EU Datenschutz Whitepaper

Oktober 2015

(Die neueste Version dieses Dokuments finden Sie unter http://aws.amazon.com/de/data-protection/). Die englische Version finden Sie unter http://aws.amazon.com/compliance/aws-whitepapers/)

Einleitung

Dieses Dokument soll Kunden helfen, die AWS für die Speicherung von Inhalten, die personenbezogene Daten enthalten, nutzen wollen. Konkret beschreibt dieses Dokument wie Kunden AWS-Services in Übereinstimmung mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ("**Richtlinie**") nutzen können. Es soll den Kunden ein besseres Verständnis zu folgenden Themen geben:

- Die Art und Weise, wie die AWS-Services funktionieren, einschließlich der Frage, wie Kunden den Anforderungen des europäischen Rechts entsprechen, ihren Sicherheitsbedürfnissen nachkommen und ihre Inhalte verschlüsseln und anderweitig schützen können.
- Die vollständige Kontrolle der Kunden über die geographischen Standorte, an denen ihre Inhalte gespeichert und abgerufen werden können sowie andere einschlägige Compliance-Erwägungen.
- Die Rollen, die dem Kunden und AWS jeweils bei der Verwaltung und der Sicherung der in den AWS-Services gespeicherten Inhalte zukommen.

Dieses Whitepaper konzentriert sich auf die typischen Fragen, die von AWS-Kunden gestellt werden, wenn diese die Auswirkungen der Richtlinie auf ihre Nutzung der AWS-Services zur Speicherung von Inhalten einschließlich personenbezogener Daten betrachten. Für jeden Kunden werden außerdem andere relevante Erwägungen zu berücksichtigen sein, etwa das Erfordernis von Kunden mit bestimmten branchenspezifischen Anforderungen sowie Gesetzen anderer Rechtsordnungen, in denen der Kunde Geschäfte betreibt, einzuhalten. Dieses Dokument dient lediglich zu Informationszwecken. Es stellt keine Rechtsberatung dar und sollte auch nicht als solche verstanden werden. Da die Anforderungen jedes Kunden unterschiedlich sein werden, ermutigt AWS seine Kunden, qualifizierten Rat einzuholen, wie er Anforderungen an Datenschutz und Datensicherheit sowie grundsätzlich das auf das jeweilige Geschäft anwendbare Recht umsetzt.

Erwägungen bezüglich Kundeninhalte

Die Speicherung von Inhalten stellt alle Organisationen vor eine Reihe von bekannten praktischen Themen, die zu berücksichtigen sind, unter anderem:

- Werden die Inhalte sicher sein?
- Wo werden die Inhalte gespeichert?
- Wer wird Zugriff auf die Inhalte haben?
- Welche Gesetze und Vorschriften sind auf die Inhalte anwendbar und was ist nötig, um diese einzuhalten?

Diese Erwägungen sind nicht neu und sind nicht Cloud-spezifisch. Sie sind für intern gehostete und betriebene Systeme genauso relevant wie für herkömmliche von Dritten gehostete Services. Wenn Kunden die AWS-Services nutzen, behalten sie die Kontrolle über ihre Inhalte und sind dafür verantwortlich – und vollumfänglich befähigt –, Sicherheitsanforderungen zum Schutz ihrer Inhalte zu regeln und zu kontrollieren, unter anderem:

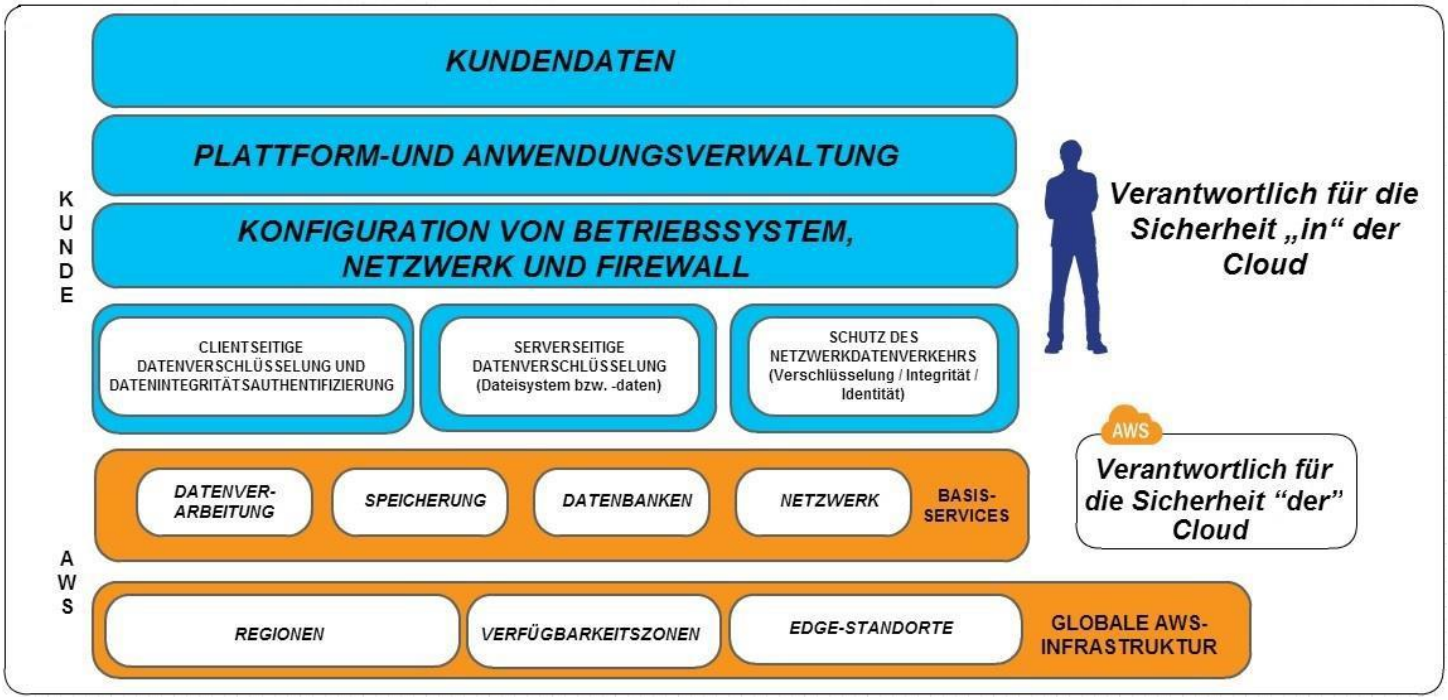
- Welche Inhalte werden für die Speicherung auf AWS ausgewählt
- Ob diese Inhalte verschlüsselt werden – im Ruhezustand und im Transit
- Welche AWS-Services werden im Zusammenhang mit den Inhalten genutzt
- Wo auf der Welt werden die Inhalte gespeichert und verarbeitet

- Das Format und die Struktur dieser Inhalte und ob sie maskiert oder anonymisiert sind
- Wem sie den Zugriff auf diese Inhalte erlauben und wie diese Zugriffsrechte erteilt, verwaltet und widerrufen werden.

Der Schutz der Kundeninhalte hängt davon ab, dass AWS und der Kunde angemessene Maßnahmen implementieren. Während AWS Sicherheitsvorkehrungen in seiner zugrunde liegenden Cloud-Umgebung implementiert, behalten AWS-Kunden die Kontrolle über ihre Inhalte und die Sicherheit dieser Inhalte. Die jeweiligen unterschiedlichen Rollen des Kunden und von AWS zu verstehen, ist im Lichte der Datenschutzanforderungen, die möglicherweise auf bei AWS gespeicherte personenbezogene Daten anwendbar sind, von grundlegender Bedeutung.

