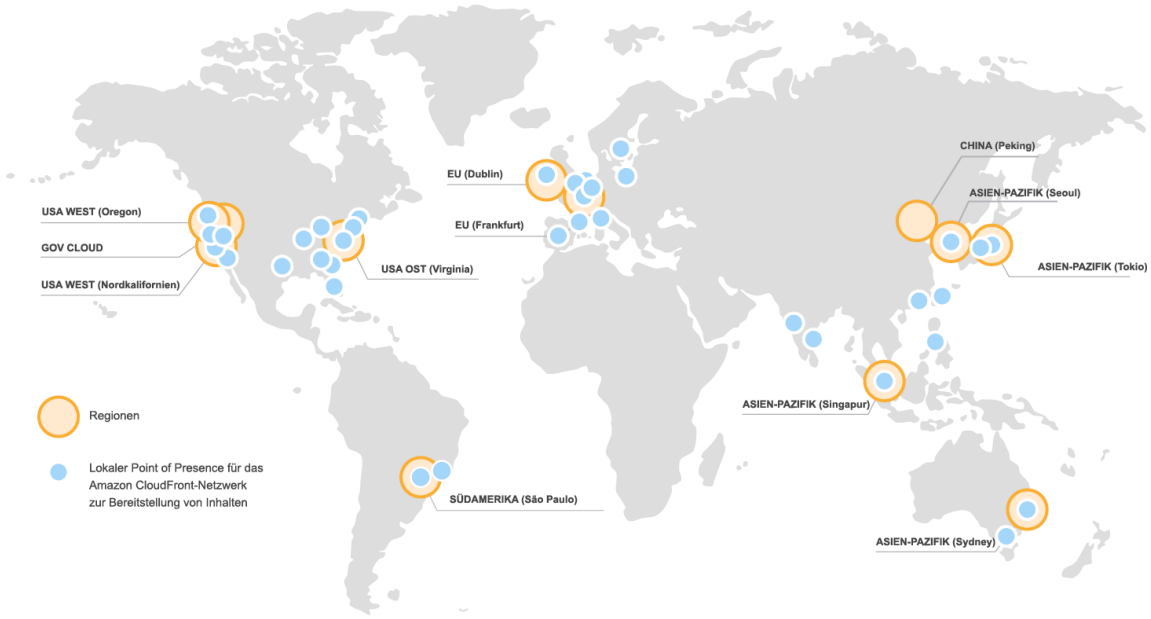

Abbildung 2 – Globale AWS-Regionen

AWS-Kunden geben an, in welcher AWS-Region oder in welchen Regionen sich ihre Inhalte und Server physisch befinden sollen. Damit können Kunden, die bestimmte geografische Anforderungen erfüllen müssen, Umgebungen an einem oder mehreren Standorten ihrer Wahl erstellen. Beispielsweise verfügt AWS derzeit keine Region in Indien. AWS-Kunden in Indien können jedoch auswählen, ihre AWS-Dienste exklusiv in der Region „Asien, Pazifik (Singapur)" bereitzustellen und ihre Inhalte auswärts in Singapur zu speichern, wenn dies ihr bevorzugter Standort ist. Wenn die Kunden diese Wahl getroffen haben, befinden sich ihre Inhalte in Singapur, sofern der Kunde die Inhalte nicht verschiebt.

[8] AWS GovCloud (USA) ist eine isolierte AWS-Region, die entwickelt wurde, damit US-Regierungsbehörden und Kunden vertrauliche Arbeitslasten in die Cloud verschieben können und dabei bestimmte behördliche Vorgaben und Compliance-Anforderungen erfüllen. Die AWS-Region „China (Peking)" ist ebenfalls eine isolierte AWS-Region. Kunden, die die AWS-Region „China (Peking)" nutzen möchten, müssen sich registrieren, um separate Konto-Anmeldeinformationen zu erhalten, die für die Region „China (**Peking**)" einzigartig sind.

Kunden haben immer die Kontrolle darüber, in welcher Region bzw. in welchen Regionen ihre Inhalte gespeichert und verarbeitet werden. AWS speichert und verarbeitet die Inhalte seiner Kunden nur in den vom Kunden gewählten Regionen und verwendet nur die vom Kunden gewählten Dienste. Die Inhalte des Kunden werden nicht verschoben, außer dies ist gesetzlich erforderlich.

Wie wählen Kunden ihre Region(en) aus?

Der Kunde legt bestimmte AWS-Regionen, in denen die AWS-Dienste verwendet werden sollen, über die AWS Management Console oder durch eine Anforderung über eine AWS-Anwendungsprogrammierschnittstelle (API) fest.

