Whitepaper zum Datenschutz in Deutschland

Februar 2017

Hinweise

Dieses Dokument dient ausschließlich Informationszwecken und bezieht sich auf das aktuelle Produktangebot und die aktuellen Praktiken von AWS zum Zeitpunkt der Erstellung dieses Dokuments. Änderungen ohne vorherige Mitteilung sind vorbehalten. Kunden sind verantwortlich für ihre eigene Bewertung und Auslegung der in diesem Dokument zur Verfügung gestellten Informationen und für die Nutzung der AWS-Produkte oder Services. Diese Informationen werden alle ohne Gewährleistung und ohne jegliche Garantie, weder ausdrücklich noch stillschweigend, bereitgestellt. Dieses Dokument ist weder eine Garantie noch Gewährleistung und enthält keine vertraglichen Verpflichtungen, Bedingungen oder Zusicherungen von AWS, ihren Tochterunternehmen, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder Teil einer solchen Vereinbarung von AWS mit seinen Kunden noch ändert es solche Vereinbarungen.

Inhalt

Übersicht

In diesem Dokument wird erklärt, wie Kunden die AWS-Services unter Einhaltung des deutschen Datenschutzgesetzes, dem Bundesdatenschutzgesetz (BDSG), nutzen können und die Kontrolle über ihre Inhalte im Allgemeinen und personenbezogene Daten im Besonderen beibehalten können.

Einführung

Dieses Whitepaper behandelt die folgenden Themen:

- Funktionsweise von AWS-Services;
- Wie Kunden bei der Nutzung von AWS das BDSG einhalten, ihre eigenen Sicherheitsanforderungen erfüllen, ihre Inhalte verschlüsseln sowie auf andere Weise schützen können;
- Die Auswirkungen des BDSG auf AWS-Services im Hinblick auf Kundenkontrollen und die damit verbundenen technischen und organisatorischen Maßnahmen;
- Relevante Überlegungen zur Compliance, einschließlich der Frage, wie Kunden festlegen können, an welchen geographischen Standorten Inhalte gespeichert und abgerufen werden können;
- Die jeweiligen Rollen von Kunden und AWS hinsichtlich der Verwaltung und des Schutzes der mit AWS-Services verarbeiteten Inhalte.

Dieses Informationsdokument beantwortet Fragen, die regelmäßig von AWS-Kunden hinsichtlich der Auswirkungen der Anforderungen des BDSG gestellt werden. Die Kunden sind dafür verantwortlich, darüber hinaus weitere relevante Aspekte anzusprechen, z. B. hinsichtlich der Einhaltung branchenspezifischer Anforderungen oder „Best Practices“.

Dieses Dokument dient nur zur Information. Es stellt keine Rechtsberatung dar und dient Kunden auch nicht als Ersatz einer Rechtsberatung. Da die Anforderungen jedes Kunden unterschiedlich sind, empfiehlt AWS seinen Kunden, geeignete Beratung zur Umsetzung ihrer Datenschutz- und Datensicherungsanforderungen einzuholen. Das gilt auch allgemein bezüglich der für ihr Unternehmen geltenden Gesetze einzuholen. Kunden verwenden AWS-Services, um eine große Bandbreite von „Kundeninhalten” zu verarbeiten, darunter alle Arten von Daten, Text, Audio, Video und Software. AWS wendet im Umgang mit allen Kundeninhalten (unabhängig davon, ob sie personenbezogene Daten enthalten oder nicht) den entsprechend hohen Standard an, der für personenbezogene Daten angemessen ist. Aus diesem Grund wird in diesem Whitepaper allgemein von Kundeninhalten und Inhalten gesprochen. Alle Verweise in diesem Dokument auf Kundeninhalte umfassen personenbezogene Daten (als möglicher Teil von Kundeninhalten).

Aufgrund der direkten Anwendbarkeit der EU-Datenschutz-Grundverordnung wird das BDSG wahrscheinlich geändert oder durch ein allgemeines Datenschutzgesetz ersetzt. Wir verfolgen derartige Entwicklungen und werden weiterhin geltende Gesetze einhalten.

Bundesdatenschutzgesetz

Datenverarbeitung im Rahmen des BDSG

Das BDSG regelt die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. „Verarbeitung" ist jeder Vorgang, der an personenbezogenen Daten vorgenommen wird (d. h. Speicherung, Veränderung, Sperrung, Löschung und Übermittlung dieser Daten). Verarbeitung in diesem Dokument bezieht sich auf alle Phasen der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Personenbezogene Daten sind Informationen, die die persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person („Betroffener") beschreiben. Darüber hinaus unterscheidet das BDSG zwischen verantwortlichen Stellen oder Auftraggebern und Auftragnehmern:

- **Verantwortliche Stelle oder Auftraggeber** – die Partei, die personenbezogene Daten erhebt, verarbeitet oder nutzt oder die andere Stellen damit beauftragt
- **Auftragnehmer (Auftragsdatenverarbeiter)** – eine Partei, die personenbezogene Daten im Auftrag des Auftraggebers verarbeitet

Der Auftraggeber ist dafür verantwortlich, sicherzustellen, dass personenbezogene Daten unter Einhaltung der Datenschutzgesetze verarbeitet werden. Dazu gehört die Überprüfung, dass die personenbezogenen Daten rechtmäßig und nach Treu und Glauben verarbeitet werden. Darüber hinaus müssen die Daten vor unbefugter oder unrechtmäßiger Verarbeitung geschützt werden.

AWS als Auftragsdatenverarbeiter für die personenbezogenen Daten der Kunden

AWS-Services werden in vielen unterschiedlichen Zusammenhängen für unterschiedliche Geschäftszwecke genutzt. Häufig sind mehr Parteien als nur AWS und der Kunde am Verarbeitungszyklus von personenbezogenen Daten beteiligt. In den mit AWS-Services verarbeiteten Inhalten oder in Rechenergebnissen, die Kunden oder deren Benutzer durch die Nutzung der AWS-Services erhalten, können Inhalte weiterer Dritte enthalten sein. Hierbei kann es sich beispielsweise um die Kunden des Kunden oder dessen Tochterunternehmen handeln. In diesem Whitepaper wird allgemein der Begriff „Kundeninhalte" verwendet. Als Grundregel gilt in Fällen, in denen personenbezogene Daten mit den AWS-Services verarbeitet werden, Folgendes:

- Der Kunde ist in Bezug auf diese personenbezogenen Daten die verantwortliche Stelle, wenn er den Zweck bestimmt, zu dem die personenbezogenen Daten verarbeitet werden und die Methode festgelegt hat, wie sie verarbeitet werden. In diesem Szenario ist AWS der Auftragnehmer.

- Der Kunde ist in Bezug auf diese personenbezogenen Daten ein Auftragnehmer, wenn er die personenbezogenen Daten lediglich im AWS-Netzwerk im Auftrag und gemäß den Weisungen eines Dritten verarbeitet (wobei der Dritte verantwortliche Stelle, ein anderer Drittanbieter in der Lieferkette oder eine natürliche Person mit rein inländischer Funktion sein kann). In diesem Fall ist AWS Unterauftragnehmer.

Die Artikel-29-Datenschutzgruppe hat außerdem Richtlinien zum Cloud Computing veröffentlicht und bestätigt, dass der Cloud-Anbieter (d. h. AWS) im Allgemeinen der Auftragnehmer ist.

Die Anwendbarkeit dieser Konzepte spielt eine entscheidende Rolle, da sie die Verantwortlichkeit für die Einhaltung der Datenschutzregeln bestimmen. Als Anbieter von „Infrastructure as a Service"-Diensten bietet AWS verschiedene Servicefunktionen und Maßnahmen an, die Kunden eigenständig (als Self-Service) nutzen können. AWS-Kunden können festlegen, welche Daten sie wo mit AWS „verarbeiten" möchten und wie sie diese Daten schützen. Insbesondere können AWS-Kunden Verschlüsselung zum Schutz ihrer Inhalte nutzen, indem sie diese Daten „unlesbar" machen. AWS nimmt keine Einsicht in Kundeninhalte im AWS-Netzwerk und hat auch keine Kenntnis über die Bestandteile der Kundeninhalte. AWS hat insbesondere keine Kenntnis darüber, ob die Kundeninhalte personenbezogene Daten enthalten.

Auftragsdatenverarbeitungsvereinbarungen und EU-Standardverträge

Für Kunden, die personenbezogene Daten mit AWS-Services verarbeiten, stellt AWS eine Auftragsdatenverarbeitungsvereinbarung als Anhang zu dem Kundenvertrag (Data Processing Addendum) zur Verfügung, um die Kunden bei der Erfüllung ihrer datenschutzrechtlichen Verpflichtungen zu unterstützen. Wenn der Kunde beabsichtigt personenbezogene Daten von der EU in ein Land außerhalb des Europäischen Wirtschaftsraums zu übermitteln, bietet AWS die EU-Standardvertragsklauseln als Anlage zur Auftragsdatenverarbeitungsvereinbarung an. Kunden können auf die Wirksamkeit der Auftragsdatenverarbeitungsvereinbarung inklusive der Standardvertragsklauseln vertrauen, da die als Artikel-29-Datenschutzgruppe bekannte Gruppe von EU-Datenschutzbehörden, am 6. März 2015 die Verwendung der Auftragsdatenverarbeitungsvereinbarung inklusive der Standardvertragsklauseln genehmigthat. Weitere Informationen zur Genehmigung durch die Artikel-29-Datenschutzgruppe finden Sie auf der Website der Luxemburger Datenschutzaufsicht (CNPD) unter:

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

Zugriff auf Kundeninhalte

AWS verarbeitet Kundeninhalte nur in dem Umfang, wie im Rahmen der Bereitstellung der vom Kunden gewählten AWS-Services an den Kunden und dessen Endnutzer erforderlich. AWS nutzt keine Kundeninhalte für eigene Zwecke, einschließlich Marketing oder Werbung.