Sicherheit von Kundeninhalten:

IT-Infrastruktur zu AWS zu verlegen, bedeutet, dass sowohl dem Kunden als auch AWS wichtige Rollen bei dem Betrieb und dem Sicherheitsmanagement in ihrem Verantwortungsbereich zukommen. AWS betreibt, verwaltet und überwacht die Komponenten von der Schicht des Host-Betriebssystems und des Virtualization Layers bis hinunter zum physischen Schutz der Einrichtungen, in denen die AWS-Services betrieben werden. Der Kunde ist verantwortlich für die Verwaltung des Gast-Betriebssystems (einschließlich Updates und Security Patches für das Gast-Betriebssystem) und der zugehörigen Anwendungssoftware sowie für die Konfiguration der von AWS bereitgestellten Security Group Firewall und anderer Sicherheits-Features. Der Kunde wird sich üblicherweise über Drittanbieter mit der AWS-Umgebung verbinden (z.B. Internetdienstanbieter). Diese Verbindungen bietet AWS nicht an. Der Kunde sollte die Sicherheit solcher Verbindungen und die Sicherheitsverantwortung solcher Anbieter im Hinblick auf die Systeme des Kunden prüfen. Tatsächlich unterscheidet sich dies nicht von der Zusammenarbeit mit einem Netzwerkanbieter, der die Verbindung zu einem vor Ort betriebenen Rechenzentrum herstellt. Dieses Model ist in der folgenden Übersicht 1 dargestellt:



Übersicht 1 – Das Sicherheitsmodell

Was bedeutet dieses Modell für die Sicherheit der Kundeninhalte?

Bei der Bewertung der Sicherheit von Cloud-Lösungen ist folgende Unterscheidung wichtig:

- Sicherheitsmaßnahmen, die der Cloud Service Anbieter (AWS) durchführt – "Sicherheit ***der*** Cloud" und
- Sicherheitsmaßnahmen, die der Kunde in Bezug auf die Sicherheit der Kundeninhalte und der Anwendungen, welche die AWS-Services nutzen, durchführt – "Sicherheit ***in*** der Cloud"

Während AWS die Sicherheit ***der*** Cloud gewährleistet, ist der Kunde für die Sicherheit ***in*** der Cloud verantwortlich, da die Kunden die Kontrolle darüber behalten, welche Sicherheitsmaßnahmen sie ergreifen, um ihre eigenen Inhalte, ihre eigene Plattform, Anwendungen, Systeme und Netzwerke zu schützen – genauso wie bei Anwendungen in einem vor Ort betriebenen Rechenzentrum. Als Teil seiner verschiedenen Serviceangebote bietet AWS seinen Kunden eine Reihe von Sicherheitsmaßnahmen an und unsere Kunden können auch eine Vielzahl von Dritten angebotene Sicherheitslösungen verwenden. AWS-Kunden sind völlig frei darin, ihre Sicherheitsarchitektur so zu gestalten, dass sie ihre Compliance-Erfordernisse erfüllt. Dies ist ein wesentlicher Unterschied zu herkömmlichen Hosting-Lösungen bei denen der Anbieter über die Architektur entscheidet. AWS stellt es dem Kunden frei, ob Sicherheitsmaßnahmen implementiert werden, und – falls ja –welche Sicherheitsmaßnahmen in der Cloud implementiert werden und ob diese für sein Geschäft angemessen sind. Wenn z.B. eine Architektur mit höherer Verfügbarkeit zum Schutz der Daten erforderlich ist, kann der Kunde redundante Systeme, Backups, Standorte, Netzwerkanbindungen usw. hinzufügen, um eine robustere, hochverfügbare Architektur zu schaffen. Wenn eine Beschränkung des Datenzugriffs erforderlich ist, kann der Kunde über die AWS-Kontrollmechanismen Konzepte zur Steuerung der Zugriffsrechte sowohl auf Systemebene als auch durch Verschlüsselung auf Datenebene implementieren. AWS ermöglicht dem Kunden daher die unmittelbare Kontrolle vieler Elemente, die technische und organisatorische Maßnahmen im Sinne der Datensicherheit darstellen.

Sicherheit *DER* Cloud

AWS ist für die Sicherheit der zugrunde liegenden Cloud-Umgebung verantwortlich. Die AWS Cloud-Infrastruktur wurde als eine der flexibelsten und sichersten Cloud Computing-Umgebungen geschaffen. Sie wurde für ein Optimum an Verfügbarkeit bei vollständiger Kundentrennung konzipiert. Sie liefert eine extrem skalierbare, sehr betriebssichere Plattform, die es den Kunden erlaubt, Anwendungen und Inhalte bei Bedarf schnell und sicher weltweit auszubringen. Die AWS-Services sind insofern inhalteunabhängig, als sie allen Kunden dasselbe hohe Sicherheitsniveau bieten, unabhängig von der Art der Inhalte oder von der geographischen Region, in der die Inhalte gespeichert werden. Da AWS nicht weiß, welche Inhalte Kunden auf AWS Services speichern, kann AWS personenbezogene Daten nicht von anderen Daten, die ein Kunde als Teil seiner Inhalte speichert, unterscheiden.

Die hochsicheren AWS-Rechenzentren auf Weltklasseniveau verwenden elektronische Überwachungsmaßnahmen auf dem Stand der Technik und mehrstufige Zugangskontrollsysteme. Die Rechenzentren sind rund um die Uhr mit ausgebildetem Sicherheitspersonal besetzt und der Zugriff wird streng nach dem Prinzip der geringsten Rechte und ausschließlich zum Zweck der Systemadministration gewährt. Für eine vollständige Darstellung aller Sicherheitsmaßnahmen, die in die Cloud-Infrastruktur, Plattformen und Services von AWS integriert sind, lesen Sie bitte das Whitepaper 'Übersicht über die Sicherheitsprozesse'.

Wir achten sehr auf die Sicherheit unserer zugrunde liegenden Cloud-Umgebung und haben hochentwickelte technische und organisatorische Maßnahmen gegen unerlaubten Zugriff implementiert. Kunden können die Sicherheitsmaßnahmen der AWS-Umgebung durch AWS Zertifikate und Berichte validieren. Hierzu gehören die AWS Service Organization Control (SOC) 1 und 2, ISO 27001-Zertifizierung und PCI-DSS-Compliance. Diese Berichte und Zertifikate werden durch unabhängige Auditoren erstellt und belegen die konstruktive und operative Wirksamkeit der AWS-

Sicherheitsmaßnahmen. Die anwendbaren AWS Compliance-Zertifikate und Berichte können unter folgender Adresse angefordert werden: http://aws.amazon.com/de/compliance/contact/ Weitere Informationen zu AWS Compliance-Zertifikaten, Berichten und zur Orientierung an Best Practices und Standards finden sich auf der AWS compliance Seite.

AWS bietet eine Auftragsdatenverarbeitungsvereinbarung an, um Kunden zu helfen, ihre datenschutzrechtlichen Verpflichtungen zu erfüllen. AWS kann die Auftragsdatenverarbeitungsvereinbarung mit dem Kunden auch um die Standardvertragsklauseln 2010/87/EU für die Übermittlung personenbezogener Daten in Drittländer (oft auch nur als „Standardvertragsklauseln“ bezeichnet) ergänzen, wenn der Kunde diese benötigt um personenbezogene Daten aus der EU in ein Land außerhalb des Europäischen Wirtschaftsraums zu übermitteln.