Abbildung 3: Auswählen globaler AWS-Regionen. Hier wird das Auswahlmenü für AWS-Regionen dargestellt, das Kunden beim Hochladen von Inhalten auf ein AWS-Speicherservice oder bei der Bereitstellung von Datenverarbeitungsressourcen über die AWS Management Console sehen.

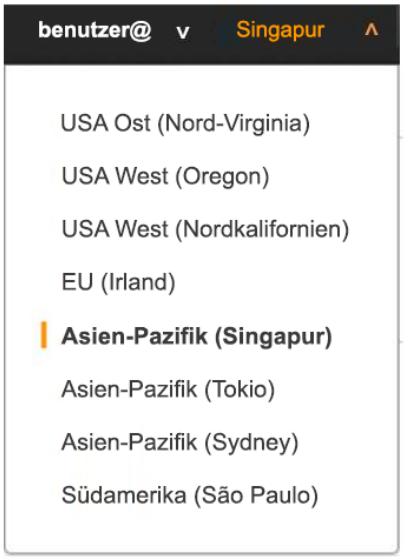

Abbildung 3 – Auswählen globaler AWS-Regionen in der AWS Management Console

Kunden können ebenfalls die AWS-Region vorgeben, die für ihre Datenverarbeitungsressourcen verwendet werden soll, indem sie die Funktionen der Amazon Virtual Private Cloud (VPC) nutzen. Mit der Amazon VPC können Kunden einen privaten, isolierten Abschnitt der AWS Cloud bereitstellen, in dem sie AWS-Ressourcen in einem selbst definierten virtuellen Netzwerk starten können. Außerdem können Kunden mit der Amazon VPC eine virtuelle Netzwerktopologie definieren, die einem herkömmlichen Netzwerk sehr ähnlich ist, das sie in ihrem eigenen Rechenzentrum betreiben könnten.

Alle Datenverarbeitungsressourcen und andere Ressourcen, die der Kunde in der VPC startet, befinden sich in der vom Kunden festgelegten AWS-Region. Wenn beispielsweise eine VPC in der Region „Asien, Pazifik (Sydney)“ erstellt und ein Link (entweder über VPN[9] oder Direct Connect[10]) zurück zum Rechenzentrum des Kunden bereitgestellt wird, werden alle in der VPC gestarteten Datenverarbeitungsressourcen ausschließlich in der Region „Asien, Pazifik (Sydney)“ gespeichert. Diese Option kann ebenfalls für andere AWS-Regionen bereitgestellt werden.

Grenzüberschreitende Übertragung von persönlichen Daten

Bei der Verwendung von AWS kann es vorkommen, dass Kunden Inhalte mit persönlichen Daten grenzüberschreitend übertragen möchten. Dazu müssen sie die gesetzlichen Bestimmungen für solche Übertragungen beachten. AWS stellt den Zusatz zur Datenverarbeitung zur Verfügung, der die 2010/87/EU-Standardvertragsklauseln (auch als „Modellklauseln“ bezeichnet) für AWS-Kunden enthält, die Inhalte mit persönlichen Daten (gemäß der EU-Richtlinie) von der EU an ein Land außerhalb des Europäischen Wirtschaftsraums übertragen, beispielsweise Singapur. AWS hat bereits die Genehmigung der EU-Datenschutzbehörde (Artikel 29 des Arbeitskreises) für den Zusatz zur AWS-Datenverarbeitung und die Musterklauseln erhalten. Dank unseres von der EU genehmigten Zusatzes zur Datenverarbeitung und der Musterklauseln können AWS-Kunden AWS weiterhin für ihre weltweiten Geschäfte verwenden und halten dabei alle EU-Gesetze ein – egal, ob sie ihren Sitz in Europa haben oder ein globales Unternehmen sind, das im Europäischen Wirtschaftsraum tätig ist. Weitere Informationen finden Sie in den häufig gestellten Fragen zum EU-Datenschutz von AWS. Weitere Informationen dazu, wie Kunden dem AWS-Zusatz zur Datenverarbeitung beitreten können, finden Sie hier (Anmeldung erforderlich).

Wer kann auf Kundeninhalte zugreifen?

Kundenkontrolle über Inhalte

Kunden behalten bei Nutzung der AWS-Dienste die effektive Kontrolle über ihre Inhalte innerhalb der AWS-Umgebung bei. Dies umfasst Folgendes:

- Festlegen, wo sich die Inhalte befinden, zum Beispiel, Festlegen der auf AWS verwendeten Speicherart und an welchem geografischen Standort (d. h. in welcher Region) die Speicherung erfolgen soll

[9] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
[10] http://aws.amazon.com/directconnect/