AWS bietet den Kunden bei der Nutzung von AWS-Services verschiedene Möglichkeiten zur Verschlüsselung ihrer Inhalte an, einschließlich der AWS-Verschlüsselungsfunktionen, der Verwaltung ihrer eigenen Verschlüsselungsschlüssel oder der Verwendung von Verschlüsselungsmechanismen von Drittanbietern ihrer Wahl.

AWS weiß grundsätzlich nicht, ob die Kundeninhalte personenbezogene Daten enthalten. Wie bereits oben erwähnt, wendet AWS hinsichtlich aller Kundeninhalte (unabhängig davon, ob personenbezogene Daten enthalten sind oder nicht) den entsprechend hohen Standard an, der für personenbezogene Daten angemessen ist. Auf diese Weise profitieren alle Kundeninhalte von denselben robusten Sicherheitsmaßnahmen, die zum Schutz personenbezogener Daten ergriffen werden. AWS stellt lediglich die vom Kunden gewählten Datenverarbeitungs-, Speicher-, Datenbank- und Netzwerkservices mit erstklassigen Sicherheitsmaßnahmen zur Verfügung, die auf der von AWS bereitgestellten Cloud-Infrastruktur eingesetzt werden. Kunden können zusätzlich auf dieser Infrastruktur entsprechende Sicherheitsmaßnahmen aufbauen, die aufgrund seiner individuellen Anforderungen erforderlich sind.

Staatliche/behördliche Zugriffsrechte

Kunden fragen häufig, ob und in welchem Umfang inländische oder ausländische Regierungsbehörden auf die in Cloud-Services gespeicherten Inhalte zugreifen können. Das Thema Datenhoheit führt bei Kunden oft zur Besorgnis. Kunden wissen nicht, ob beziehungsweise unter welchen Voraussetzungen Regierungen auf ihre Inhalte zugreifen können. Die geltenden Gesetze in der Jurisdiktion, in der sich die Inhalte befinden, sind für solche Zugriffsrechte wichtig. Die Kunden müssen allerdings auch in Betracht ziehen, ob für sie Gesetze anderer Jurisdiktion gelten können, je nachdem, wo sie – oder ihre Kunden – geschäftlich tätig sind. Kunden sollten sich rechtlich beraten lassen, um die Anwendbarkeit von relevanten Gesetzen auf ihr Unternehmen und ihre Geschäftstätigkeit zu prüfen.

Wenn es um Bedenken oder Fragen zu den Zugriffsrechten inländischer oder ausländischer Regierungen auf die in der Cloud gespeicherten Inhalte geht, müssen Kunden Folgendes in Betracht ziehen: Staatliche Stellen können durch die auf den Kunden anwendbaren Gesetze ermächtigt sein, Zugriff auf Inhalte zu verlangen. Beispiel: Ein in Land X geschäftlich tätiges Unternehmen, könnte eine behördliche Anfrage hinsichtlich Zugangs von Inhalten erhalten,

auch wenn die Inhalte in Land Y gespeichert sind. In der Regel fordert eine staatliche Stelle direkt die Gesellschaft zur Herausgabe von Information auf und nicht den Cloud-Anbieter.

Grundsätzlich haben die EU-Mitgliedstaaten Gesetze, die es Strafverfolgungs- und nationalen Sicherheitsbehörden ermöglichen, Zugriff auf Informationen zu verlangen. Auch ausländische Strafverfolgungsbehörden können mit lokalen Strafverfolgungsbehörden und nationalen Sicherheitsbehörden zusammenarbeiten, um Zugriff auf Informationen in der EU zu erlangen. Die meisten Länder verfügen über Verfahren (einschließlich bilateraler Rechtshilfeübereinkommen), die die Übermittlung von Informationen in andere Länder im Rahmen einer gesetzlichen Anfrage (z. B. im Zusammenhang mit Verbrechen) zulassen. Eine Übermittlung ist aber nur unter bestimmten Voraussetzungen zulässig, je nach anwendbarem Recht. Beispielsweise muss eine staatliche Stelle, die Zugriff auf Informationen erhalten möchte, regelmäßig ein berechtigtes Interesse für den Zugriff vorweisen. Möglicherweise ist auch ein Gerichtsbeschluss oder Durchsuchungsbefehl erforderlich.

AWS-Richtlinie hinsichtlich staatlichen Zugriffs

AWS ist stets darauf bedacht, Kundeninhalte zu schützen. Diese Auffassung gilt unabhängig davon, woher eine Anfrage für Kundeninhalte kommt oder wer der Kunde ist. AWS legt keine Kundeninhalte offen, sofern dies nicht durch eine gültige und rechtlich bindende Anordnung verlangt wird, beispielsweise eine Auskunftsanordnung („Subpoena“) oder einen Gerichtsbeschluss. Staatliche Stellen außerhalb der USA müssen in der Regel international anerkannte Verfahren, wie bilaterale Rechtshilfeübereinkommen mit der US-Regierung, einhalten, um solche gültigen oder bindenden Anordnungen zu erhalten. AWS prüft jede Anforderung sorgfältig, um ihre Richtigkeit zu authentifizieren und zu bestätigen, dass sie die anwendbaren Gesetze einhält. AWS geht gegen unzureichende Anordnungen vor, insbesondere wenn die Anordnung zu allgemein ist, die Befugnis des Anfragenden überschreitet oder nicht vollständig von geltendem Recht abgedeckt ist. Beispiel: AWS geht gegen Anordnungen vor, wenn die relevanten Daten nicht in der Jurisdiktion gespeichert sind, aus der die anfordernde Behörde stammt. Aufgrund eines neuen Gerichtsurteils sind diese Vorgehen äußerst erfolgversprechend. AWS versucht außerdem, die anfordernde Behörde direkt an den Kunden zu verweisen und kann dabei die Grundkontaktinformationen des Kunden zur Verfügung stellen. Wenn AWS verpflichtet ist, Kundeninhalte offenzulegen, benachrichtigt AWS seine Kunden vor der Herausgabe ihrer Inhalte, um dem Kunden die Möglichkeit zu geben, gegen die Herausgabe vorzugehen, es sei denn es wurde AWS verboten oder wenn es klare Anzeichen für ein illegales Verhalten in Verbindung mit der Nutzung der AWS-Services gibt. Weitere Informationen finden Sie in unserem aktuellen Transparenzbericht und unseren Amazon Strafverfolgungsrichtlinien.

AWS-Regionen: Wo werden die Inhalte gespeichert?

Die AWS-Datenzentren sind weltweit verschiedenen Ländern in Clustern in aufgesetzt. Wir bezeichnen ein Cluster von Rechenzentren in einem bestimmten Land als „Region“. Kunden haben weltweit Zugang zu 16 AWS-Regionen, darunter drei Regionen in der EU: Irland (Dublin), Deutschland (Frankfurt) und Großbritannien (London). Im kommenden Jahr gehen außerdem weitere Regionen online. Kunden können eine Region, alle Regionen oder eine Kombination aus beliebigen Regionen auswählen. Die Wahl, die der Kunde trifft, ist für AWS bindend. In Abbildung 1 sind die AWS-Regionen dargestellt.

Abbildung 1: AWS-Regionen und Availability Zones

Kunden wählen die AWS-Region(en) aus, in der (denen) ihre Inhalte gehostet werden. So können Kunden mit bestimmten geografischen Anforderungen Umgebungen am gewünschten Standort (oder an mehreren Standorten) einrichten. Kunden in Europa können beispielsweise festlegen, dass ihre AWS-Dienste nur in der EU-Region Frankfurt bereitgestellt werden. Wenn der Kunde diese Region auswählt, kann er einen bestimmten Speicherort seiner Inhalte in Deutschland nennen. Ohne die Auswahl einer weiteren AWS-Region werden die Kundeninhalte nicht auf Servern einer anderen AWS-Region gespiegelt.

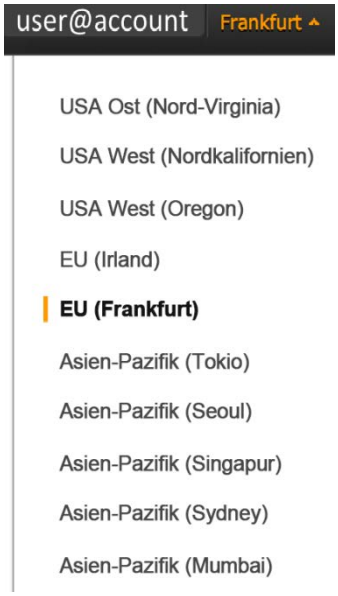
Die Kunden können Inhalte kopieren und in mehreren Regionen sichern. AWS verschiebt oder kopiert Kundendaten nicht ohne entsprechende Anweisungen des Kunden. Kunden haben

immer die Kontrolle darüber, in welcher Region beziehungsweise in welchen Regionen ihre Inhalte gespeichert und verarbeitet werden. AWS speichert und verarbeitet jede Instanz der Inhalte seiner Kunden nur in diesen Regionen. Kundeninhalte werden nicht in andere als die vom Kunden ausgewählte(n) Region(en) verschoben, außer dies ist gesetzlich erforderlich.

Auswählen der Regionen

Der Kunde legt bestimmte AWS-Regionen, in denen die AWS-Dienste verwendet werden sollen, über die Management Console oder durch eine Anforderung über eine AWS-Anwendungsprogrammierschnittstelle (API) fest. Abbildung 2: Auswählen globaler AWS-Regionen zeigt das Auswahlmenü, das Kunden sehen, wenn sie Inhalte auf einen AWS-Speicherdienst hochladen oder Ressourcen für die Datenverarbeitung über die AWS Management Console bereitstellen.