Am 6. März 2015 wurde die um die Standardvertragsklauseln ergänzte Auftragsdatenverarbeitungsvereinbarung von der als “Artikel-29-Datenschutzgruppe” bezeichneten Gruppe der nationalen Datenschutzbehörden der EU-Mitgliedstaaten genehmigt. Diese Genehmigung bedeutet, dass jeder AWS-Kunde, der die Standardvertragsklauseln benötigt, sich jetzt darauf verlassen kann, dass die AWS Auftragsdatenverarbeitungsvereinbarung ausreichende vertragliche Verpflichtungen enthält, um internationale Datenströme in Übereinstimmung mit der Richtlinie zu ermöglichen. Ausführliche Informationen zu der Genehmigung der Artikel-29-Datenschutzgruppe erhalten Sie auf folgender Seite der luxemburgischen Datenschutzbehörde:

http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

Sicherheit *IN* der Cloud

Kunden behalten die Kontrolle über ihre Inhalte, wenn sie AWS-Services verwenden. Nicht AWS, sondern die Kunden entscheiden darüber, welche Inhalte sie bei AWS speichern, kontrollieren, wie sie ihre Umgebungen konfigurieren und ihre Inhalte schützen, ob sie ihre Inhalte in Ruhe oder im Transit verschlüsseln, wer Zugang zu diesen Inhalten hat und welche Zugangsdaten verlangt werden (einschließlich der Nutzung von Multi-Faktor-Authentifizierung) und welche zuätzlichen Sicherheit-Features und Tools sie nutzen und wie sie sie nutzen. Da unsere Kunden die Kontrolle über ihre Sicherheit behalten, bleiben sie auch für die Sicherheit von allem, was ihre Organisation an AWS überträgt oder was sie mit ihrer AWS-Infrastruktur verbinden, wie etwas das Gast-Betriebssystem, Anwendungen auf ihrer Recheninstanz und Inhalte, die in AWS Speicher-, Plattform- und Datenbank-Services gespeichert und verarbeitet werden, verantwortlich.

Kunden können ihre AWS-Services so konfigurieren, dass sie eine Reihe von optionalen Sicherheits-Features, Tools und Kontrollmechanismen zum Schutz ihrer Inhalte einsetzen, einschließlich hochentwickelter Identitäts- und Zugriffsmanagement-Tools, Verfügbarkeitseinstellungen, Backup-Funktionen, Sicherheitsfunktionen, Verschlüsselung und Netzwerksicherheit. Um Kunden beim Design, bei der Implementierung und beim Betrieb ihrer eigenen sicheren AWS-Umgebung zu unterstützen, bietet AWS eine Vielzahl von Sicherheits-Features, die Kunden nutzen können. Kunden können aber auch ihre eigenen Sicherheits-Tools und Kontrollmechanismen oder die von Dritten nutzen. Beispielsweise können Kunden die folgenden Maßnahmen ergreifen, um den Schutz ihrer Inhalte zu verbessern:

- Policies für starke Passwörter, die angemessene Berechtigungen an Nutzer erteilen und robuste Maßnahmen zum Schutz der Zugriffsschlüssel enthalten;
- Angemessene Firewalls und Netzwerktrennung (einschließlich Virtual Private Cloud), Verschlüsselung von Inhalten, Benutzung von SSL und eine geeignete Systemarchitektur, um das Risiko von Datenverlust und unberechtigtem Zugriff zu verringern;
- Angemessene Redundanz-Modelle und Backup-Strategien, um das Risiko des Verlusts oder der Nichtverfügbarkeit von Daten zu entschärfen.

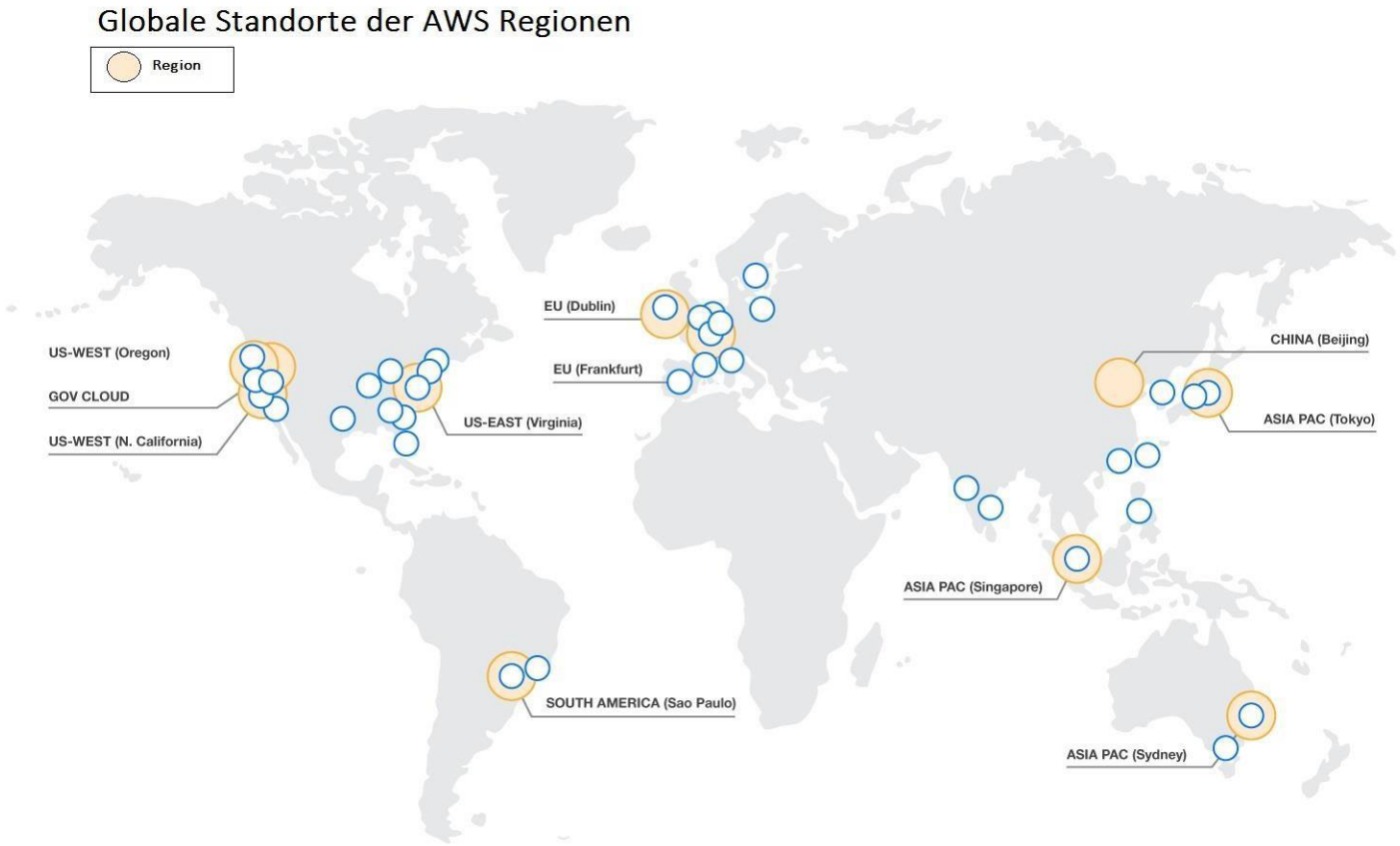
Über alle diese Faktoren hat der Kunde die Kontrolle, nicht AWS. AWS hat keinen Einblick in die Inhalte, die der Kunde auf AWS einstellt, und ändert auch nicht die Einstellungen des Kunden. Diese werden durch den Kunden festgelegt und

stehen unter dessen Kontrolle. Da es der Kunde ist, der darüber entscheidet, welchen Inhalt er in die AWS-Cloud stellt, kann auch nur der Kunde entscheiden, welches Sicherheitsniveau für die dort gespeicherten Daten angemessen ist.

