Eine Navigationshilfe für den Umgang mit Anforderungen der EU an Datentransfers

7. September 2021

Hinweise

Kunden sind eigenverantwortlich für die unabhängige Bewertung der Informationen in diesem Dokument zuständig. Dieses Dokument: (a) dient rein zu Informationszwecken, (b) spiegelt die aktuellen Produktangebote und Verfahren von AWS wider, die sich ohne vorherige Mitteilung ändern können, und (c) impliziert keinerlei Verpflichtungen oder Zusicherungen seitens AWS und dessen Tochtergesellschaften, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Gewährleistungen, Zusicherungen oder Bedingungen bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden wird durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen zwischen AWS und seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Überblick

Dieses Dokument enthält Informationen über Services und Ressourcen, die Amazon Web Services (AWS) Kunden anbietet, um diesen bei der Bewertung von Datentransfers im Lichte des „Schrems II“-Urteils über die Übertragung personenbezogener Daten, die der Datenschutzgrundverordnung und den anschließenden Empfehlungen des Europäischen Datenschutzausschusses unterliegen, zu helfen. Dieses Dokument beschreibt auch wichtige ergänzende Maßnahmen, die AWS ergriffen hat und die AWS zur Verfügung stellt, um Kundendaten zu schützen.

Einführung

AWS verpflichtet sich, seinen Kunden zu ermöglichen, alle AWS-Services unter Einhaltung der EU-Datenschutzrichtlinien zu nutzen, inklusive der Datenschutz-Grundverordnung (DSGVO). Dieses Papier beschreibt, wie Kunden AWS-Services unter Berücksichtigung der sich schnell entwickelnden Datenschutzlandschaft in der EU infolge des Schrems-II-Urteils und der nachfolgenden Empfehlungen des Europäischen Datenschutzausschusses (EDSA) nutzen können. In diesem Dokument wird Schritt für Schritt erklärt, wie Kunden gemäß des Schrems-II-Urteils und den Empfehlungen des EDSA Bewertungen ihrer Nutzung der AWS-Services durchführen und somit die EU-Datenschutzbestimmungen einhalten können.

Übersicht des Schrems-II-Urteils

Am 16. Juli 2020 hat der Gerichtshof der Europäischen Union (EuGH) ein Urteil (das sogenannte „Schrems II"-Urteil) zur Übermittlung personenbezogener Daten, die der DSGVO unterliegen, außerhalb des Europäischen Wirtschaftsraums (EWR) gefällt. In Schrems-II hat der EuGH geurteilt, dass das EU-US-Datenschutzschild kein gültiger Mechanismus zur Übertragung personenbezogener Daten aus dem EWR in die Vereinigten Staaten mehr ist.

Jedoch bestätigte der EuGH In demselben Urteil, dass Organisationen (vorbehaltlich der Erfüllung bestimmter, nachstehend zusammengefasster Bedingungen) weiterhin Standardvertragsklauseln (engl. „standard contractual clauses", kurz: SCCs) als gültigen Mechanismus für die Übertragung personenbezogener Daten außerhalb des EWR verwenden können. Der EuGH bestätigte, dass Organisationen, die personenbezogene Daten in Länder außerhalb des EWR übermitteln (Datenexporteure), in Zusammenarbeit mit den Empfängern dieser personenbezogenen Daten (Datenimporteure) prüfen müssen, ob für die übermittelten personenbezogenen Daten ein Schutzniveau besteht, das im Wesentlichen dem im EWR durch die DSGVO garantierten Schutzniveau entspricht.

Datenexporteure müssen diese Bewertung auch dann durchführen, wenn Datenexporteure und Datenimporteure SCCs als Basis für die Übertragung verwenden. Bei der Übermittlung personenbezogener Daten, die Kunden mit AWS-Services in ihre AWS-Konten außerhalb des EWR hochgeladen haben (Kundendaten), gelten die Kunden als Datenexporteure und AWS ist Datenimporteur.

In Schrems II bestätigte der EuGH zudem, dass AWS und seine Kunden je nach Ergebnis der obigen Bewertung eventuell „zusätzliche Maßnahmen" (zusätzlich zur Implementierung von SCCs) ergreifen müssen, um ein im Wesentlichen gleichwertiges Schutzniveau für personenbezogene Daten, die in Länder außerhalb des EWR übertragen werden, zu gewährleisten.

Überblick über die Empfehlungen des EDSA

Der EDSA, ein Gremium, welches aus Repräsentanten der Datenschutzbehörden aller EU-Mitgliedstaaten besteht, gab Beispiele zu diesen zusätzlichen Maßnahmen in seinen „Empfehlungen 01/2020 zu Maßnahmen, welche die Übertragungsinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten“ (EDSA-Empfehlungen).