Abbildung 2 – Auswählen globaler AWS-Regionen in der AWS Management Console



Kunden können die Amazon Virtual Private Cloud (VPC) nutzen, um die AWS-Region vorzugeben, in der die Daten verarbeitet werden sollen. Amazon VPC ermöglicht Kunden die Bereitstellung eines logisch abgegrenzten Bereichs der AWS-Cloud, in dem sie AWS-Ressourcen in einem von ihnen selbst definierten virtuellen Netzwerk ausführen. Mit der Amazon VPC können Kunden eine virtuelle Netzwerktopologie definieren, sehr ähnlich zu einem herkömmlichen Netzwerk, das in ihrem eigenen Rechenzentrum betrieben werden könnte.

Alle Ressourcen zur Datenverarbeitung und andere Ressourcen, die der Kunde in der VPC startet, befinden sich in der vom Kunden festgelegten Region.

Sicherheit von Kundeninhalten

AWS ist für die Verwaltung der Sicherheit der zugrunde liegenden Cloud-Umgebung verantwortlich. Dies wird als „Sicherheit der Cloud“ bezeichnet. Die AWS Cloud-Infrastruktur ist eine der sichersten Cloud Computing-Umgebungen, die es gibt.

AWS behandelt die Sicherheit der Kunden mit größter Sorgfalt. Wir haben leistungsstarke technische und physische Maßnahmen zum Schutz unserer Cloud Computing-Umgebung umgesetzt. Eine ausführliche Liste aller Sicherheitsmaßnahmen, die in unserer grundlegenden AWS Cloud-Infrastruktur, den Plattformen und Services integriert sind, finden Sie in folgenden Whitepaper-Dokumenten:

- Amazon Web Services: "Überblick über Sicherheitsprozesse"
- AWS – Risiko und Compliance

Ausführliche Informationen finden Sie außerdem weiter unten im Abschnitt Technische und organisatorische Maßnahmen.

Das robuste Sicherheitsvorfallmanagement von AWS

Ein wichtiger Bestandteil der Sicherheitsmaßnahmen von AWS ist die Erkennung und Abhilfe von Sicherheitsrisiken. AWS Mitarbeiter sind rund um die Uhr, sieben Tage die Woche und an 365 Tagen im Jahr im Einsatz, um Störungen und andere Vorfälle zu erkennen und zu lösen sowie die Auswirkungen zu begrenzen.

AWS bestimmt, verwaltet und überwacht die Sicherheit für die zugrunde liegende Cloud-Infrastruktur (d. h. die Hardware, die Einrichtungen, in der die Hardware untergebracht sind, und die Netzwerkinfrastruktur). AWS scannt beispielsweise regelmäßig alle mit dem Internet verbundenen IP-Adressen von Service-Endpunkten auf Schwachstellen (die Instanzen der Kunden werden nicht gescannt). Wird eine Schwachstelle erkannt, behebt AWS auf Basis von branchenüblichen Methoden und „Best Practices“ unternehmenskritische Schwachstellen.

AWS betreibt die Infrastruktur und setzt die dafür geltenden Sicherheitsmaßnahmen um. AWS führt daher folgende Maßnahmen durch:

- AWS identifiziert potenzielle Störungen und andere Vorfälle in der Infrastruktur.
- AWS prüft, ob aufgrund der Störung oder anderen Vorfalls auf Kundeninhalte zugegriffen wurde.
- AWS prüft, ob dieser Zugriff tatsächlich rechtswidrig oder unbefugt war, beispielsweise, ob er gegen die Sicherheitsrichtlinien von AWS verstößt.

AWS informiert den Kunden, wenn AWS Kenntnis von entweder (a) einem rechtswidrigen Zugriff auf Kundendaten, die bei AWS (auf AWS Equipment oder in AWS Einrichtungen)

gespeichert sind, oder auf (b) einen unbefugten Zugriff auf dieses Equipment oder diese Einrichtungen erhält, und in jeden Fall wenn der Zugriff zu Verlust, Offenlegung oder Änderung von Kundeninhalten führt(jeweils ein („Sicherheitsvorfall“). AWS informiert die Kunden unabhängig davon, ob es sich bei den Kundeninhalten um personenbezogene Daten handelt und ob die Daten sensibel sind.

Der Sicherheitsvorfallmanagementplan von AWS ist nach ISO 27001, 27017, 27018 und 9001 umgesetzt und zertifiziert und wird im Rahmen der AWS Service Organization Control (SOC) 1, 2 und 3 Auditierung ausführlich geprüft. Alle Verfahren und Richtlinien wie ISO27001, ISO27018 und SOC 3 sind unter https://aws.amazon.com/de/compliance/ abrufbar.

Kunden können potenzielle Schwachstellen ebenfalls an AWS melden. Auf der Seite Berichte zu Schwachstellen wird beschrieben, wie AWS gemeldete Schwachstelle behandelt.

Geteilte Verantwortlichkeit („Shared Responsibility“) bei der Verwaltung der Cloud-Sicherheit

Das Auslagern der IT-Infrastruktur in eine von AWS betriebene cloudbasierte Infrastruktur führt zu dem Modell der geteilten Verantwortlichkeit („Shared Responsibility“-Model) zwischen dem Kunden und AWS, da sowohl der Kunde als auch AWS wichtige Rollen für den Einsatz, die Umsetzung und die Verwaltung von Sicherheitsmaßnahmen in ihren Verantwortungsbereichen einnehmen. Alle sicherheitsrelevanten Bestandteile, vom Host-Betriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Anlagen, von denen die AWS-Services erbracht werden, werden von AWS umgesetzt, verwaltet und kontrolliert. Der Kunde ist verantwortlich für die Verwaltung des Betriebssystems eines Drittanbieters (einschließlich Updates und Sicherheitspatches) und damit verbundene Anwendungssoftware. Der Kunde ist auch verantwortlich für die Konfiguration der von AWS bereitgestellten Firewall der relevanten Sicherheitsgruppe und für andere sicherheitsrelevante Funktionen. Der Kunde stellt über von Drittanbietern bereitgestellte Dienste (z. B. Internetdienstanbieter) eine Verbindung zur AWS-Umgebung her. Da AWS diese Verbindung nicht bereitstellt, ist der Kunde für die Sicherheit der Verbindung verantwortlich. AWS steuert und bestimmt nicht die Datenverarbeitung für die Kunden. Kunden sollten diese Aspekte und die Verantwortlichkeit von Drittanbietern in der Bewertung ihrer Systeme und Systemsicherheit berücksichtigen. Diese Verteilung der Verantwortlichkeit unterscheidet sich nicht von der Zusammenarbeit mit einem Netzwerkdienstanbieter, der die Verbindungen zu Rechenzentren vor Ort beim Kunden bereitstellt. Die jeweiligen Rollen von Kunden und AWS im Modell übergreifender Verantwortlichkeit sind in Abbildung 3 dargestellt.

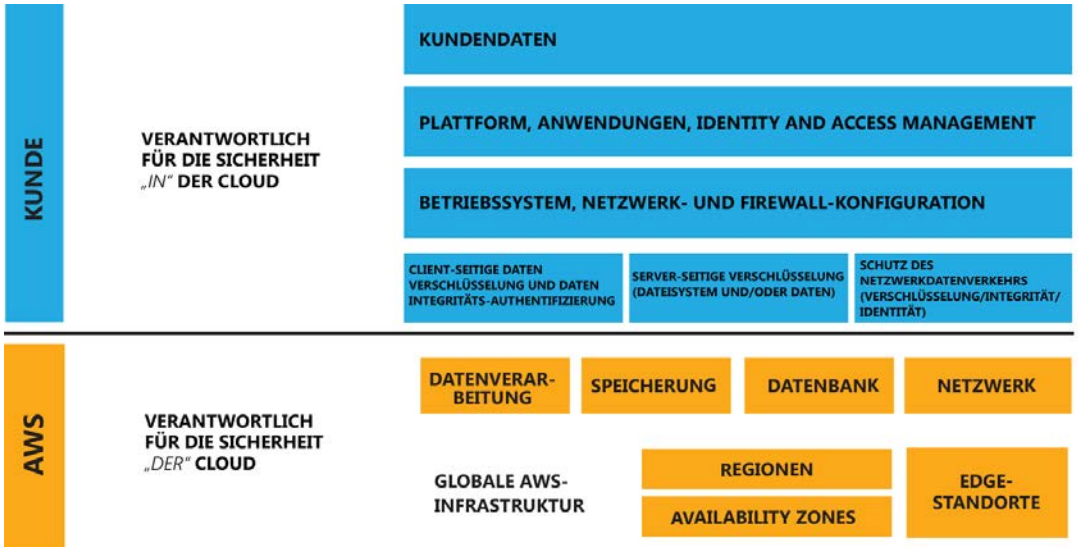


Abbildung 3 – Sicherheitsmodell

Das „Shared-Responsibility"-Modell und Kundeninhalte

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

- Sicherheitsmaßnahmen, die der Cloud-Dienstanbieter (AWS) umsetzt und verwaltet d.h. Maßnahmen, die die Sicherheit der physischen Infrastruktur wie Verfügbarkeit und Integrität betreffen (Sicherheit *„der"* Cloud); und
- Sicherheitsmaßnahmen, die der Kunde umsetzt und verwaltet, d.h. Maßnahmen, die die Sicherheit der Kundeninhalte und -anwendungen betreffen, die von AWS-Dienste nutzen („Sicherheit *in* der Cloud").