Um Kunden bei der Integration der AWS Sicherheitskontrollmechanismen in den bei ihnen bestehenden Rahmen von Kontrollmechanismen zu unterstützen und um Kunden bei der Planung und Durchführung von Sicherheitsprüfungen der Nutzung von AWS-Services durch ihre eigene Organisation zu helfen, veröffentlicht AWS eine Reihe von Whitepapers, die sich mit Sicherheit, Governance, Risiko und Compliance befassen, sowie eine Reihe von Checklisten und Best Practices. Es steht Kunden frei, Sicherheitsprüfungen nach ihren eigenen Vorlieben zu planen und durchzuführen. Sie können die Erlaubnis beantragen, Scans ihrer Cloud-Infrastruktur durchzuführen (sofern diese Scans auf die Recheninstanzen des Kunden beschränkt sind und nicht gegen die AWS Acceptable Use Policy verstoßen).

AWS Regionen

Die AWS Rechenzentren sind in Clustern in verschiedenen Ländern der Welt errichtet. Wir bezeichnen jedes unserer Rechenzenter-Cluster im jeweiligen Land als eine "Region". Kunden haben Zugang zu elf AWS-Regionen rund um den Globus, einschließlich zwei Regionen in der EU – Irland (Dublin) und Deutschland (Frankfurt). Kunden können sich entscheiden, eine Region zu verwenden oder alle Regionen oder jede Kombinationen von Regionen. Übersicht 2 zeigt die Lage der AWS-Regionen:



Übersicht 2 – AWS-Regionen in der Welt

AWS-Kunden wählen die AWS-Region(en), in denen ihre Inhalte gehosted werden. Dies erlaubt Kunden mit besonderen Anforderungen an den Ort der Datenverarbeitung, Umgebungen an einem Standort bzw. an Standorten ihrer Wahl einzurichten. Zum Beispiel können sich AWS-Kunden in Europa dafür entscheiden, ihre AWS-Services ausschließlich in

der EU (Deutschland) Region einzusetzen. Wenn der Kunde sich so entscheidet, werden die Inhalte in Deutschland gespeichert, es sei denn, der Kunde wählt eine andere AWS-Region.

Kunden können Inhalte in mehr als einer Region replizieren und als Backup sichern, aber AWS selbst überträgt Kundeninhalte nicht außerhalb der vom Kunden gewählten Region(en).

Wie können Kunden ihre Region(en) auswählen?

Durch Auswahl in der AWS Management Console oder durch Übermittlung einer Anfrage über eine AWS-Programmierschnittstelle (API) bestimmt der Kunde die genaue(n) Region(en), in denen er die AWS-Services nutzen möchte. Übersicht 3 zeigt ein Beispiel für die Auswahl der weltweiten AWS Regionen, die dem Kunden beim Upload von Inhalten auf einen AWS Speicherservice oder bei der Bereitstellung von Rechenleistung unter Rückgriff auf die AWS Management Console zur Verfügung stehen.

Übersicht 3 – Auswahl der weltweiten AWS Regionen in der AWS Management Console

Kunden können die AWS-Region, die für ihre Rechenleistungen verwendet wird, auch vorgeben, indem sie die Funktion Amazon Virtual Private Cloud (VPC) nutzen. Die Amazon VPC erlaubt es dem Kunden, einen Teil der AWS Cloud zu bestimmen, in dem der Kunde AWS Ressourcen in einem virtuellen Netzwerk starten kann, das der Kunde definiert. Mit der Amazon VPC können Kunden eine virtuelle Netzwerktopologie definieren, die einem herkömmlichen Netzwerk, das in einem ihrer eigenen Rechenzentren laufen könnte, stark ähnelt.

Jede Rechen- und andere Ressource, die der Kunde in der VPC startet befindet sich in der vom Kunden gewählten Region. Kontrollen des Kunden und Zugriff auf Kundeninhalte

Kontrolle des Kunden über Inhalte

Kunden, die AWS nutzen, behalten die Kontrolle über ihre Inhalte in der AWS-Umgebung. Sie können

- darüber bestimmen, wo sie abgelegt werden, z.B. die Art der Speicherumgebung und die geographische Lage des Speichers;
- das Format des Inhalts bestimmen, z.B. Nur-Text, maskiert, anonymisiert oder verschlüsselt, indem sie entweder die von AWS bereitgestellte Verschlüsselung oder einen vom Kunden gewählten Verschlüsselungsmechanismus eines Drittanbieters verwenden;
- andere Zugriffskontrollen verwenden, wie Identitätsmanagement und Sicherheitsanmeldeinformationen;
- die Nutzung von SSL, Virtual Private Cloud und anderen Netzwerksicherheitsmaßnahmen zur Verhinderung unberechtigter Zugriffe kontrollieren.

Dies erlaubt es AWS-Kunden, den gesamten Lebenszyklus ihrer Inhalte bei AWS zu kontrollieren und die Inhalte gemäß ihren eigenen konkreten Anforderungen zu verwalten, einschließlich Klassifizierung, Zugriffskontrolle, Aufbewahrung und Löschung.

Zugriff auf Kundeninhalte

AWS greift nicht auf Kundeninhalte zu, es sei denn, dies ist notwendig, um gegenüber dem jeweiligen Kunden die AWS-Services zu erbringen, die dieser ausgewählt hat. AWS greift auf Kundeninhalte für keinen anderen Zweck zu.

AWS weiß nicht, welche Inhalte Kunden auf AWS speichern, und kann nicht zwischen personenbezogenen Daten und anderen Inhalten unterscheiden, so dass AWS alle Kundeninhalte gleich behandelt. Auf diese Weise kommen dieselben robusten AWS Sicherheitsmaßnahmen allen Kundeninhalten zu Gute, unabhängig davon, ob Sie personenbezogene Daten enthalten oder nicht. AWS stellt einfach nur die Rechen-, Speicher-, Datenbank und Netzwerkservices zur Verfügung, die der Kunde auswählt, unter Anwendung von best-in-class Sicherheitsmaßnahmen für die von AWS angebotene Cloud-Infrastruktur. Dem Kunden steht es dann frei, auf diese Infrastruktur Sicherheitsmaßnahmen entsprechend seinen eigenen Anforderungen aufzubauen.

Zugriffsrechte von Regierungen

Häufig kommen Fragen auf, welche Rechte in- oder ausländische Regierungsorganisationen haben, auf Inhalte zuzugreifen, die in Cloud-Services gespeichert sind. Kunden haben häufig Bedenken hinsichtlich der Datenhoheit, unter anderem ob und unter welchen Umständen Regierungen Zugriff auf ihre Inhalte haben. Das Recht des Landes, in dem die Inhalte gespeichert sind, ist ein wichtiger Faktor für manche Kunden. Allerdings sollten Kunden auch prüfen, ob Gesetze anderer Länder vielleicht auf sie anwendbar sind, abhängig davon, wo sie oder ihre Kunden aktiv sind. Kunden sollten sich beraten lassen, um die Anwendung einschlägiger Gesetze auf ihren Geschäftsbetrieb zu verstehen.