- Kontrolle über das Format, die Struktur und die Sicherheit der Kundeninhalte, einschließlich der Entscheidung bezüglich des Verbergens, Anonymisierens oder der Verschlüsselung AWS bietet Kunden die Möglichkeit zur Implementierung einer zuverlässigen Verschlüsselung für ihre Inhalte während der Übertragung und der Speicherung. Kunden können außerdem ihre eigenen Verschlüsselungsschlüssel verwalten oder Verschlüsselungsmechanismen von Drittanbietern ihrer Wahl verwenden
- Verwalten anderer Zugriffskontrollen, wie Identitätskontrolle, Zugriffsverwaltung, Berechtigungen und Sicherheitsanmeldedaten

Auf diese Weise können AWS-Kunden den gesamten Lebenszyklus ihrer Inhalte auf AWS steuern und die Inhalte ihren speziellen Bedürfnissen entsprechend verwalten, wozu unter anderem die Inhaltsklassifizierung, Zugriffskontrolle, Aufbewahrung und Löschung zählt.

AWS-Zugriff auf Kundeninhalte

AWS stellt allen Kunden Datenverarbeitungs-, Speicher-, Datenbank- und Netzwerkservices sowie andere, auf unserer Website beschriebene Dienste zur Verfügung. Kunden haben bei der Nutzung dieser Dienste verschiedene Möglichkeiten zur Verschlüsselung ihrer Inhalte, einschließlich der AWS-Verschlüsselungsfunktionen, der Verwaltung ihrer eigenen Verschlüsselungsschlüssel oder der Verwendung von Verschlüsselungsmechanismen von Drittanbietern ihrer Wahl. AWS greift nicht auf die Kundeninhalte zu oder verwendet sie – außer dies ist gesetzlich oder für die Bereitstellung der vom Kunden gewählten AWS-Dienste an den Kunden und dessen Endbenutzer erforderlich. AWS verwendet niemals Kundeninhalte für andere Zwecke, wie zum Beispiel Marketing oder Werbung, oder leitet Informationen für diese Zwecke daraus ab.

Zugriffsrechte der Regierung

Es erreichen uns häufig Fragen bezüglich der Zugriffsrechte inländischer oder ausländischer Regierungsbehörden auf die in Cloud-Services gespeicherten Inhalte. Unter den Kunden herrscht zum Thema der Datenhoheit oft Verwirrung und sie wissen nicht, ob bzw. unter welchen Umständen Regierungen auf ihre Inhalte zugreifen dürfen. Die geltenden Gesetze in der Jurisdiktion, in der sich die Inhalte befinden, spielen für manche Kunden eine wichtige Rolle. Kunden sollten sich jedoch informieren, ob nicht auch die Gesetze anderer Jurisdiktionen für sie gelten. Sie sollten einen Rechtsbeistand zurate ziehen, um sich einen Überblick über die Anwendbarkeit von relevanten Gesetzen auf ihr Unternehmen und ihre Geschäftstätigkeit zu verschaffen.

Bezüglich etwaiger Bedenken oder Fragen zu den Zugriffsrechten inländischer oder ausländischer Regierungen auf die in der Cloud gespeicherten Inhalte ist es wichtig zu verstehen, dass die entsprechenden Regierungsbehörden aufgrund von Gesetzen, die ohnehin für den Kunden gelten, berechtigt sein können, Anforderungen zur Offenlegung dieser Inhalte zu stellen. Ein Unternehmen, das beispielsweise in Land X Geschäfte tätigt, könnte eine gesetzliche Anfrage nach Informationen erhalten, auch wenn die Inhalte in Land Y gespeichert sind. Normalerweise fordert eine Regierungsbehörde Informationen direkt von der Entität und nicht vom Cloud-Anbieter an.

In den meisten Ländern gelten Gesetze, die es Strafverfolgungs- und Sicherheitsbehörden ermöglichen, Zugriff auf Informationen anzufordern. Die meisten Länder verfügen über Verfahren (einschließlich bilateraler Rechtshilfeverträge), die die Übertragung von Informationen in andere Länder aufgrund einer gesetzlichen Anfrage (z. B. im Zusammenhang mit Verbrechen) ermöglichen. Beachten Sie jedoch auch, dass jedes maßgebliche Gesetz Kriterien enthält, die von der entsprechenden Strafverfolgungsbehörde erfüllt werden müssen, damit die Anforderung Gültigkeit hat. Beispielsweise muss eine Regierungsbehörde, die Zugriff auf Informationen erhalten möchte, nachweisen, dass ein berechtigter Grund für die Gewährung des Zugriffs vorliegt, und sie muss möglicherweise einen Gerichtsbeschluss oder Durchsuchungsbefehl erwirken.