Die EDSA-Empfehlungen enthalten auch Leitlinien für die Beurteilung, ob bei Datenübertragungen außerhalb des EWR nach Schrems II ein im Wesentlichen gleichwertiges Schutzniveau besteht. Die EDSA-Empfehlungen besagen, dass Datenexporteure bei Datenübertragungen die folgende Sechs-Schritte-Bewertung ausführen sollen (EDSA-Datenübertragungsbewertung):

- **Schritt 1:** Erstellen Sie eine Übersicht der internationalen Datentransfers und bewerten Sie, ob die übertragenen Daten adäquat und auf das notwendige limitiert sind.
- **Schritt 2**: Verifizieren Sie, auf welchem Datenübertragungswerkzeug der Datentransfer basiert (beispielsweise verlassen sich Kunden auf die SCCs, um Kundendaten zu übertragen).
- **Schritt 3:** Bewerten Sie die Gesetze oder Praktiken der Drittländer, welche die Wirksamkeit der geeigneten Sicherheitsmaßnahmen des Übertragungswerkzeugs beeinträchtigen können, unter anderem anhand der Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien für Überwachungsmaßnahmen.
- **Schritt 4:** Wenn der Datenexporteur feststellt, dass die Verwendung des Übertragungswerkzeugs allein kein im Wesentlichen gleichwertiges Schutzniveau bieten würde, sind die ergänzenden vertraglichen, technischen oder organisatorischen Maßnahmen zu identifizieren, die erforderlich sind, um das Schutzniveau der übertragenen Daten auf den EWR-Standard der wesentlichen Gleichwertigkeit zu bringen.
- **Schritt 5:** Befolgen Sie jeden formellen Verfahrensschritt, welche die Anwendung Ihrer ergänzenden Maßnahme(n) erfordern könnten.
- **Schritt 6:** Bewerten Sie in angemessenen Abständen das Schutzniveau der Daten neu, welche die Datenexporteure an Drittländer übertragen und überwachen Sie, ob es Entwicklungen gab oder Entwicklungen geben wird, die dies beeinflussen könnten.

Auswirkungen von Schrems II und der EDSA-Empfehlungen auf die Nutzung von AWS-Services

AWS-Kunden können AWS-Services weiterhin nutzen, um Kundendaten unter Einhaltung der Datenschutzgesetze (inklusive DSGVO) außerhalb des EWR zu übermitteln. AWS integriert den AWS-DSGVO-Zusatz zur Datenverarbeitung (auf englisch: „AWS GDPR Data Processing Addendum“, kurz „AWS GDPR DPA“) in die AWS-Service-Bedingungen, was bedeutet, dass der AWS-DSGVO-Zusatz automatisch für alle Kunden gilt, welche AWS-Dienste nutzen, um Kundendaten zu verarbeiten, die der DSGVO unterliegen, wobei AWS der Verarbeiter (wie in der DSGVO definiert) dieser Kundendaten ist.

Bei AWS hat der Schutz der Kundendaten die höchste Priorität. AWS implementiert strenge technische und organisatorische Maßnahmen, um Vertraulichkeit, Integrität und Verfügbarkeit zu schützen, unabhängig von der AWS-Region, welche der Kunde ausgewählt hat.

AWS bietet fortschrittliche Verschlüsselungsservices und Werkzeuge, welche AWS-Kunden verwenden können, um ihre Kundendaten zu schützen. AWS-Kunden können ihre eigenen Chiffrierschlüssel aus einer Reihe von nativen AWS-Lösungen sowie Lösungen von Drittanbietern heraus verwalten. AWS befolgt strenge Richtlinien für den Umgang mit Offenlegungsbegehren von staatlichen Stellen und geht starke vertragliche Verpflichtungen ein, um Kundendaten zu schützen, was im Abschnitt zu Vertraglichen Maßnahmen in diesem Papier genauer erklärt wird.

AWS wird seine Methoden weiter aktualisieren, um den sich entwickelnden Bedürfnissen und Erwartungen von Kunden und Gesetzgebern zu entsprechen und um vollständig alle geltenden Gesetze in jedem Land einzuhalten, in dem AWS operiert.

Weitere Informationen finden Sie im Kundenupdate zum EU-US-Datenschutzschild und im Kundenupdate zu verstärkten Verpflichtungen zum Schutz von Kundendaten.

Wenn Sie Fragen zur Übertragung von Kundendaten nach und aus dem Vereinigten Königreich nach dem Brexit haben, besuchen Sie bitte die AWS- und Brexit -Webseite.

Übersicht über die Transfers von Kundendaten

Dieser Abschnitt hilft Ihnen, Schritt 1 der EDSA-Datenübertragungsbewertung zu erfüllen.