Wenn Bedenken oder Fragen geäußert werden im Hinblick auf das Recht in- oder ausländischer Regierungen, Zugriff auf die in der Cloud gespeicherten Inhalte zu verlangen, ist es wichtig zu verstehen, dass relevante Regierungsorganisationen bereits nach den aktuell auf den Kunden anwendbaren Gesetzen das Recht haben können, solche Inhalte heraus zu verlangen. Zum Beispiel kann ein Unternehmen, welches Geschäfte in Land X macht, einem Auskunftsanspruch ausgesetzt sein, selbst wenn der Inhalt in Land Y gespeichert ist. Üblicherweise wird eine Regierungsorganisation, die Zugriff auf die Daten eines Unternehmens nehmen will, ihr Auskunftsverlangen direkt an dieses Unternehmen richten, anstatt sich an den Cloud-Anbieter zu wenden.

Im Allgemeinen gibt es in den Mitgliedstaaten der EU Gesetze, welche die öffentlichen Strafverfolgungsbehörden und nationale Sicherheitsbehörden ermächtigen, Zugriff auf Informationen zu verlangen. Ausländische Strafverfolgungsbehörden können auch mit den lokalen Strafverfolgungsbehörden und nationalen Sicherheitsbehörden zusammenarbeiten, um Zugriff auf Informationen in der EU zu erhalten. Die meißten Länder verfügen über Prozesse (einschließlich gegenseitige Rechtsbeihilfeabkommen), um zur Beantwortung angemessener rechtmäßiger

Informationsersuchen den Transfer von Informationen in anderen Ländern zu ermöglichen. Allerdings ist es wichtig, sich zu vergegenwärtigen, dass nach dem jeweiligen Recht bestimmte Kriterien erfüllt sein müssen, bevor dem Zugriffsverlangen einer Strafverfolgungsbehörde stattgegeben wird. Zum Beispiel wird die Regierungsorganisation, die den Zugriff verlangt, höchstwahrscheinlich nachweisen müssen, dass es einen triftigen Grund für das Zugriffsverlangen auf die Inhalte gibt, und wird wohl einen Gerichtsbeschluss oder Durchsuchungsbefehl erwirken müssen.

Die meisten Länder haben Gesetze zum Zugriff auf Daten, die auch über die Landesgrenzen hinaus anwendbar sein sollen. Ein Beispiel eines US Gesetzes mit extraterritorialer Reichweite, das häufig im Zusammenhang mit Cloud-Services genannt wird, ist der US Patriot Act. Der Patriot Act unterscheidet sich nicht von den Gesetzen vieler anderer Industriestaaten, welche die Regierungen ermächtigen, Informationen im Zusammenhang mit den Ermittlungen zu internationalem Terrorismus und anderen Angelegenheiten des Auslandsgeheimdienstes zu erhalten. Jedes Verlangen auf Herausgabe von Dokumenten unter dem Patriot Act erfordert einen Gerichtsbeschluss, der darlegt, dass das Verlangen im Einklang mit den Gesetzen steht, z.B. dass das Verlangen mit rechtmäßigen Ermittlungen zusammenhängt.

AWS Policy

Unabhängig davon, wo ein Ersuchen bezüglich Kundeninhalten herkommt oder wer der Kunde ist, AWS ist stets achtsam hinsichtlich des Schutzes der Inhalte unserer Kunden. AWS wird Kundeninhalte nicht offen legen, außer dies ist erforderlich, um rechtlich gültigen und bindenden Anordnungen, wie etwa einem Untersuchungsbescheid (subpoena) oder einer richterlichen Anordnung, nachzukommen. Nicht-US-Behörden müssen in der Regel anerkannte internationale Prozesse, wie etwa gegenseitige Rechtsbeihilfeabkommen mit der US-Regierung, befolgen, um gültige und bindende Anordnungen zu erwirken. Wir prüfen jedes Ersuchen sorgfältig, um seine Richtigkeit und Übereinstimmung mit dem anwendbaren Recht zu verifizieren. Wir werden Ersuchen in Frage stellen, die zu weit gefasst sind, die Kompetenz der ersuchenden Behörde überschreiten oder nicht vollständig mit dem anwendbaren Recht in Einklang stehen. Wenn wir gezwungen sind, Kundeninhalte herauszugeben, benachrichtigen wir unsere Kunden vor der Herausgabe, um ihnen die Möglichkeit zu geben, sich gegen die Herausgabe zu wehren, außer dies ist rechtlich verboten.

Datenschutz in der EU

Die Richtlinie

Im Folgenden betrachten wir die Anforderungen, die sich aus der Richtlinie ergeben[1]. Grob gesagt stellt die Richtlinie eine Reihe von Datenschutzanforderungen auf, die anwendbar sind, wenn personenbezogene Daten verarbeitet werden. In diesem Kontext umfasst der Begriff "verarbeiten" jeden Vorgang oder jede Gesamtheit von Vorgängen in Bezug auf personenbezogene Daten. Gemäß der Richtlinie werden "personenbezogene Daten" definiert als alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"). Darüber hinaus unterscheidet die Richtlinie zwischen (a) dem "für die Verarbeitung Verantwortlichen" bzw. der "verantwortlichen Stelle" (*data controller*) – die Partei, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet und (b) einem "Auftragsverarbeiter" (*data processor*) – die Partei, welche die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet.

Es ist die Aufgabe der verantwortlichen Stelle, sicherzustellen, dass die Verarbeitung der personenbezogenen Daten mit den Datenschutzvorschriften in Einklang steht. So muss zum Beispiel die verantwortliche Stelle sicherstellen, dass die personenbezogenen Daten angemessen und rechtmäßig verarbeitet werden und dass die Daten gegen eine unberechtigte und unrechtmäßige Verarbeitung geschützt werden.

[1] Es ist zu beachten, dass die Richtlinie nicht unmittelbar auf Organisationen mit Sitz in einem EU Mitgliedsstaat anwendbar ist. Stattdessen müssen die EU Mitgliedsstaaten die Richtlinie in ihre nationalen Gesetze umsetzten. Als Folge davon kann es zu Abweichungen bei den konkreten Pflichten in den verschiedenen Mitgliedsstaaten kommen. Kunden sollten sich daher beraten lassen, welche nationalen Rechte auf sie anwendbar sind.

AWS ist sich bewusst, dass seine Services als Bestandteil unterschiedlichster Geschäftsabläufe genutzt werden und dass viele verschiedene Parteien in die Lieferkette eingebunden sein können. Falls jedoch personenbezogene Daten in den Kundeninhalten enthalten sind, die unter Nutzung der AWS-Services gespeichert werden, kann Folgendes als allgemeine Leitlinie gelten:

- Der Kunde ist verantwortliche Stelle in Bezug auf die personenbezogenen Daten, für die der Kunde den Verarbeitungszweck bestimmt hat und bei denen er entschieden hat, wie sie verarbeitet werden.

- Der Kunde ist Auftragsverarbeiter in Bezug auf solche personenbezogene Daten, bei denen er die personenbezogenen Daten lediglich im Auftrag und nach den Wünschen eines Dritten auf dem AWS-Netzwerk verarbeitet (wobei der Dritte seinerseits verantwortliche Stelle sein kann, oder aber eine andere Partei in der Lieferkette oder eine Einzelperson, die nur in eigenen Belangen handelt).