Während AWS für die Sicherheit *der* Cloud selbst zuständig ist, liegt die Verantwortung für die Sicherheit *in* der Cloud beim Kunden. Kunden können selbst für ausreichende Sicherheitsmaßnahmen zum Schutz ihrer eigenen Netzwerke, Systeme, Plattformen, Anwendungen und Inhalte (von der Betriebssystemebene des Servers bis zur Anwendungsebene) sorgen, wie dies auch in einem eigenen Rechenzentrum vor Ort beim Kunden der Fall wäre. Im Rahmen seiner verschiedenen Serviceangebote stellt AWS für seine Kunden eine Auswahl an Sicherheitsmaßnahmen bereit. Kunden können außerdem auch eine Vielzahl von Sicherheitslösungen von Drittanbietern nutzen. AWS-Kunden haben im Rahmen der Konzipierung der Sicherheitsarchitektur, die ihren Compliance-Anforderungen und ihren internen und externen gesetzlichen bzw. regulatorischen Anforderungen entspricht,

umfassende Gestaltungsfreiheit. Dies ist ein Hauptunterschied zu herkömmlichen Hosting-Lösungen, in denen der Anbieter generell die Entscheidungen über die Architektur trifft. AWS überlässt dem Kunden die Entscheidung, ob Sicherheitsmaßnahmen umgesetzt werden sollen. Werden Sicherheitsmaßnahmen umgesetzt, entscheidet der Kunde, welche Sicherheitsmaßnahmen in der Cloud umgesetzt werden und ob diese für das Unternehmen angemessen und ausreichend sind. Wenn beispielsweise eine Architektur mit hoher Verfügbarkeit zum Schutz der Daten erforderlich ist, kann der Kunde redundante Systeme, Sicherungen, Standorte, Netzwerk-Uplinks usw. nutzen, um eine stabilere, hoch verfügbare Architektur zu erstellen. Wenn der Zugriff auf die Daten eingeschränkt werden soll, ermöglichen die von AWS bereitgestellten Maßnahmen dem Kunden die Implementierung von Zugriffsberechtigungen – sowohl auf Systemebene als auch über die Verschlüsselung auf Datenebene. AWS bietet dem Kunden somit die direkte Einwirkungs- und Entscheidungsmöglichkeit hinsichtlich vieler Elemente der technischen und organisatorischen Maßnahmen für die Datensicherheit.

Wir achten sehr auf die Sicherheit der Cloud-Umgebung und haben leistungsstarke technische und organisatorische Maßnahmen zum Schutz vor nicht autorisiertem Zugriff eingerichtet. Wie bereits erwähnt, können Kunden die in der AWS-Umgebung vorhandenen Sicherheitsmaßnahmen durch die von AWS gehaltenen Zertifizierungen und entsprechende Berichte nachvollziehen und überprüfen. Diese Berichte umfassen die Berichte der AWS Service Organization Control (SOC) 1, 2 und 3 und der ISO 27001-, 27017- und 27018-Zertifizierungen und PCI-DSS-Compliance-Berichte. Diese Berichte und Zertifizierungen werden von unabhängigen Auditoren erstellt und bestätigen die Wirksamkeit des Konzepts und Betriebs der AWS-Sicherheitsumgebungen. Die SOC-Berichte werden zweimal im Jahr veröffentlicht und decken die Sechs-Monats-Zeiträume vom 1. Oktober bis zum 31. März und vom 1. April bis zum 30. September des jeweiligen Jahres ab. ISO 27001, 27017 und 27018 sind jährliche Zertifizierungen. Die PCI-DSS-Compliance-Berichte werden ebenfalls einmal im Jahr herausgegeben.

Kundenkontrollen (technische und organisatorische Maßnahmen) – § 9 BDSG und Anlage zu § 9 BDSG

Der Auftraggeber ist verantwortlich, angemessene technische und organisatorische Maßnahmen (i) zum Schutz der personenbezogenen Daten vor versehentlicher oder unrechtmäßiger Zerstörung oder versehentlichem Verlust, Veränderung, unbefugter Weitergabe oder unbefugtem Zugriff sowie (ii) Gewährleistung der Verfügbarkeit umzusetzen. Wenn ein Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, ist der Auftraggeber auch dafür verantwortlich einen Auftragnehmer auszuwählen, der angemessene technische und organisatorische Maßnahmen bereitstellt.

In den folgenden Abschnitten sind einige der wichtigsten Datenschutzprinzipien zusammengefasst, die die Kunden im Allgemeinen in diesem Zusammenhang berücksichtigen müssen. Im Folgenden sind auch Informationen bereitgestellt, die Ihnen dabei helfen, AWS als Ihren Auftragnehmer unter Einhaltung des BDSG auszuwählen. Der Einfachheit halber werden die Bestimmungen im Anhang zu § 9 BDSG in der gleichen Reihenfolge genannt, wie sie im BDSG angegeben sind. Wir behandeln auch in diesem Zusammenhang relevante Aspekte der AWS-Services. In der folgenden Zusammenfassung gehen wir davon aus, dass der Kunde der Auftraggeber ist. Wie oben erwähnt, ist uns jedoch bewusst, dass es viele verschiedene Umstände geben kann, unter denen der Kunde selbst als Auftragnehmer auftritt.

Kontrolle der Kunden über Kunden-Inhalte

Kunden behalten die Kontrolle über ihre Inhalte innerhalb der AWS-Umgebung. AWS ermöglicht Kunden das Folgende:

- Festzulegung, wo sich die Inhalte befinden, zum Beispiel, Festlegung der auf AWS verwendeten Speicherart und des geografischen Standortes (in Europa, nach Ländern), an dem die Speicherung und Verarbeitung erfolgen soll. Gleichzeitig wird hierdurch die Nutzung von anderen Regionen ausgeschlossen.

- Kontrolle über das Format, die Struktur und die Sicherheit der Kundeninhalte, einschließlich der Entscheidung bezüglich des Verfremdens, Anonymisierens oder der Verschlüsselung von Daten. AWS bietet Kunden die Möglichkeit die Inhalte mit einer starken Verschlüsselung zu schützen. Die Verschlüsselung gilt auch für Inhalte während der Übertragung und der Speicherung. Kunden können außerdem ihre Schlüssel selbst verwalten oder Verschlüsselungsmechanismen von Drittanbietern ihrer Wahl verwenden.

- Verwaltung weiterer Zugriffskontrollen, wie Identitätskontrolle, Zugriffsverwaltung, Berechtigungen und Sicherheitsanmeldeinformationen.

- Kontrolle der Netzwerkeinrichtung und -struktur, einschließlich Netzwerksicherheitsmaßnahmen, um unbefugten Zugriff zu verhindern und Zugriffe auf personenbezogene Daten sowie Veränderungen von personenbezogenen Daten nachvollziehen zu können.

Auf diese Weise können AWS-Kunden den gesamten Lebenszyklus ihrer Inhalte auf AWS steuern und die Inhalte ihren speziellen Bedürfnissen entsprechend verwalten. Hierzu gehört die Einteilung des Inhalts in Klassen, Zugriffskontrolle, Speicherung und Löschung.

Anlage zu § 9 BDSG

1. Zutrittskontrolle (unbefugter Zutritt zu Rechenzentren)

Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)

AWS

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, die die AWS Einrichtungen vor unbefugtem physischem Zutritt schützen. Derzeit umfassen diese Maßnahmen unter anderem:

- Die AWS Rechenzentren, Server, Netzwerkausstattung und Hostsoftwaresysteme (physische Bestandteile des AWS Netzwerks) sind in unscheinbaren Gebäuden untergebracht.
- Die AWS Gebäude sind durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt sowohl weiträumig (z. B. Zaun, Wände) als auch in den Gebäuden selbst zu verhindern.
- Der Zutritt zu Serverstandorten wird elektronische Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird.
- Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde.
- Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet.
- Zutritt zu sensiblen Bereichen wird durch Videoüberwachung überwacht.
- Ausgebildete Sicherheitskräfte bewachen die AWS-Rechenzentren und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.

2. Zugangskontrolle (unbefugte Nutzung von Datenverarbeitungssystemen)

zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)

AWS

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, die das AWS-Netzwerk von unbefugtem Zugang schützen. Derzeit umfassen diese Maßnahmen unter anderem:

- Der Benutzer- und Administratorzugriff auf das AWS-Netzwerk beruhen auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.
- Der Benutzerzugriff auf das AWS-Netzwerk wird erst aktiviert, wenn die Personalabteilung einen entsprechenden Datensatz im HR-System erstellt hat.
- Bei AWS gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen.
- Die erteilten Zugriffsrechte auf AWS IT-Systeme werden mindestens vierteljährlich von zuständigen Mitarbeitern überprüft. Zugriffsberechtigungen werden sofort aufgehoben, wenn die entsprechenden Zugriffsrechte für die Tätigkeiten des Benutzers nicht mehr erforderlich sind.
- Die Zugriffsrechte auf das AWS IT-System werden innerhalb von 24 Stunden nach Deaktivierung des jeweiligen Mitarbeiterdatensatzes im HR-System durch die Personalabteilung aufgehoben.
- Passwörter/Pass-Phrasen für die Erstanmeldung bestehen aus einem einmaligen Wert und werden nach der ersten Verwendung sofort geändert.
- Benutzerpasswörter/-Pass-Phrasen werden spätestens alle 90 Tage geändert. Es sind nur komplexe Passwörter zulässig. Die Änderung des Passworts durch einfache Passwortvariationen z. B. durch Ändern einer einzigen Stelle, ist nicht möglich.
- Das Erstellen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsmerkmalen wird zusammen mit einem Zeitstempel protokolliert.
- Auf Amazon Equipment (z. B. Notebooks) ist Antivirus-Software installiert, die einen E-Mail-Filter sowie eine Malware-Erkennung enthält.
- AWS Firewall Geräte sind so konfiguriert, dass sie den Zugriff auf die Datenverarbeitungsumgebung beschränken und die Absicherung der Computing-Cluster verstärken.