In vielen Ländern existieren Gesetze für den Zugriff auf Daten, die einen Anspruch auf exterritoriale Geltung haben. Ein Beispiel eines US-amerikanischen Gesetzes mit extraterritorialer Reichweite, das häufig im Zusammenhang mit Cloud-Services erwähnt wird, ist der U.S. Patriot Act. Der Patriot Act ähnelt den Gesetzen in anderen entwickelten Nationen, die es Regierungen ermöglichen, Informationen für Ermittlungen in Zusammenhang mit internationalem Terrorismus und zu anderen Fragen ausländischer Geheimdienste zu erhalten. Für jede Anforderung von Dokumenten unter dem Patriot Act ist ein Gerichtsbeschluss erforderlich, der nachweist, dass die Anforderung dem Gesetz entspricht. Dazu gehört beispielsweise auch, dass die Anforderung in Bezug zu legitimen Ermittlungen steht. Der Patriot Act gilt im Allgemeinen für alle Unternehmen mit Geschäftstätigkeit in den USA, unabhängig davon, wo sie eingebunden und/oder ob sie global tätig sind, sowie unabhängig davon, ob die Informationen in der Cloud, in einem Rechenzentrum vor Ort oder in physischen Datensätzen gespeichert sind. Das bedeutet, dass Unternehmen mit Hauptsitz oder Geschäftstätigkeit außerhalb der USA dem Patriot Act unterliegen können, wenn sie zudem in den USA geschäftlich tätig sind.

AWS-Richtlinie zur Zugriffserteilung an Regierungen

AWS behandelt die Sicherheit der Kunden mit größter Vorsicht und veröffentlicht oder verschiebt keine Daten auf Anfrage der US-amerikanischen oder anderer Regierungen, wenn dies nicht gesetzlich erforderlich ist und ein gesetzlicher oder rechtlich bindender Auftrag wie z. B. eine Vorladung oder ein Gerichtsbeschluss erfüllt werden muss oder dies aufgrund von geltendem Recht anderweitig erforderlich ist. Wenn uns dies nicht per Gesetz verboten ist oder es klare Anzeichen für ein illegales Verhalten in Verbindung mit der Nutzung von AWS gibt, benachrichtigen wir nach Möglichkeit die Kunden, bevor wir ihre Inhalte offenlegen, damit sie versuchen können, von dieser Offenlegung befreit zu werden.

Allgemeine Überlegungen zu Datenschutz und Datensicherung

Viele Länder haben Gesetze zum Schutz von persönlichen Daten. In einigen Ländern gibt es ein einziges umfassendes Datenschutzgesetz, während in anderen der Datenschutz durch eine Reihe von Gesetzen und Vorschriften differenzierter gehandhabt wird. Während die gesetzlichen und regulatorischen Anforderungen unterschiedlich sein können – aufgrund von rechtlichen, branchenspezifischen und inhaltsspezifischen Anforderungen – gibt es dennoch einige gemeinsame Überlegungen, die von mehreren führenden Gesetzen zum Datenschutz aufgegriffen wurden. Diese können auf den typischen Lebenszyklus von persönlichen Daten abgestimmt werden.

Um Kunden dabei zu unterstützen, ihre Datenschutz- und Datensicherungsanforderungen bei der Nutzung von AWS zum Speichern und Verarbeiten von Inhalten mit persönlichen Daten zu analysieren und zu berücksichtigen, stellen wir nachfolgend die unterschiedlichen Stufen dieses Datenlebenszyklus dar, nennen die wichtigsten Überlegungen für jede dieser Stufen und stellen relevante Informationen zur Funktionsweise von AWS zur Verfügung.

Viele Gesetze zum Datenschutz weisen Verantwortlichkeiten abhängig davon zu, wie ein Beteiligter mit den persönlichen Daten interagiert und über welche Zugriffsebene bzw. Kontrolle dieser Beteiligter über die persönlichen Daten verfügt. Ein häufig verwendeter Ansatz ist die Unterscheidung zwischen dem Datenverantwortlichen, dem Auftragsverarbeiter und dem Datensubjekt. Die in den verschiedenen Jurisdiktionen verwendete Terminologie kann unterschiedlich sein und manche Gesetze treffen feinere Unterscheidungen. AWS weiß es zu schätzen, dass seine Services in vielen verschiedenen Kontexten für unterschiedliche Geschäftszwecke verwendet werden, und dass am Datenlebenszyklus von persönlichen Daten, die mit den Kundeninhalten in AWS gespeichert und verarbeitet werden, mehrere Parteien beteiligt sein können. In der Anleitung, die in der nachfolgenden Tabelle enthalten ist, wird der Einfachheit angenommen, dass im Kontext der in AWS gespeicherten und verarbeiteten Kundeninhalte die Kunden wie folgt agieren:

- Sie erfassen persönliche Daten ihrer Endbenutzer oder anderer Personen (Datensubjekte) und bestimmen den Zweck, für den diese persönlichen Daten erfasst und benutzt werden.
- Sie haben die Möglichkeit zu steuern, wer auf die persönlichen Daten zugreifen, diese aktualisieren und verwenden kann.
- Sie verwalten die Beziehung mit der Einzelperson, der die persönlichen Daten zugeordnet sind (in diesem Abschnitt als „Datensubjekt“ bezeichnet). Dies beinhaltet die erforderliche Kommunikation mit dem Datensubjekt, um alle entsprechenden Offenlegungs- und Zustimmungsanforderungen zu erfüllen.