Als Anbieter einer Selbstbedienungs-Infrastruktur, die vollständig unter der Kontrolle des Kunden ist (einschließlich hinsichtlich des Ob und Wie der „Datenverarbeitung"), bietet AWS lediglich Infrastruktur-Services für Kunden an, die Inhalte auf das AWS-Netzwerk hochladen und dort verarbeiten wollen. In diesem Zusammenhang hat AWS keinen Einblick in oder Kenntnis davon, was Kunden auf das AWS-Netzwerk hochladen, und auch nicht, ob der Inhalt personenbezogene Daten enthält oder nicht. AWS-Kunden haben zudem die Möglichkeit, Verschlüsselung zu verwenden, um die Inhalte für AWS unlesbar zu machen. AWS verarbeitet Kundeninhalte nicht, es sei denn, dies ist erforderlich für die Erbringung der Services (oder um dem Gesetz oder einer wirksamen und bindenden Anordnung nachzukommen). Zudem verfügt AWS über Systeme, Maßnahmen und Richtlinien, um jeden Zugriff auf Kundeninhalte von AWS-Angestellten zu verhindern. Außerdem bietet AWS für Kunden, die personenbezogenen Daten verarbeiten möchten, eine Auftragsdatenverarbeitungsvereinbarung an, um diesen Kunden zu helfen, ihre datenschutzrechtlichen Verpflichtungen zu erfüllen. AWS kann die Auftragsdatenverarbeitungsvereinbarung mit dem Kunden auch um die Standardvertragsklauseln ergänzen, wenn der Kunde diese benötigt um personenbezogene Daten aus der EU in ein Land außerhalb des Europäischen Wirtschaftsraums zu übermitteln.

Am 6. März 2015 wurde die um die Standardvertragsklauseln ergänzte Auftragsdatenverarbeitungsvereinbarung von der als "Artikel-29-Datenschutzgruppe" bezeichneten Gruppe der nationalen Datenschutzbehörden der EU-Mitgliedstaaten genehmigt. Diese Genehmigung bedeutet, dass jeder AWS-Kunde, der die Standardvertragsklauseln benötigt, sich jetzt darauf verlassen kann, dass die AWS Auftragsdatenverarbeitungsvereinbarung ausreichende vertragliche Verpflichtungen enthält, um internationale Datenströme in Übereinstimmung mit der Richtlinie zu ermöglichen. Ausführliche Informationen zu der Genehmigung der Artikel-29-Datenschutzgruppe erhalten Sie auf folgender Seite der luxemburgischen Datenschutzbehörde:
http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

Die verantwortliche Stelle muss dafür Sorge tragen, dass technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten gegen zufällige oder unrechtmäßige Zerstörung oder zufälligen Verlust, Veränderung unberechtigte Offenlegung oder Zugriff getroffen werden. Erfolgt die Datenverarbeitung durch einen Auftragsverarbeiter im Auftrag der verantwortlichen Stelle, ist die verantwortliche Stelle auch dafür verantwortlich, einen Auftragsverarbeiter auszusuchen, der ausreichende technische und organisatorische Maßnahmen zum Schutz der durchzuführende Datenverarbeitung zur Verfügung stellt.

In der folgenden Tabelle fassen wir einige wesentliche datenschutzrechtliche Prinzipien zusammen, die Kunden üblicherweise in diesem Zusammenhang berücksichtigen. Wir erörtern auch Aspekte der AWS-Services die im Rahmen dieser Prinzipien relevant sind. Zum Zwecke dieser Tabelle sind wir davon ausgegangen, dass der AWS-Kunde verantwortliche Stelle ist. Wie vorstehend bereits erwähnt, ist uns jedoch bewusst, dass es viele Situationen geben kann, in denen der AWS-Kunde der Auftragsverarbeiter ist. Aber auch in diesen Situationen können die folgenden Ausführungen für den Kunden in seiner Beziehung zur verantwortlichen Stelle hilfreich sein.

Datenschutzgrundsatz	**Zusammenfassung der datenschutzrechtlichen Verpflichtung**	**Erwägungen**
Fairness	Betroffene sollten korrekte und vollständige Informationen über die Identität der verantwortlichen Stelle, den Zweck der Verarbeitung und alle anderen Informationen, die für eine angemessene Datenverarbeitung erforderlich sind, erhalten.	**Kunde:** Der Kunde (oder dessen Kunde) entscheidet darüber, welche Informationen er erhebt und für welchen Zweck er diese Informationen verwendet. In vielen Fällen wird der Kunde eine direkte Beziehung zu den Betroffenen haben und somit in einer guten Ausgangslage sein, um direkt mit ihnen zu kommunizieren. Darüber hinaus sollte der Kunde über den Umfang jeder vorherigen Mitteilung an die Betroffenen informiert sein. **AWS:** AWS hat keine Kontrolle darüber, welche Art von Inhalten der Kunde in AWS speichert und für welchen Zweck dies geschieht. AWS hat keinen Einblick in die Inhalte (einschließlich der Frage, ob diese Inhalte personenbezogene Daten enthalten). AWS hat keine Möglichkeit, Betroffene, deren personenbezogene Daten der Kunde auf der AWS-Infrastruktur gespeichert hat, zu identifizieren oder zu kontaktieren. AWS kann daher Betroffenen keine relevanten Informationen geben.

Datenschutzgrundsatz	**Zusammenfassung der datenschutzrechtlichen Verpflichtung**	**Erwägungen**
Ermächtigungsgrundlage	Die verantwortliche Stelle benötigt eine Ermächtigungsgrundlage für die Verarbeitung, die zumindest einem der in der Richtlinie aufgestellten Kriterien entspricht.	**Kunde:** Wenn der Kunde darüber entscheidet, ob und für welchen Zweck er personenbezogene Daten verarbeitet, muss der Kunde auch bedenken, ob er eines der Kriterien der Richtlinie erfüllt. Zu den Kriterien gehört beispielsweise, dass der Betroffene seine Einwilligung erklärt hat oder dass die Verarbeitung für die Durchführung eines Vertrags mit dem Betroffenen erforderlich ist. **AWS:** Wie vorstehend dargelegt, hat AWS keine Kontrolle darüber, welche Art von Inhalten der Kunde bei AWS speichert (und auch nicht, ob diese Inhalte personenbezogene Daten umfassen). AWS bestimmt nicht, welche Architektur der Kunde durch die Kombination der AWS-Service-Angebote erstellt und ob diese für die konkreten Bedürfnisse des Kunden angemessen ist. AWS ist nicht in den Entscheidungsprozess eingebunden, ob und für welchen Zweck die Daten verarbeitet werden. Dementsprechend ist AWS nicht in der Lage zu beurteilen, ob eine Ermächtigungsgrundlage für die Verarbeitung vorliegt.
Zweckbindung	Personenbezogen Daten dürfen nur für bestimmte, genau festgelegte und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer Art verarbeitet werden, die mit diesen Zwecken nicht vereinbar ist.	**Kunde:** Es ist Sache des Kunden zu bestimmen, welche personenbezogenen Daten er erhebt und für welche Zwecke sie verwendet werden. Wenn er diese Entscheidung trifft, muss der Kunde sicherstellen, dass es einen bestimmten, genau festgelegten und rechtmäßigen Zweck gibt. Der Kunde entscheidet darüber, ob die Daten danach für andere Zwecke verarbeitet werden und kann abwägen, ob diese anderen Zwecke mit dem ursprünglichen Zweck vereinbar sind. **AWS:** AWS hat keine Kontrolle über den Zweck, zu dem der Kunde die Daten nutzt und in der AWS-Cloud speichert. Sofern die Kundeninhalte personenbezogene Daten enthalten, verarbeitet AWS diese Daten nur, um gegenüber diesem Kunden die vom Kunden ausgewählten Services zu erbringen (mit Ausnahme der begrenzten Fälle, in denen dies erforderlich ist, um dem Gesetz oder wirksamen und bindenden Anordnung nachzukommen).