- AWS Firewall-Richtlinien (d.h. Konfigurationsdateien) werden automatisch alle 24 Stunden an die Firewall-Geräte übertragen und aufgespielt.
- Die Kommunikation im AWS-Netzwerk erfolgt SSH-Verschlüsselt („Public key“) durch einen Bastion-Host, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt und alle Aktivitäten im AWS-Netzwerk für eine Sicherheitsüberprüfung protokolliert.

Kunde

AWS bietet den Kunden in der Management Console verschiedene Optionen, um Sicherheitsmaßnahmen in ihrer Cloud-Umgebung umzusetzen. AWS ermöglicht es den Kunden außerdem eigene Sicherheitsmaßnahmen zu ergreifen. Der Kunde ist für die Umsetzung sowie die Pflege und Verwaltung der Sicherheitsmaßnahmen im Rahmen des AWS-Netzwerks verantwortlich. Der Kunde ist insbesondere dafür verantwortlich, die Architektur der Lösung über die von AWS bereitgestellte Management Console oder andere Service-Schnittstellen zu konfigurieren sowie die Plattform und Anwendungen entsprechend den individuellen Anforderungen des Kunden zu konfigurieren und zu installieren. Dazu gehören unter anderem Sicherheitsmaßnahmen, um Zugangsinformationen für Benutzer zu verwalten; insbesondere wenn Benutzer diese Zugangsinformation benötigen, um für den Kunden über Service-Schnittstellen auf die AWS-Services zuzugreifen.

Darüber hinaus kann der Kunde seine Daten bei der Übertragung und bei der Speicherung verschlüsseln. Weitere Informationen finden Sie im Whitepaper AWS-Sicherheit – Best Practices.

- **Schützen Sie Ihre Daten während der Übertragung.** Cloud-Anwendungen kommunizieren oft über öffentliche Verbindungen (wie dem Internet). Wenn Sie Anwendungen in der Cloud nutzen, ist es wichtig, Daten bei der Übertragung vor unberechtigten Zugriffen zu schützen. Dies beinhaltet den Schutz des Netzwerkverkehrs zwischen Clients und Servern sowie zwischen Servern untereinander.

  Die AWS-Services ermöglichen die Nutzung von IPSec und SSL/TLS zum Schutz von Daten während der Übermittlung. IPSec ist ein Protokoll, das den IP-Protokollstapel erweitert (oft innerhalb der Netzwerkinfrastruktur) und sicherstellt, dass Anwendungen auf den oberen Schichten ohne Modifizierung sicher kommunizieren können. SSL/TLS befindet sich auf der Sitzungsschicht und arbeitet oft mit Anwendungen der Anwendungsschicht zusammen. Diese Aufgabe können SSL/TLS-Wrapper von Drittanbietern übernehmen können.

- **Schützen Sie Ihre Daten während der Speicherung.** Sicherheitsmaßnahmen, die auf Verschlüsselung beruhen, benötigen Schlüssel. Diese Schlüssel müssen sicher aufbewahrt werden, unabhängig davon, ob eine Cloud-Umgebung oder ein lokales System genutzt wird.

Sie können entweder ihre eigenen bereits bestehenden Prozesse verwenden, um Schlüssel in der Cloud zu verwalten oder die serverseitige Verschlüsselung, inklusive der AWS Schlüsselverwaltung und den vorhandenen Speicherfunktionen, nutzen.

Wenn Sie sich entscheiden, Ihre eigenen Schlüsselverwaltungsprozesse zu verwenden, haben Sie verschiedene Möglichkeiten die Schlüssel zu speichern und zu schützen. Wir empfehlen dringend die Schlüssel in manipulationssicheren Speichern zu speichern, zum Beispiel einem Hardware-Sicherheitsmodul (HSM). Amazon Web Services bietet mit AWS CloudHSM einen sicheren HSM-Service in der Cloud. Alternativ können Sie eigene HSMs einsetzen, die die Schlüssel lokal speichern. Auf diese Schlüssel können Sie über sichere Verbindungen zugreifen, zum Beispiel über Amazon VPC in einem mit IPSec gesicherten VPN (virtuelles privates Netzwerk) oder AWS Direct Connect mit IPSec.

3. Zugriffskontrolle (nicht autorisierte Nutzung von Daten)

zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

AWS

AWS hat die folgenden technischen und organisatorischen Maßnahmen zur Einräumung und Regelung von Zugriffsrechten für Mitarbeiter von AWS und freien Mitarbeitern, die mit AWS zusammenarbeiten, umgesetzt. Derzeit umfassen diese Maßnahmen unter anderem:

- Benutzer- und Administratorzugriff auf das AWS-Netzwerk beruhen auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzer und Administratoren genutzt werden können.
- Bei AWS gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen.
- Die erteilten Zugriffsrechte auf AWS IT-Systeme werden mindestens vierteljährlich von zuständigen Mitarbeitern überprüft.

- Das Erstellen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsmerkmalen wird zusammen mit einem Zeitstempel protokolliert.
- AWS hat einen Vorfallreaktionsplan erstellt, der bei einem Vorfall Folgendes regelt:
  - Rollen, Verantwortlichkeiten, Kommunikations- und Kontaktstrategien für den Gefährdungsfall;
  - Konkrete Verfahren als festgelegte Reaktion auf bestimmte Vorfälle;
  - Abdeckung und Ansprache sämtlicher wichtigen Bestandteile des Systems.

Kunde

AWS bietet den Kunden in der Management Console verschiedene Optionen, um Sicherheitsmaßnahmen in ihrer Cloud-Umgebung umzusetzen. AWS ermöglicht es den Kunden außerdem eigene Sicherheitsmaßnahmen zu ergreifen. Die Kunden sind für Maßnahmen auf den Schichten oberhalb des AWS-Netzwerks verantwortlich. Der Kunde ist insbesondere für die Umsetzung sowie die Pflege und Verwaltung der Zugriffsberechtigungen auf personenbezogene Daten verantwortlich.

Die Kunden können ihre Daten bei der Übertragung und bei der Speicherung verschlüsseln. Weitere Informationen finden Sie im Whitepaper AWS-Sicherheit – Best Practices (insbesondere die im Abschnitt 2. oben angegebenen Informationen).

Das Whitepaper „AWS-Sicherheit – Best Practices" enthält zusätzlich die folgenden relevanten Informationen, die Ihnen bei der Verwaltung von Konten und Zugriffsberechtigungen behilflich sein können:

- **AWS-Konto.** Dies ist das Konto, das Sie bei der erstmaligen Anmeldung auf AWS erstellen. Das AWS-Konto ist Teil der Geschäftsbeziehung zwischen Ihnen und AWS und ermöglicht es Ihnen Ihre AWS-Ressourcen und -Services zu verwalten. AWS-Konten besitzen Root-Rechte für alle AWS-Ressourcen und –Services und haben großen Einfluss auf die AWS-Services. Verwenden Sie Root-Zugangsinformationen daher nicht für die tägliche Arbeit auf AWS. Unter Umständen entscheidet sich Ihr Unternehmen dazu, mehrere AWS-Konten zu nutzen, beispielsweise ein Konto für jede wesentliche Abteilung. Unter diesen AWS-Konten können Sie IAM-Benutzer für die entsprechenden Personen und Ressourcen einrichten. Weitere Informationen finden Sie auch in den Empfehlungen zu bewährten Methoden für IAM unter http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html.
- **IAM-Benutzer.** Mit IAM können Sie viele Benutzer einrichten und ihnen individuellen Sicherheits-Anmeldedaten zuteilen. Alle angelegten Benutzer werden unter dem jeweiligen AWS-Konto verwaltet. IAM-Benutzer kann eine Person, ein Service oder eine Anwendung sein, die über die Management Console, CLI oder direkt über APIs auf

Ihre AWS-Ressourcen zugreifen muss. Idealerweise wird für jede Person Service oder Anwendung ein eigener IAM-Benutzer eingerichtet, der Zugriff auf Services und Ressourcen Ihres AWS-Kontos erhält. Sie können fein abgestimmte Berechtigungen für den Zugriff auf Ressourcen Ihres AWS-Konto einreichen und auf von Ihnen erstellte Gruppen anwenden. Sie können jeder dieser Gruppen Benutzer zuordnen. Benutzer einer Gruppe erhalten so die vorher definierten Berechtigungen. Dieses „Best Practice“ hilft Ihnen, sicherzustellen, dass Benutzer nur genau die Berechtigungen besitzen, die sie für ihre Aufgaben benötigen.

Die Kunden sind dafür verantwortlich, die Konten und Zugriffsberechtigungen regelmäßig zu überprüfen.

4. Weitergabekontrolle

zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle)

AWS

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, um sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Diese Maßnahmen stellen auch sicher, dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen oder erfolgt ist. Derzeit umfassen diese Maßnahmen unter anderem:

- **Verhinderung von unbefugtem Kopieren:** Die von AWS ergriffenen Maßnahmen zur Verhinderung von unbefugtem Kopieren der physischen Speicherinfrastruktur als solche (z. B. Kopieren der Daten des Kunden durch Übertragung auf ein externes Speichermedium wie eine Festplatte) sind in den Maßnahmen wie oben in Ziffern 1–3 beschrieben enthalten. Darüber hinaus dürfen AWS Mitarbeiter und freie Mitarbeiter keine privaten elektronischen Geräte und mobile Datenträger an AWS-Informationssysteme anschließen.
- **Nutzung eines rollenbasierten Zugriffsberechtigungsmodells:** siehe oben
- **Firewall-Richtlinien:** siehe oben.
- **Implementieren eines Vorfallreaktionsplans:** siehe oben.