Die Kunden nehmen somit eine Rolle ein, die der des Datenverantwortlichen entspricht, da sie die Inhalte kontrollieren, Entscheidungen über die Behandlung dieser Inhalte treffen und festlegen, wer diese Inhalte in ihrem Namen verarbeiten darf. Im Vergleich dazu nimmt AWS eine Rolle ein, die dem Auftragsverarbeiter entspricht, da AWS die Inhalte der Kunden nur verwendet, um die vom Kunden gewählten AWS-Dienste für diesen Kunden bereitzustellen. Die Inhalte von Kunden werden für keine anderen Zwecke verwendet. Beachten Sie, dass die Begriffe „Datenverantwortlicher“ und „Auftragsverarbeiter“ EU-rechtlich eine sehr unterschiedliche Bedeutung haben und dieses Whitepaper nicht dazu dient, spezifische EU-Anforderungen zu erläutern. Ein Leitfaden zu den EU-Datenschutzanforderungen in Bezug auf „Datenverantwortliche“ und „Auftragsverarbeiter“ ist in unserem Whitepaper zum EU-Datenschutz zu finden[11].

Wenn ein Kunde persönliche Daten im Namen oder auf Anweisung Dritter (der ein Verantwortlicher für die persönlichen Daten sein kann oder ein Dritter, mit dem der Kunde eine Geschäftsbeziehung hat) mit AWS verarbeitet, werden die in der Tabelle genannten Kundenverantwortlichkeiten vom Kunden und diesem Dritten gemeinsam wahrgenommen und verwaltet.

[11] http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf

Stufe des Datenlebenszyklus	**Zusammenfassung und Beispiele**	**Überlegungen**
Erfassen persönlicher Daten	Es kann angemessen oder erforderlich sein, Personen (Datensubjekte) vor dem Erfassen ihrer persönlichen Daten darüber zu informieren oder ihre Zustimmung dazu einzuholen. Dazu kann auch die Benachrichtigung über den Zweck gehören, für den ihre Informationen erfasst, verwendet oder offengelegt werden. Es können Anforderungen gelten, von wem persönliche Daten erfasst werden, d. h. die Anforderungen können unterschiedlich sein, wenn persönliche Daten von einem Dritten statt direkt von der Einzelperson erfasst werden. Die Erfassung von persönlichen Daten kann nur dann zulässig sein, wenn sie aus einem berechtigten oder sinnvollem Zweck erfolgt.	**Kunde:** Die Kunden bestimmen und steuern, wann, wie und warum sie persönliche Daten von Personen erfassen, und entscheiden, ob diese persönlichen Daten in den mit AWS gespeicherten und verarbeiteten Kundeninhalten enthalten sein sollen. Die Kunden müssen eventuell den jeweiligen Datensubjekten den Zweck offenlegen, für den die Daten erfasst werden, sowie sicherstellen, dass die Daten nur von zulässigen Quellen erfasst und für einen zulässigen Zweck verwendet werden. Die Kunden haben nicht nur eine Beziehung mit AWS, sie haben auch eine Beziehung mit den Personen, deren persönliche Daten sie auf AWS speichern. Daher können Kunden direkt mit diesen Personen über die Erfassung und Behandlung ihrer persönlichen Daten kommunizieren. Nicht AWS, sondern die Kunden kennen das Ausmaß der Benachrichtigungen an diese Personen oder die von diesen Personen erhaltenen Zustimmungen in Bezug auf die Erfassung ihrer persönlichen Daten. **AWS:** AWS erfasst keine persönlichen Daten von Personen, deren persönliche Daten in den mit AWS gespeicherten und verarbeiteten Kundeninhalten enthalten sind, und AWS hat keinen persönlichen Kontakt zu diesen Personen. Daher ist AWS nicht verpflichtet, mit den jeweiligen Personen zu kommunizieren und erforderliche Zustimmungen einzuholen, bzw. kann dies unter den gegebenen Umständen auch gar nicht tun. AWS verwendet die Inhalte der Kunden nur, um die vom Kunden gewählten AWS-Dienste für diesen Kunden bereitzustellen. Die Inhalte von Kunden werden für keine anderen Zwecke verwendet.