Datenschutzgrundsatz	**Zusammenfassung der datenschutzrechtlichen Verpflichtung**	**Erwägungen**
Rechte der Betroffenen	Betroffene müssen in der Lage sein, Zugriff auf ihre personenbezogenen Daten zu haben und die Berichtigung, Löschung oder Sperrung der personenbezogenen Daten zu erreichen, die anders als in Einklang mit der Richtlinie verarbeitet werden.	**Kunden:** Der Kunde behält die Kontrolle über die Inhalte, die er bei AWS speichert und kann daher darüber bestimmen, wie die Betroffenen auf ihre personenbezogenen Daten, die in den Inhalten enthalten sind, zugreifen können. Ebenso ist der Kunde am besten in der Lage, Anfragen oder Beschwerden eines Betroffenen hinsichtlich der Zulässigkeit der Datenverarbeitung durch den Kunden zu beantworten. **AWS**: Wie vorstehend dargelegt, hat AWS keine Kontrolle darüber, welche Art von Inhalten der Kunde bei AWS speichert und zu welchem Zweck dies geschieht. AWS hat keinen Einblick in diese Inhalte (einschließlich der Frage, ob diese Inhalte personenbezogene Daten enthalten). AWS kann die Betroffenen, deren personenbezogene Daten der Kunde in AWS gespeichert hat, nicht identifizieren und hat keinen Kontakt zu ihnen (mit Ausnahme der Fälle in denen die Daten sich auf den Kunden selbst beziehen). AWS kann daher den jeweiligen Betroffenen keine Informationen liefern. AWS ist nicht in der Lage, Daten, die auf AWS gespeichert sind, mit einer bestimmten Person in Verbindung zu bringen. Diese Information liegt ausschließlich in der Kontrolle des Kunden.
Richtigkeit	Die verantwortliche Stelle muss sicherstellen, dass die personenbezogenen Daten richtig sind, und – sofern erforderlich – sie auf dem aktuellen Stand halten.	**Kunden:** Der Kunde hat die Kontrolle über die personenbezogenen Daten, die er in AWS speichert. Er ist daher dafür verantwortlich, ihre Richtigkeit zu überprüfen und aufrecht zu erhalten (und kann sie gegebenenfalls aktualisieren und berichtigen). Darüber hinaus verantwortet der Kunde die Sicherheit ***in*** der Cloud, so dass der Kunde sicherstellen kann, dass er angemessene Maßnahmen zum Schutz der Daten vor Verfälschung implementiert hat. **AWS**: AWS hat keine Kontrolle darüber, welche Art von Inhalten der Kunde in AWS speichert. AWS hat keinen Einblick in die Inhalte. AWS gibt keine Daten im Auftrag des Kunden ein oder ändert sie in seinem Auftrag. AWS

Datenschutzgrundsatz	**Zusammenfassung der datenschutzrechtlichen Verpflichtung**	**Erwägungen**
		kann daher weder die Richtigkeit der Daten überprüfen noch die Daten ggf. aktualisieren. Der AWS SOC 1 Typ 2 Bericht enthält allerdings detaillierte Angaben über die Kontrollen, die AWS aufrechterhält, um die Integrität der Daten auf der zugrunde liegenden Cloud-Umgebung zu gewährleisten.
Datensicherheit	Die verantwortliche Stelle muss angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor zufälliger oder unberechtigter Zerstörung oder vor zufälligem Verlust, Veränderung, unberechtigter Offenlegung oder Zugriff treffen.	**Kunden:** Nur der Kunde ist in der Lage festzustellen, ob eine bestimmte Sicherheitsarchitektur, die er geplant oder implementiert hat, angemessen ist, um eine bestimmte Art von Inhalten einschließlich personenbezogener Daten zu schützen. Kunden sind für die Sicherheit ***in*** der Cloud verantwortlich, einschließlich der Sicherheit ihrer Inhalte (und der darin enthaltenen personenbezogenen Daten) und der Implementierung einer angemessenen Architektur bei der Nutzung der AWS-Service-Angebote. Insbesondere sind Kunden verantwortlich für die ordnungsgemäße (a) Konfiguration der AWS-Services, (b) Benutzung der Kontrollmechanismen, die im Zusammenhang mit den Services zur Verfügung stehen und (c) Ergreifung von Maßnahmen, die sie für notwendig erachten, um angemessene Sicherheitsvorkehrungen und Datensicherungen ihrer personenbezogenen Daten aufrecht zu erhalten (z.B. durch Nutzung von Verschlüsselungstechnologie, um personenbezogene Daten vor unberechtigtem Zugriff zu schützen, sowie regelmäßige Archivierung). **AWS:** AWS ist dafür verantwortlich, die Sicherheit ***der*** zugrunde liegenden Cloud-Umgebung herzustellen. Für eine vollständige Darstellung aller Sicherheitsmaßnahmen, die in die Cloud-Infrastruktur, Plattformen und Services von AWS integriert sind, lesen Sie bitte das Whitepaper 'Übersicht über die Sicherheitsprozesse'. AWS verwendet externe Auditoren, um die Wirksamkeit seiner Sicherheitsmaßnahmen, einschließlich der

Datenschutzgrundsatz	**Zusammenfassung der datenschutzrechtlichen Verpflichtung**	**Erwägungen**
		Sicherheit der physischen Rechenzentren, aus denen AWS seine Services erbringt, überprüfen zu lassen. Auf schriftliche Anfrage des Kunden und nach Unterzeichnung einer Vertraulichkeitsvereinbarung übersendet AWS dem Kunden eine Zusammenfassung des Prüfberichts, so dass der Kunde die AWS-Sicherheitsmaßnahmen angemessen überprüfen kann. AWS wird diese Zusammenfassung ebenfalls auf Anfrage an Datenschutzaufsichtsbehörden übermitteln.
Aufbewahrung der Daten	Personenbezogene Daten sollen (in identifizierbarer Form) nicht länger aufbewahrt werden, als dies für den Zweck, für den sie erhoben oder verarbeitet wurden, erforderlich ist.	**Kunden:** Es ist Sache des Kunden darüber zu entscheiden, für welche Zwecke die in der AWS-Cloud gespeicherten personenbezogenen Daten verwendet werden und wie lange eine Speicherung dieser Daten dementsprechend notwendig ist. Der Kunde kann die personenbezogenen Daten löschen oder anonymisieren, wenn sie nicht länger benötigt werden. **AWS:** AWS hat keinen Einblick, ob gespeicherte Daten personenbezogenen Daten beinhalten oder für welche Zwecke der Kunde die von ihm in der Cloud gespeicherten Daten verarbeitet. Entsprechend kann AWS nicht darüber entscheiden, für wie lange eine Datenspeicherung erforderlich ist, um diese Zwecke zu erreichen. Wenn ein Kunde Inhalte von den AWS-Services löscht, werden sie unlesbar oder unbrauchbar gemacht und die zu Grunde liegenden Speichereinheiten auf dem AWS-Netzwerk, die zur Speicherung der Inhalte verwendet wurden, werden in Einklang mit den AWS Standard Policies und Löschungsfristen gesäubert, bevor sie wieder vergeben und überschrieben werden. Die AWS-Prozesse sehen auch sichere Stilllegungsprozesse vor, die durchgeführt werden, bevor Speichermedien, die zur Erbringung der AWS-Services verwendet wurden, entsorgt werden. Als Teil dieses Prozesses werden Speichermedien entmagnetisiert oder gelöscht und physisch zerstört oder nach dem Stand der Technik unbrauchbar gemacht.