- **Außerbetriebnahme von Speichergeräten:** Wenn die Lebensdauer eines Speichergeräts zu Ende geht, führt AWS einen speziellen Prozess zur Außerbetriebnahme durch, damit Kundeninhalte nicht an unbefugte Personen gelangen. Alle stillgelegten Magnetspeichergeräte werden entmagnetisiert und den branchenüblichen Vorgehensweisen und dem geltenden Datenschutzgesetz entsprechend physisch zerstört.
- **Sichere Zugangspunkte:** AWS verfügt über eine beschränkte Anzahl von Zugriffspunkten zur Cloud. Diese Kundenzugriffspunkte heißen API-Endpunkte und dienen dem sicheren HTTP-Zugriff (HTTPS). Kunden können hierdurch sicher mit den Speicher- oder Datenverarbeitungs-Instanzen auf der AWS-Plattform kommunizieren.
- **Schutz der Übertragung:** Die Kunden können eine Verbindung mit einem AWS-Zugriffspunkt über HTTP oder HTTPS aufbauen. HTTP oder HTTPS sind Verschlüsselungsprotokolle, die zum Schutz vor Abhörangriffen, Datenmanipulation oder Fälschung von Nachrichten entwickelt wurde. Kunden, die zusätzliche Netzwerksicherheitsschichten benötigen, bietet AWS die Amazon Virtual Private Cloud (VPC) an. Die AWS VPC ist ein privates Subnetz innerhalb der AWS-Cloud und ermöglicht die Verwendung eines IPsec Virtual Private Network (VPN)-Geräts. Hierdurch können Kunden einen verschlüsselten Tunnel zwischen dem Amazon-VPC und dem Rechenzentrum des Kunden herstellen.
- **Verbindungen mit dem AWS-Netzwerk durch AWS-Mitarbeiter:** AWS-Mitarbeiter greifen SSH-Verschlüsselt („Public key“) durch einen Bastion-Host auf das AWS Netzwerk zu. Der Bastion-Host beschränkt den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten.

Kunde

AWS bietet den Kunden in der Management Console verschiedene Optionen, um Sicherheitsmaßnahmen in ihrer Cloud-Umgebung umzusetzen. AWS ermöglicht es den Kunden außerdem eigene Sicherheitsmaßnahmen zu ergreifen. Die Kunden sind für Maßnahmen auf den Schichten oberhalb des AWS-Netzwerks verantwortlich. Der Kunde ist insbesondere für die Umsetzung sowie die Pflege und Verwaltung von Maßnahmen verantwortlich, die verhindern, dass die übertragenen personenbezogenen Daten während der Übertragung, des Transports oder der Speicherung innerhalb der Services ohne Autorisierung des Kunden gelesen, kopiert, verändert oder gelöscht werden können.

Die Kunden können ihre Daten bei der Übertragung und bei der Speicherung verschlüsseln. Weitere Informationen finden Sie im Whitepaper AWS-Sicherheit – Best Practices (insbesondere die im Abschnitt 2. oben angegebenen Informationen).

Das Whitepaper AWS-Sicherheit – Best Practices enthält außerdem Informationen zur Amazon Virtual Private Cloud (VPC):

- Mit der Amazon Virtual Private Cloud (VPC) können Sie private Clouds innerhalb einer öffentlichen AWS-Cloud erstellen.
- Jede Amazon VPC eines Kunden verwendet einen vom Kunden zugewiesenen Bereich von IP-Adressen. Amazon VPC ermöglicht Ihnen insbesondere die Nutzung privater IP-Adressen (wie von RFC 1918 empfohlen) und Erstellung von privaten Clouds oder verbundene zugeordnete Netzwerke in der Cloud, die nicht direkt über das Internet routingfähig sind.

Amazon VPC bietet nicht nur die Isolationsmöglichkeit zu anderen Kunden in der privaten Cloud, sondern bietet außerdem eine Schicht 3-Isolierung (IP-Routing durch die Vermittlungsschicht) vom Internet.

5. Eingabekontrolle

zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

AWS

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, die es ermöglichen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Derzeit umfassen diese Maßnahmen unter anderem:

- **Dateneingabe nicht im Umfang der Services enthalten:** Die von AWS angebotenen Services, die der Kunde nutzen kann, sind reine Infrastruktur-Services. Sie umfassen keine Eingabe von personenbezogenen Daten im AWS-Netzwerk durch AWS für den Kunden.
- **Nachverfolgen von API-Aufrufen:** Derzeit ermöglicht AWS den Kunden, API-Anfragen nachzuverfolgen, die im Rahmen des AWS Enterprise-Kontos entstehen. Zu diesem Zweck stellt AWS den Kunden den Web-Service CloudTrail zur Verfügung.
- **Protokollieren und Überwachen von überprüfbaren Ereigniskategorien:** AWS hat für alle Systeme und Geräte innerhalb des AWS-Systems Ereigniskategorien festgestellt, die sich durch Audits überprüfen lassen. Service-Teams konfigurieren die Auditfunktionen sicherheitsrelevante Ereignisse zu protokolieren. Die Auditdaten enthalten eine Gruppe von Datenelementen („Wann" (Zeitstempel), „Wo" (Quelle), „Wer" (Benutzername), „Was" (Inhalt)), um die Anforderungen an erforderliche Auswertungen der Überprüfung zu unterstützen. Zusätzlich stehen sie dem AWS-Sicherheitsteam oder anderen relevanten Teams zur Prüfung oder Auswertung und für

die Behebung sicherheitsrelevanter oder geschäftsbeeinträchtigende Ereignisse zur Verfügung.

- **Protokollieren von Benutzeraktivitäten:** AWS-Entwickler und Administratoren, die zur Wartung der AWS Services Zugriff auf die AWS Cloud-Komponenten benötigen, müssen ausdrücklich Zugriff auf die entsprechenden Komponenten beantragen. Berechtigte AWS-Mitarbeiter greifen SSH-verschlüsselt („Public key") durch einen Bastion-Host auf das AWS Netzwerk zu. Der Bastion-Host beschränkt den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten und protokolliert alle Aktivitäten zur Sicherheitsüberprüfung.

Kunde

Kunden können personenbezogene Daten durch die Verwendung des Service eingeben und sind daher verantwortlich für die Umsetzung, Pflege und Wartung von Maßnahmen zur Dokumentation wann und von wem personenbezogene Daten in das Datenverarbeitungssystem eingegeben, geändert oder gelöscht wurden, zum Beispiel durch Erstellung eines Prüfpfads.

Weitere Informationen zur Eingabekontrolle, einschließlich der formalen Richtlinien und Verfahren zum Bestimmen der Mindeststandards für den logischen Zugriff auf AWS-Ressourcen nach den DIN ISO/IEC 27001-Normen, finden Sie im Whitepaper Amazon Web Services: Risiko und Compliance. Im SOC 1 Type II-Bericht von AWS sind die Sicherheitsmaßnahmen im Rahmen der Bereitstellung des Zugriffs auf AWS-Ressourcen beschrieben.

AWS CloudTrail ist ein Web-Service, der Anfragen an AWS-APIs im Rahmen Ihres AWS-Kontos protokolliert und entsprechende Protokolldateien an Sie übermittelt. Zu den aufgezeichneten Informationen gehören unter anderem die Identität des über die Schnittstelle Anfragenden, den Zeitpunkt der API-Anfrage, die Quell-IP-Adresse des über die Schnittstelle Anfragenden, die Anfrageparameter und die Bestandteile der Antwort, die vom AWS-Service zurückgegeben werden. Mit CloudTrail erhalten Sie einen Verlauf der Anfragen an AWS-APIs im Rahmen Ihres AWS-Kontos, einschließlich über die AWS Management Console, AWS SDKs, Befehlszeilen-Tools und allgemeine AWS-Services (z. B. AWS CloudFormation) erfolgte Anfragen und AWS APIs. Der AWS-API-Aufrufverlauf, der von CloudTrail generiert wird, ermöglicht eine Sicherheitsanalyse, Nachverfolgung von Ressourcenänderungen und Überwachung der Einhaltung von Vorschriften.

6. Auftragskontrolle

zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

AWS

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, um sicherzustellen, dass personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Derzeit umfassen diese Maßnahmen unter anderem:

- **Interne Kommunikation:** AWS hat weltweit verschiedene Verfahren zur internen Kommunikation eingeführt, um AWS Mitarbeitern ihre individuellen Funktionen und Verantwortlichkeiten näher zu bringen, und um wichtige Ereignisse fristgerecht zu kommunizieren. Hierzu zählen Einführungs- und Schulungsprogramme für neu eingestellte Mitarbeiter sowie regelmäßige Besprechungen des Geschäftsführung zur Unternehmensleistung und anderen Themen.
- **Trennung vom Unternehmensnetzwerk von Amazon:** Das AWS-Produktionsnetzwerk ist logisch vom Amazon-Unternehmensnetzwerk getrennt. Die Trennung erfolgt durch den Einsatz von komplexen Vorrichtungen zur Netzwerksicherheit und Netzwerktrennung. AWS-Entwickler und Administratoren des Unternehmensnetzwerks, die zur Wartung der AWS Services Zugriff auf die AWS Cloud-Komponenten benötigen, müssen ausdrücklich Zugriff auf die entsprechenden Cloud-Komponenten beantragen. Alle Anforderungen werden vom zuständigen Service-Inhaber überprüft und müssen von diesem genehmigt werden. Berechtigte AWS-Mitarbeiter stellen danach eine Verbindung zum AWS-Netzwerk durch einen Bastion-Host her, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt und alle durchgeführten Aktivitäten zum Zweck einer Sicherheitsprüfung protokolliert. Der Zugriff auf Bastion-Hosts erfordert für alle Benutzerkonten auf dem Host eine SSH-Verschlüsselung („Public key“).
- **Zuverlässiges Compliance-Programm:** Die von AWS für Kunden bereitgestellte IT-Infrastruktur wurde unter Berücksichtigung von „Best Practices“ in Übereinstimmung mit einer Reihe von IT-Sicherheitsstandards entwickelt und wird nach denselben Grundsätzen betrieben und verwaltet. Dazu gehören: SOC 1 (früher SAS 70), SOC 2, SOC 3 und FedRAMP, PCI DSS Level 1, ISO 27001.