Stufe des Datenlebenszyklus	Zusammenfassung und Beispiele	Überlegungen
Verwendung und Offenlegung persönlicher Daten	Es ist wahrscheinlich angemessen oder erforderlich, persönliche Daten nur für den Zweck zu verwenden oder offenzulegen, für den sie erfasst wurden. Die Person (Datensubjekt) sollte daher eventuell informiert werden, dass der Kunde AWS als Service-Anbieter verwendet.	**Kunde:** Der Kunde bestimmt und steuert, warum persönliche Daten erfasst werden, wofür die Daten verwendet werden, von wem die Daten verwendet werden können und an wen sie offengelegt werden. Der Kunde muss sicherstellen, dass die Datenerfassung nur für zulässige Zwecke erfolgt. Wenn der Kunde persönliche Daten in die in AWS gespeicherten Kundeninhalte aufnimmt, muss der Kunde das Format und die Struktur der Inhalte festlegen und wie diese vor der Offenlegung an Unbefugte geschützt werden. Dazu gehört auch, ob die Inhalte anonymisiert oder verschlüsselt werden. Die Kunden wissen, ob sie in AWS Kundeninhalte, die persönliche Daten enthalten, speichern oder verarbeiten, und sie sind daher am besten in der Lage, Personen gegebenenfalls darüber zu informieren, dass sie AWS als Service-Anbieter nutzen. **AWS:** AWS verwendet die Inhalte des Kunden nur, um die vom Kunden gewählten AWS-Dienste für diesen Kunden bereitzustellen. Die Inhalte von Kunden werden für keine anderen Zwecke verwendet.

Auslagern persönlicher Daten	Wenn persönliche Daten ausgelagert werden, kann es erforderlich oder angemessen sein, Personen (Datensubjekte) darüber zu informieren, in welchen Ländern ihre persönlichen Daten gespeichert werden, und/oder ihre Zustimmung für die Speicherung ihrer persönlichen Daten an diesem Standort einzuholen. Es sollte ebenfalls berücksichtigt werden, ob die Datenschutzgesetze im Land, in dem die persönlichen Daten gespeichert werden, vergleichbare Schutzmaßnahmen ermöglichen.	**Kunde:** Wenn Kunden einer geografischen oder regionalen Einschränkung unterliegen, können sie eine AWS-Region (oder Regionen) ihren Anforderungen entsprechend auswählen und ihre Inhalte werden in dieser Region gespeichert und verarbeitet. Kunden sollten überlegen, ob sie die Standorte an Personen offenlegen, an denen die persönlichen Daten dieser Personen gespeichert und verarbeitet werden, und ob gegebenenfalls eine erforderliche Zustimmung hierfür einzuholen ist. Die Kunden haben nicht nur eine Beziehung mit AWS, sie haben auch eine Beziehung mit den Personen, deren persönliche Daten sie auf AWS speichern. Daher können Kunden direkt mit diesen Personen über diese Themen kommunizieren. **AWS:** AWS speichert und verarbeitet die Inhalte seiner Kunden nur in den vom Kunden gewählten Regionen und verwendet nur die vom Kunden gewählten Dienste. Die Inhalte des Kunden werden nicht verschoben, außer dies ist gesetzlich erforderlich. Wenn ein Kunde entscheidet, Inhalte in mehr als einer Region zu speichern, oder Inhalte zwischen Regionen zu kopieren oder zu verschieben, ist dies ausschließlich eine Entscheidung des Kunden. Der Kunde hat weiterhin die effektive Kontrolle über die Inhalte, wo auch immer diese gespeichert und verarbeitet werden. **Allgemein:** AWS ist gemäß ISO 27001 zertifiziert[12] und bietet allen Kunden zuverlässige Sicherheitsfunktionen, unabhängig von der geografischen Region, in der sie ihre Inhalte speichern.

Stufe des Datenlebenszyklus	Zusammenfassung und Beispiele	Überlegungen
Sicherung persönlicher Daten	Es ist wichtig, Maßnahmen zum Schutz von persönlichen Daten zu treffen.	**Kunde:** Kunden sind für die Sicherheit ***in*** der Cloud verantwortlich, einschließlich der Sicherheit ihrer Inhalte (und der persönlichen Daten in ihren Inhalten). **AWS:** AWS ist für die Verwaltung der Sicherheit ***für*** die zugrunde liegende Cloud-Umgebung verantwortlich. Eine ausführliche Liste aller Sicherheitsmaßnahmen, die in unserer grundlegenden AWS-Cloud-Infrastruktur, den Plattformen und Diensten integriert sind, finden Sie im Whitepaper Übersicht über die Sicherheitsmaßnahmen[13] . Kunden können die in der AWS-Umgebung vorhandenen Sicherheitskontrollen anhand von AWS-Zertifizierungen und -Berichten überprüfen, einschließlich der Berichte zur AWS Service Organization Control (SOC) 1, 2 und 3, der ISO 27001-, 27017- und 27018-Zertifizierungen und der PCI-DSS-Compliance-Berichte.