Übermittlung	Personenbezogene Daten sollen nicht in Länder oder Gebiete außerhalb des Europäischen Wirtschaftsraums ("EWR") übermittelt werden, es sei denn, dass in diesem Land oder Gebiet ein angemessenes Schutzniveau für die Rechte und Freiheiten der Betroffenen in Bezug auf die Verarbeitung der personenbezogenen Daten sichergestellt ist.	**Kunden:** Der Kunde kann die Region(en) wählen, in denen sich seine Inhalte und seine Server befinden. Der Kunde kann sich dazu entscheiden, seine AWS-Services exklusiv in den AWS-EU-Regionen in Deutschland oder Irland einzusetzen. **AWS:** AWS überträgt Kundeninhalte nicht außerhalb der vom Kunden ausgewählten Region(en), es sei denn, dies ist aufgrund Gesetzes oder einer gültigen und bindenden staatlichen Anordnung erforderlich. AWS bietet eine Auftragsdatenverarbeitungsvereinbarung, um Kunden zu helfen, ihre datenschutzrechtlichen Verpflichtungen zu erfüllen. AWS kann die Auftragsdatenverarbeitungsvereinbarung mit dem Kunden auch um die Standardvertragsklauseln ergänzen, wenn der Kunde diese benötigt um personenbezogene Daten aus der EU in ein Land außerhalb des Europäischen Wirtschaftsraums zu übermitteln. Am 6. März 2015 wurde die um die Standardvertragsklauseln ergänzte Auftragsdatenverarbeitungsvereinbarung von der als “Artikel-29-Datenschutzgruppe” bezeichneten Gruppe der nationalen Datenschutzbehörden der EU-Mitgliedstaaten genehmigt. Diese Genehmigung bedeutet, dass jeder AWS-Kunde, der die Standardvertragsklauseln benötigt, sich jetzt darauf verlassen kann, dass die AWS Auftragsdatenverarbeitungsvereinbarung ausreichende vertragliche Verpflichtungen enthält, um internationale Datenströme in Übereinstimmung mit der Richtlinie zu ermöglichen. Ausführliche Informationen zu der Genehmigung der Artikel-29-Datenschutzgruppe erhalten Sie auf folgender Seite der luxemburgischen Datenschutzbehörde: http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

Datenpannen

Da die Kunden bei der Nutzung von AWS die Verwaltung von und die Kontrolle über personenbezogene Daten behalten, bleiben die Kunden verantwortlich dafür, ihre eigene Umgebung auf Datenpannen hin zu überwachen und die Aufsichtsbehörden und die betroffenen Personen nach Maßgabe der anwendbaren Gesetze hierüber zu informieren. Nur der Kunde hat die Möglichkeit, dieser Verantwortung nachzukommen.

Kunden kontrollieren ihre eigenen Zugriffsschlüssel und bestimmen, wer berechtigt ist, auf ihren AWS-Account

zuzugreifen. Unter diesen Umständen hat AWS keinen Einblick in die Zugriffsschlüssel oder darin, wer und wer nicht berechtigt ist, sich in einen Account einzuloggen. Daher ist der Kunde dafür verantwortlich, die Nutzung, den Missbrauch, die Vergabe oder den Verlust von Zugriffsschlüsseln zu überwachen.

Falls nach anwendbarem Recht erforderlich, wird AWS den Kunden unverzüglich benachrichtigen, wenn AWS tatsächliche Kenntnis einer bestätigten Verletzung der AWS-Sicherheitsstandards in Bezug auf das AWS-Netzwerk hat.

Subunternehmer

AWS verwendet eine Reihe von externen Subunternehmern, die AWS bei der Erbringung der Services unterstützen. Allerdings haben unsere Subunternehmer keinen Zugriff auf Kundeninhalte. Darüber hinaus setzt AWS nur solche Subunternehmer ein, denen wir vertrauen, und wir setzen angemessene vertragliche Schutzmaßnahmen ein, die wir überwachen, um zu gewährleisten, dass die geforderten Standards aufrecht erhalten bleiben.

Externe Service-Anbieter des Kunden

Wie bereits oben in diesem Dokument angemerkt, ist die AWS-Umgebung auch mit anderen Services verbunden, die direkt durch Dritte erbracht werden (z.B. Internetdienstanbieter). Diese Dritten bleiben für ihr eigenes System verantwortlich, einschließlich der Sicherheit, und AWS ist nicht für die Aktivitäten dieser Dritten verantwortlich.

Weitere Erwägungen

Dieses Whitepaper berücksichtigt neben der Datenschutz-Richtlinie keine anderen Gesetze mit Datenschutzbezug (einschließlich branchenspezifischer Anforderungen), die für Kunden auch relevant sein könnten. Welche Datenschutz- und Datensicherheitsgesetze und Verordnungen auf den einzelnen Kunden anwendbar sind, hängt von verschiedenen Faktoren ab. Hierzu gehören insbesondere, wo der Kunde Geschäfte betreibt, in welcher Branche er tätig ist, die Art der Inhalte, die er speichern will, woher oder von wem der Inhalt kommt und wo der Inhalt gespeichert wird.

Kunden, die sich über ihre datenschutzrechtlichen Verpflichtungen Gedanken machen, sollten zunächst sicherstellen, dass sie die anwendbaren Anforderungen identifizieren und verstehen und angemessenen Rat suchen.

Schlussbemerkungen

Für AWS hat Sicherheit immer höchste Priorität. Wir erbringen Services für hunderttausende Betriebe, einschließlich Unternehmen, Bildungseinrichtungen und Regierungsorganisationen in über 190 Ländern. Unser Kundenstamm umfasst Finanzdienstleister und Dienstleister aus dem Gesundheitswesen und wir bekommen einige ihrer vertraulichsten Informationen anvertraut, einschließlich personenbezogener Gesundheitsdaten und Finanzberichte.

Die AWS-Services sind so gestaltet, dass sie den Kunden die Flexibilität geben, wie sie ihre Lösungen konfigurieren und einsetzen. Sie geben den Kunden die Kontrolle über ihre Inhalte, einschließlich der Frage wo er gespeichert wird, wie er gespeichert wird und wer Zugriff darauf hat. AWS-Kunden können ihre eigenen sicheren Applikationen erstellen und Inhalte sicher bei AWS speichern.

Weiterführende Hinweise

Um Kunden ein besseres Verständnis zu geben, wie sie ihre datenschutz- und datensicherheitsrechtlichen Anforderungen umsetzen können, ermutigen wir die Kunden, die auf der AWS-Webseite veröffentlichten Risiko-, Compliance- und Sicherheits-Whitepapers, Best Practices, Checklisten und Leitfäden zu lesen. Diese Unterlagen finden sie unter http://aws.amazon.com/de/compliance und http://aws.amazon.com/de/security.

AWS bietet auch Schulungen an, die Kunden dabei helfen zu lernen, wie verfügbare, effiziente und sichere Anwendungen in der AWS-Cloud entworfen, entwickelt und betrieben werden und ihre Kenntnisse über die Services und Lösungen von AWS zu vertiefen. Wir bieten kostenlose Schulungsvideos, Übungen im Selbststudium, und von Dozenten geleitete Schulungen. Weitere Informationen zu den AWS-Trainings sind verfügbar unter http://aws.amazon.com/de/training/.

AWS-Zertifikate bescheinigen die technischen Fähigkeiten und das Wissen über Best Practices, um sichere und zuverlässige Cloud-basierte Anwendungen unter Verwendung von AWS-Technologie zu schaffen. Weitere Formationen zum AWS-Zertifizierungsprogramm sind verfügbar unter http://aws.amazon.com/de/certification/.

Sollten Sie weitere Informationen benötigen, kontaktieren Sie bitte AWS unter https://aws.amazon.com/de/contact-us/ oder kontaktieren Sie Ihren lokalen AWS Account-Verantwortlichen.