- **Verhinderung des Zugriffs durch Unternehmensangehörige:** AWS hat spezielle SOC 1-Maßnahmen umgesetzt, die das Risiko unbefugter Zugriffe durch Unternehmensangehörige angehen. AWS-Zertifizierungen und Bescheinigungen von Drittanbietern, die sich auf den logischen Zugriff auf AWS Systeme beziehen, berücksichtigten präventive und nachträglich Maßnahmen zur Aufdeckung von unbefugten Zugriffen, die von AWS umgesetzt wurden. Zusätzlich werden regelmäßig Risikobewertungen erstellt, wie der Zugriff durch Unternehmensangehörige kontrolliert und überwacht werden kann.
- **Richtlinien und Schulungen zur Sicherheitssensibilisierung:** AWS führt für jährliche Schulungen zur Sensibilisierung von Sicherheitsrisiken durch. Diese Schulungen werden für alle Benutzer der AWS Systeme durchgeführt, die für AWS tätig werden. Die Richtlinien und Verfahren wurden von AWS unter Berücksichtigung der Anforderungen an Sicherheit und Datenschutz festgelegt. Die AWS-Richtlinien, Prozesse und relevanten Schulungsprogramme werden von unabhängigen, externen Auditoren überprüft. Die Administratoren der AWS-Systeme unterliegen der Geheimhaltungspflicht und sind verpflichtet, sicherzustellen, dass die Kundeninhalte nicht entgegen der AWS-Richtlinien, Prozesse und Schulungsprogramme verarbeitet werden.
- **Prüfungen zu krimineller Vergangenheit:** AWS prüft, soweit nach anwendbarem Recht zulässig, vor einer Einstellung eines AWS Mitarbeiters auf relevante Vorstrafen. Diese Prüfungen beziehen sich explizit auf die Position des Mitarbeiters und den Umfang des Zugangs zu AWS-Einrichtungen.

Kunde

Unsere Services werden von unseren Kunden durch Anfragen über Schnittstellen (API) oder die AWS Management Console bereitgestellt und kontrolliert.

Weitere Informationen zur Bereitstellung unserer Services über API-Anfragen finden Sie auf der Informationsseite zum Signieren von AWS API-Anfragen.

Kunden können die Amazon Web Services (AWS)-API über zwei Wege anfragen: Sie können eine REST-Anfragen über HTTP/HTTPS senden oder Wrapper-Funktionen in einem der AWS SDKs aufrufen. In dieser Anleitung wird beschrieben, wie Sie Ihre REST-Anfrage signieren. Wenn Sie ein AWS SDK verwenden, übernimmt das SDK den Signaturprozess für Sie.

- **REST-/Anfrage:** REST- oder Anfrage sind HTTP- oder HTTPS-Anforderungen, die ein HTTP-Verb (wie GET oder POST) und einen Parameter namens „Action" oder „Operation" verwenden. HTTP-Verb und Parameter geben die API an, die Sie aufrufen. Eine API mit einer REST- /Anfrage aufzurufen, ist der direkte Weg auf einen Web-Service zuzugreifen. Allerdings ist erforderlich, dass Ihre Anwendung mit niedrigen Anforderungen, wie dem Erstellen des Hash-Zeichens zum Signieren der Anforderung

oder der Fehlerbehebung zurechtkommt. Der Vorteil der REST- Anfrage besteht darin, dass Sie Zugriff auf die vollständige Funktionalität einer API haben.

- **AWS SDKs:** Die SDKs von AWS stellen Wrapper-Funktionen für eine API bereit und übernehmen viele der Verbindungsdetails, wie Berechnen der Signaturen, Umgang mit Anfragewiederholungen und Fehlerbehandlung. Die SDKs enthalten außerdem Beispiel-Code, Tutorials und weitere Ressourcen, die Sie beim Schreiben von Anwendungen zum Aufrufen von AWS unterstützen. Durch Aufrufen der Wrapper-Funktionen in einem SDK kann der Prozess zum Schreiben einer AWS-Anwendung erheblich vereinfacht werden.
- **Signieren von REST-/Anfragen:** AWS erfordert, dass Sie jede Anforderung authentifizieren, indem Sie sie signieren. Zum Signieren einer Anforderung berechnen Sie eine digitale Signatur mit einer kryptografischen Hash-Funktion. Ein kryptografischer Hash ist eine einfache Funktion. Sie gibt auf Grundlage der Eingabe einen einzigartigen Hash-Wert zurück. Die Eingabe zur Hash-Funktion beinhaltet den Text der Anforderung und den geheimen Zugriffsschlüssel. Die Hash-Funktion gibt einen Hash-Wert zurück. Dieser wird der Anforderung als Signatur hinzugefügt.

  Nach dem Erhalt Ihrer Anforderung berechnet AWS die Signatur mit derselben Hash-Funktion und den von Ihnen zum Signieren der Anforderung eingegebenen Daten neu. Wenn die so berechnete Signatur mit der Signatur in der Anforderung übereinstimmt, verarbeitet AWS die Anforderung. Andernfalls wird die Anforderung abgelehnt.

  Zur Verbesserung der Sicherheit wird die Übertragung Ihrer Anforderungen von der API nur akzeptiert, wenn Secure Sockets Layer (SSL) mit HTTPS verwendet wird. Mit SSL wird die Übertragung verschlüsselt und Ihre Anforderung oder die Antwort geschützt, sodass sie bei der Übertragung nicht angesehen werden kann.

7. Verfügbarkeitskontrolle

zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

AWS

AWS hat die folgenden technischen und organisatorischen Maßnahmen zum Schutz der Daten gegen zufällige Zerstörung oder Verlust umgesetzt. Derzeit umfassen diese Maßnahmen unter anderem:

- **Branderkennung und -bekämpfung:** AWS hat Einrichtungen zur automatischen Branderkennung und -bekämpfung in den AWS-Rechenzentren installiert. Das Branderkennungssystem setzt Rauchsensoren in der gesamten Umgebung der Rechenzentren, in mechanischen und elektrischen Bereichen der Infrastruktur,

Kühlräumen und sowie in den Räumen, in denen die Generatoren untergebracht sind, ein.

- **Redundante Stromversorgungssysteme:** Die elektrischen Anlagen der Rechenzentren wurden so entwickelt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs gewartet werden können. Die redundanten Rechenzentren laufen rund um die Uhr, sieben Tage die Woche. Unterbrechungsfreie Stromversorgung (Uninterruptable Power Supply-Geräte, UPS) sorgen im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Rechenzentren verfügen darüber hinaus über Generatoren, die die gesamte Anlage mit Notstrom versorgen können.
- **Klimatisierung und Temperaturkontrolle:** Mitarbeiter und entsprechende Systeme überwachen und steuern die Temperatur und Luftfeuchtigkeit innerhalb der Rechenzentren auf einem angemessenen Niveau.
- **Vorbeugende Wartungsmaßnahmen:** Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

- **Mehrere Verfügbarkeitszonen (Availability Zones):** AWS bietet den Kunden die Flexibilität, Instanzen innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones verteilt aufzusetzen und Daten innerhalb dieser einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Kategorien für Überschwemmungsrisiken). Sämtliche Availability Zones sind redundant mit mehreren Schicht-1-Transit-Providern verbunden.
- **Überprüfung der Notfallpläne durch die Geschäftsführung:** Die AWS-Notfallpläne werden durch Mitglieder der Geschäftsführung und des Prüfungsausschusses des Vorstands regelmäßig überprüft.

Kunde

AWS bietet den Kunden in der Management Console verschiedene Optionen, um Sicherheitsmaßnahmen in ihrer Cloud-Umgebung umzusetzen. AWS ermöglicht es den Kunden außerdem eigene Sicherheitsmaßnahmen zu ergreifen. Unsere Kunden sind für die ordnungsgemäße Gestaltung und Konfiguration der Architektur unter Verwendung der Serviceangebote verantwortlich, um die Anforderungen der Kunden im Hinblick auf die Verfügbarkeit von personenbezogenen Daten zu erfüllen (z.B. durch Hinzufügen von Redundanz und Konfiguration geeigneter Archivierungs-/Datensicherungskonzepte je nach Relevanz der Daten/Konfiguration der logischen Architektur als 3-Schichten-Ansatz). Wir empfehlen den Kunden, regelmäßige Back-Ups der Kundeninhalte zu erstellen. Zudem sollten Kunden branchenübliche Maßnahmen gegen unbefugten Zugriff auf Kundeninhalte, unbefugtes Löschen oder versehentlichen Verlust von Kundeninhalten zu ergreifen. Darüber hinaus sollten Kunden verpflichtende Richtlinien einführen, die die Nutzung von Antiviren- und Firewall-Software auf Systemen vorschreiben, die den Zugriff auf die Service-Offerings oder die Kundeninhalte ermöglichen.