[12] Detaillierte Informationen zu unserer Zertifizierung nach ISO 27001 finden Sie unter https://aws.amazon.com/compliance/iso-27001-faqs/.
[13] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Stufe des Datenlebenszyklus	Zusammenfassung und Beispiele	Überlegungen
Zugriff auf persönliche Daten und Korrektur persönlicher Daten	Personen (Datensubjekte) müssen eventuell auf ihre persönlichen Daten zugreifen, beispielsweise, um sie zu korrigieren.	**Kunde:** Der Kunde behält die Kontrolle darüber, wie Inhalte in AWS gespeichert und verarbeitet werden. Dies umfasst auch die Kontrolle darüber, wie die Inhalte gesichert sind und wer darauf zugreifen und diese ändern kann. Außerdem haben die Kunden nicht nur eine Beziehung mit AWS, sie haben auch eine Beziehung mit den Personen, deren persönliche Daten in den Kundeninhalten enthalten sind, die sie auf AWS speichern oder verarbeiten. Daher sollte auch der Kunde und nicht AWS mit den betreffenden Personen zusammenarbeiten, um ihnen Zugriff auf die in den Kundeninhalten gespeicherten persönlichen Daten zu erteilen, sowie ihnen die Möglichkeit zur Korrektur dieser Daten bereitstellen. **AWS**: AWS verwendet Kundeninhalte nur, um die vom Kunden gewählten AWS-Dienste für diesen Kunden bereitzustellen. AWS hat keinen persönlichen Kontakt zu den Personen, deren persönliche Daten in den Inhalten enthalten sind, die ein Kunde in AWS speichert oder verarbeitet. Aufgrund dessen und aufgrund der umfangreichen Kontrolle, die Kunden über ihre Inhalte haben, ist AWS nicht verpflichtet und auch nicht in der Lage, diesen Personen Zugriff auf ihre persönlichen Daten zu gewähren oder es ihnen zu ermöglichen, diese zu korrigieren.

Stufe des Datenlebenszyklus	Zusammenfassung und Beispiele	Überlegungen
Pflege der Qualität von persönlichen Daten	Es kann von Bedeutung sein, dass persönliche Daten genau sind und dass deren Integrität gewahrt wird.	**Kunde:** Wenn ein Kunde Inhalte, die persönliche Daten enthalten, mit AWS speichert oder verarbeitet, hat der Kunde die Kontrolle über die Qualität dieser Inhalte und kann darauf zugreifen und sie korrigieren. Dies bedeutet, dass der Kunde alle erforderlichen Maßnahmen treffen muss, damit die in den Kundeninformationen enthaltenen persönlichen Daten genau, vollständig und nicht irreführend sind und aktuell gehalten werden. **AWS**: Die im SOC 1, Typ 2-Bericht von AWS beschriebenen Kontrollen sorgen in angemessenem Maß dafür, dass Datenintegrität in allen Phasen, einschließlich Übertragung, Speicherung und Verarbeitung, gewährleistet ist.
Löschen oder Unkenntlichmachen persönlicher Daten	Persönliche Daten sollten im Normalfall nicht länger aufbewahrt werden, als für die Zwecke, für die sie erfasst wurden, erforderlich ist. Andernfalls dürfen sie im Allgemeinen nur gemäß den geltenden Gesetzen zur Vorratsdatenspeicherung aufbewahrt werden.	**Kunde:** Nur der Kunde weiß, warum persönliche Daten in den in AWS gespeicherten Kundeninhalten erfasst wurden, und nur der Kunde kann beurteilen, wann es nicht mehr notwendig ist, diese persönlichen Daten für legitime Zwecke aufzubewahren. Der Kunde sollte die persönlichen Daten löschen oder anonymisieren, wenn sie nicht mehr benötigt werden. **AWS:** AWS stellt dem Kunden Kontrollen zur Verfügung, um Inhalte zu löschen. Dies wird in der unter http://aws.amazon.com/documentation verfügbaren Dokumentation beschrieben.

Datenschutzverletzungen

Da Kunden bei der Nutzung von AWS die Kontrolle über ihre Inhalte behalten, obliegt es auch ihrer Verantwortung, die eigene Umgebung auf Datenschutzverletzungen zu überwachen und Regulierer sowie betroffene Personen gemäß der geltenden Gesetze darüber zu informieren. Diese Verantwortung kann nur der Kunde übernehmen.