8. Trennungskontrolle

> zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle)

AWS

AWS hat die folgenden technischen und organisatorischen Maßnahmen ergriffen, um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- **Mandantenfähige Umgebung:** Die AWS-Umgebung ist eine virtualisierte Mehrmandantenumgebung. AWS hat Prozesse zur Sicherheitsverwaltung sowie

Sicherheitskontrollen eingerichtet, die die Trennung von Daten einzelner Kunden ermöglicht. AWS-Systeme sind so konzipiert, dass Kunden nicht auf physische Hosts oder Instanzen zugreifen können, die nicht zu ihrem AWS-Account gehören. Dies wird durch die Filterung im Rahmen einer Virtualisierungssoftware ermöglicht. Der Hypervisor wird regelmäßig von internen und externen Expertenteams auf neue und vorhandene Schwachstellen und Angriffsmöglichkeiten geprüft. Der Hypervisor eignet sich gut für die Aufrechterhaltung einer strikten Trennung zwischen virtuellen Gastmaschinen.

- **Einzelmandantenoptionen:** AWS-Services, z. B. Virtual Private Cloud (VPC), ermöglichen den Kunden, Instanzen zu verwenden, die auf der Host-Hardware-Ebene physisch isoliert sind. Kunden können AWS-Services auch vom Internet isolieren. Solche AWS-Services werden auf Einzelmandantenhardware ausgeführt.
- **Trennung vom Unternehmensnetzwerk von Amazon:** siehe oben.
- **Eindeutiger Verschlüsselungsschlüssel:** AWS-Kunden verwalten ihre eigene Verschlüsselung inklusive der Schlüssel. Das gilt dann nicht, wenn die Kunden den AWS-Service für die serverseitige Verschlüsselung nutzen. In diesem Fall erstellt AWS pro Mandanten einen eindeutigen Verschlüsselungsschlüssel.

Kunde

Kontrolle und Eigentum an den eigenen Daten verbleiben bei den AWS-Kunden. Kunden können zur Erfüllung ihrer Anforderungen Richtlinien und Verfahren für die Kennzeichnung und Verarbeitung einführen. Weitere Informationen finden Sie im Whitepaper Amazon Web Services: Risiko und Compliance.

Die Trennung von Inhalten (Daten) liegt in der Verantwortung der AWS-Kunden. Die AWS-Kunden behalten die Kontrolle über ihre selbst aufgespielten Gastbetriebssysteme, Software, Anwendungen und Daten. Durch Konfigurationstools, wie die AWS Management Console und APIs können Kunden Service-Funktionen verwenden, z. B. Blockverschlüsselungen, um die Datentrennung zu erzwingen. Kunden können auch Verschlüsselungstools von Drittanbietern nutzen. Der Kunde ist verantwortlich, diese zusätzlichen Maßnahmen - soweit für die vom Kunden beabsichtigte Trennung erforderlich - umzusetzen.

Berichtigen, Löschen und Sperren von Inhalten

Die AWS-Services ermöglichen es den Kunden Maßnahmen zum Abrufen, Korrigieren, Löschen oder Sperren von Kundeninhalten einzurichten (wie in den Benutzer- und Administratoranleitungen für die Services unter http://aws.amazon.com/documentation beschrieben).

Wenn ein Kunde seine Inhalte aus den AWS-Services löscht, werden die Inhalte unleserlich oder unbrauchbar gemacht. Die für die Speicherung der Kundeninhalte genutzten Bereiche im AWS-Netzwerk werden gemäß den AWS-Standardrichtlinien und Löschungsfristen auf sichere Weise gelöscht, bevor sie erneut verwendet und überschrieben werden.

Kundeninhalte werden ohne Zustimmung des Kunden von AWS nicht korrigiert, gelöscht oder blockiert.

Unterauftragnehmer

AWS nimmt eine Reihe von externen Unterauftragnehmern in Anspruch, die uns bei der Bereitstellung der Services unterstützen. Unsere Unterauftragnehmer haben jedoch keinen logischen Zugriff auf Kundeninhalte. AWS arbeitet nur mit vertrauenswürdigen Unterauftragnehmern zusammen. AWS vereinbart angemessene vertragliche Schutzmaßnahmen, deren Einhaltung AWS regelmäßig überprüft, um sicherzustellen, dass die erforderlichen Standards aufrechterhalten werden. Weitere Informationen über Unterauftragnehmer, die auf Kundeninhalte, einschließlich personenbezogener Daten, zugreifen können, sind auf der AWS-Website aufgeführt.

Datenschutzverstöße

Da bei der Nutzung von AWS die Verantwortlichkeit und Kontrolle über personenbezogene(n) Daten bei den Kunden verbleibt, obliegt es auch ihrer Verantwortung, die eigene Umgebung auf Datenschutzverletzungen zu überwachen und Aufsichtsbehörden sowie Betroffene gemäß den anwendbaren Gesetzen darüber zu informieren.

Kunden haben die Kontrolle über ihre eigenen Zugriffsschlüssel und legen fest, wer berechtigt ist, auf ihr AWS-Konto zuzugreifen. AWS hat keinerlei Einblick oder Kenntnis, welche Zugriffsschlüssel verwendet werden und welche Personen berechtigt sind, sich in dem AWS Konto anzumelden. Der Kunde ist dafür verantwortlich, Nutzung, Missbrauch, Vergabe oder Verlust von Zugriffsschlüsseln zu überwachen.

AWS benachrichtigt den Kunden unverzüglich, wenn AWS Kenntnis von einem nachweislichen Verstoß gegen die AWS-Sicherheitsstandards in Bezug auf das AWS-Netzwerk hat.

Löschung bei Beendigung

Die AWS-Services ermöglichen dem Kunden selbst über die Löschung von Daten zu entscheiden. Die AWS-Services sind ein Self-Service-Modell sind und reagieren lediglich automatisch auf die Weisungen des Kunden, die dieser über die AWS Management Console oder die APIs erteilt.

Wenn der Kunde Kundeninhalte löschen möchte (sei es während des Nutzungszeitraums der AWS-Services oder bei Beendigung der Nutzung der AWS-Services), muss der Kunde die entsprechenden Daten über die AWS Management Console oder die APIs für jede Instanz von Kundeninhalten löschen.

AWS verwaltet oder löscht keine Kundeninhalte im Namen des Kunden.

Der Kunde kann das entsprechende Ausgabeformat der Kundeninhalte nach der Löschung wählen. So behält der Kunde die vollständige Kontrolle zur Erhöhung des Schutzes im Hinblick auf die zu löschenden Kundeninhalte.

Maßnahmen zur Erhöhung des Schutzes der zu löschenden Kundeninhalte:

- Der Kunde kann die Kundeninhalte vor dem Löschen zurücksetzen („wipe"), wenn der genutzte Service dies zulässt.
- Der Kunde kann die Kundeninhalte vor dem Löschen verschlüsseln.

Wenn der Kunde Kundeninhalte in einem verschlüsselten Format löscht, bleiben die Inhalte während des AWS-Löschvorgangs verschlüsselt. Ohne den Verschlüsselungsschlüssel ist es nicht möglich, diese Daten zu entschlüsseln. Zur Erhöhung des Schutzes von Kundeninhalten hat der Kunde außerdem die Möglichkeit, den Verschlüsselungsschlüssel außerhalb der AWS-Umgebung zu speichern und ihn zu zerstören, um eine Entschlüsselung zu verhindern.

Aber auch wenn der Verschlüsselungsschlüssel immer noch verfügbar bliebe, wäre eine Entschlüsselung aus den folgenden Gründen äußerst unwahrscheinlich:

- Die Kundeninhalte werden auf verschiedenen Speichermedien in der relevanten AWS-Region gespeichert und die Zuordnung zwischen diesen verschiedenen Speichermedien wird aufgehoben, wenn der Kunde die Daten löscht.
- Nachdem der Kunde die Kundeninhalte gelöscht hat, können jederzeit einzelne Bereiche der Daten überschrieben werden, da die Speichermedien, auf denen die Daten gespeichert wurden, erneut bereitgestellt werden. Je nachdem wie die Daten strukturiert sind, ist eine Entschlüsselung ohne alle Daten unter Umständen nicht möglich.

Drittanbieter des Kunden

Wie bereits zuvor in diesem Dokument erwähnt, sind mit der AWS-Umgebung auch andere Services verknüpft, die direkt von Drittanbietern (z. B. Internetdienstanbietern) für den Kunden bereitgestellt werden. Diesen Drittanbietern sind für ihre eigenen Systeme verantwortlich, einschließlich der Sicherheit. AWS ist nicht für die Aktivitäten dieser Drittanbieter verantwortlich.

Sonstige Überlegungen

Dieses Whitepaper behandelt außer dem BDSG keine anderen Datenschutzgesetze, die für die Kunden ebenfalls relevant sein könnten, einschließlich branchenspezifischer Anforderungen, wie spezielle Anforderungen für Banken, Versicherungsgesellschaften, Ärzte und Krankenhäuser. Ob für einzelne Kunden andere Datenschutz- und Datensicherungsgesetze gelten, hängt 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 regulatorischen und datenschutzrechtlichen Anforderung haben, sollten zuerst die für sie geltenden Anforderungen ermitteln und entsprechende Beratung einholen.

Fazit

Sicherheit hat 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 äußerst sensible Informationen anvertrauen, beispielsweise personenbezogene Gesundheits- und Finanzdaten.

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.

Weitere Informationen

Um Kunden ein besseres Verständnis zu vermitteln, wie sie ihre Datenschutz- und Datensicherungsanforderungen umsetzen 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.

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 von Dozenten geleitete Schulungen. Weitere Informationen zu AWS-Schulungen finden Sie unter http://aws.amazon.com/training/.

AWS-Zertifizierungen sind dafür konzipiert, die technischen Fähigkeiten und Kenntnisse in Bezug auf bewährte Verfahrensweisen für die Erstellung von sicheren und zuverlässigen cloudbasierten Anwendungen anhand der AWS-Technologie zu bestätigen. Weitere Informationen zu AWS-Zertifizierungen finden Sie unter http://aws.amazon.com/certification/.

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

Am Dokument vorgenommene Änderungen

Datum	Beschreibung
Februar 2017	Erstveröffentlichung