Die AWS-Zugriffsschlüssel eines Kunden stellen eine Begründung dar, warum der Kunde und nicht AWS am besten in der Lage ist, diese Verantwortung zu tragen. Kunden haben die Kontrolle über Zugriffsschlüssel und legen fest, wer berechtigt ist, auf ihr AWS-Konto zuzugreifen. AWS hat keinen Einblick auf die Zugriffsschlüssel oder darauf, wer berechtigt und wer nicht berechtigt ist, sich bei einem Konto anzumelden. Daher ist der Kunde für die Überwachung von Verwendung, Missbrauch, Verteilung oder Verlust der Zugriffsschlüssel verantwortlich.

In manchen Jurisdiktionen ist es verpflichtend, Personen oder einen Regulierer über unbefugten Zugriff oder der Offenlegung von persönlichen Daten zu informieren, und es können Situationen auftreten, in denen dies die beste Vorgehensweise zur Minimierung von Risiken darstellt, auch wenn sie nicht verpflichtend ist. Die Kunden bestimmen selbst, wann sie es für angemessen halten, Personen zu informieren, und welchem Benachrichtigungsprozess sie dabei folgen.

Weitere rechtliche Überlegungen

Wie bereits zuvor erwähnt, erläutert dieses Whitepaper keine bestimmten Datenschutz- oder Datensicherungsgesetze. Kunden sollten überlegen, welche speziellen Anforderungen für sie gelten. Dazu gehören auch branchenspezifische Anforderungen. Die für die einzelnen Kunden geltenden entsprechenden Datenschutz- und Datensicherungsgesetze hängen von mehreren Faktoren ab. Dazu zählen der Ort der Geschäftstätigkeit des Kunden, die Branche, in der der Kunde tätig ist, die Art der Inhalte, die gespeichert werden sollen, woher bzw. von wem die Inhalte stammen und wo die Inhalte gespeichert werden.

Kunden, die Bedenken bezüglich ihrer behördlichen Verpflichtungen zum Datenschutz haben, sollten zuerst die für sie geltenden Anforderungen ermitteln und entsprechende Beratung einholen.

Schlussbemerkungen

Sicherheit hat immer höchste Priorität bei AWS. Wir bieten unsere Dienste mehr als einer Million aktiven Kunden an, darunter Unternehmen, Bildungseinrichtungen und Regierungsbehörden aus über 190 Ländern. Zu unseren Kunden zählen Finanz- und Gesundheitsdienstleister, die uns einige ihrer sensibelsten Informationen anvertrauen.

AWS wurde konzipiert, um Kunden Flexibilität in der Konfiguration und der Bereitstellung ihrer Lösungen sowie auch Kontrolle über ihre Inhalte zu bieten. Diese Kontrolle umfasst, wo die Inhalte gespeichert werden, wie sie gespeichert werden und wer darauf Zugriff hat. AWS-Kunden können ihre eigenen, sicheren Anwendungen erstellen und Inhalte sicher auf AWS speichern.

Zusätzliche Ressourcen

Um Kunden ein besseres Verständnis zu vermitteln, wie sie ihre Datenschutz- und Datensicherungsanforderungen handhaben können, stehen auf der AWS-Website Whitepapers zu Risiko, Compliance und Sicherheit, bewährte Methoden, Checklisten und Anleitungen zur Verfügung. Diese Informationen finden Sie unter http://aws.amazon.com/compliance und http://aws.amazon.com/security. Zum Erstellungsdatum dieses Dokuments sind spezielle Whitepapers mit Überlegungen zu Datenschutz und Datensicherung für die folgenden Länder oder Regionen verfügbar:

Australien[14]
Europäische Union[15]
Malaysia[16]
Neuseeland[17]
Singapur[18]

Weitere Informationen

AWS bietet ebenfalls Schulungen, in denen Kunden das Entwerfen, Entwickeln und Betreiben zuverlässiger, effizienter und sicherer Anwendungen in der AWS-Cloud erlernen und ihre Kenntnisse in Bezug auf Amazon Web Services und AWS-Lösungen erweitern und vertiefen können. Wir bieten kostenlose Schulungsvideos, Übungen im Selbststudium und Schulungen mit Dozent an. Weitere Informationen zu AWS-Schulungen finden Sie unter: http://aws.amazon.com/training/.

AWS-Zertifizierungen bescheinigen das technische Wissen und die Kenntnisse bewährter Methoden für die Erstellung sicherer und zuverlässiger Cloud-basierter Anwendungen mit der AWS-Technologie. Weitere Informationen zu AWS-Zertifizierungen finden Sie unter: http://aws.amazon.com/certification/.

Wenn Sie weitere Informationen benötigen, wenden Sie sich unter https://aws.amazon.com/contact-us/ an AWS oder nehmen Sie mit Ihrem örtlichen AWS-Kundenbetreuer Kontakt auf.

---

[14] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf
[15] http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf
[16] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Malaysian_Privacy_Considerations.pdf
[17] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf
[18] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Singapore_Privacy_Considerations.pdf