> **Schritt 1:** Erstellen Sie eine Übersicht der internationalen Datentransfers und bewerten Sie, ob die übertragenen Daten adäquat und auf das limitiert sind, was wirklich notwendig ist.

AWS-Vertragspartei

Wie in der AWS Kundenvereinbarung beschrieben, welche die Nutzung von AWS-Services durch AWS-Kunden regelt, ist Amazon Web Services EMEA SARL mit Sitz in Luxemburg die AWS-Vertragspartei, die AWS-Services für Kunden in Europa, dem Nahen Osten und Afrika (außer Südafrika) bereitstellt. Gemäß der AWS-Kundenvereinbarung stellen andere mit AWS verbundene Unternehmen die AWS-Services für andere Kunden außerhalb von Europa, dem Nahen Osten und Afrika bereit.

Wie Kunden Ihre Kundendaten übertragen können

Gemäß des AWS GDPR DPA wählen Kunden die AWS-Region in welcher sie ihre Kundendaten speichern. Kunden können eine Übersicht der verfügbaren AWS-Regionen auf der Website zu Regionen und Availability Zones finden. Gemäß des AWS-DSGVO-Zusatzes zur Datenverarbeitung (AWS GDPR DPA) wird AWS keine Kundendaten außerhalb der vom Kunden gewählten AWS-Region übertragen, es sei denn, es ist zur Erbringung der vom Kunden initiierten AWS-Services erforderlich oder nötig, um Gesetze oder eine gültige und verbindliche Anordnung einer staatlicher Stelle einzuhalten.

Mit AWS bleiben Kunden im Besitz ihrer Kundendaten, sie kontrollieren den Ort der Datenverarbeitung und wer Zugriff auf diese Kundendaten hat. AWS macht transparent, wie AWS-Services Kundendaten verarbeiten. Wie auf der Website zu Datenschutzfunktionen von AWS-Services dargelegt, kann jeder Kunde AWS-Services mit der Gewissheit nutzen, dass Kundendaten in der vom Kunden ausgewählten AWS-Region verbleiben.

Eine kleine Anzahl von AWS-Services beinhaltet die Übertragung von Kundendaten, beispielsweise um diese AWS-Services zu entwickeln und zu verbessern —in diesem Fall können Kunden die Übertragung ablehnen— oder weil die Übertragung ein wesentlicher Bestandteil des AWS-Services ist (wie zum Beispiel bei einem Content-Delivery-Service zur weltweiten Bereitstellung von Inhalten). AWS untersagt den Fernzugriff von AWS-Personal auf Kundendaten, unabhängig vom Zweck des Zugriffs; entsprechend werden AWS-Systeme so entworfen, dass ein solcher Fernzugriff ausgeschlossen wird. Dies beinhaltet Wartungsmaßnahmen an Services, es sei denn, der Zugriff wird von den Kunden beantragt, ist zur Verhinderung von Betrug und Missbrauch oder zur Einhaltung von Gesetzen erforderlich.

Weitere Informationen über die Vorgehensweise von AWS bei der Bearbeitung von Anfragen staatlicher Stellen finden Sie in den Abschnitten Bewertung der Gesetze des Empfängerlandes und Ergänzende Maßnahmen in diesem Dokument.

Unterverarbeitung

Sie können den Ort der Verarbeitung von Kundendaten identifizieren, indem Sie die Website der AWS-Unterverarbeiter aufrufen, wo AWS die Unterauftragnehmer auflistet, die mit der Verarbeitung von Kundendaten im Namen des Kunden beauftragt wurden (Unterverarbeiter).

Die für einen einzelnen Kunden relevanten Unterverarbeiter hängen von der AWS-Region ab, die der Kunde ausgewählt hat, sowie von bestimmten AWS-Services, die der Kunde nutzt.

Es gibt drei Arten von Unterverarbeitern:

- Juristische Einheiten von AWS, welche die Infrastruktur bereitstellen, auf der AWS-Services betrieben werden.
- Juristische Einheiten von AWS, die spezifische AWS-Services unterstützen, wozu eine Verarbeitung der Kundendaten durch diese Einheiten nötig ist.
- Drittparteien, die AWS beauftragt hat, Verarbeitungsaktivitäten für bestimmte AWS-Services bereitzustellen.

AWS aktualisiert die Website der Unterverarbeiter mindestens 30 Tage vor der Beauftragung eines neuen Unterverarbeiters, und wenn Sie die Aktualisierungen abonnieren, werden Sie von AWS per E-Mail über Änderungen dieser Website informiert.

Übertragungswerkzeug

Dieser Abschnitt hilft Ihnen, Schritt 2 der EDSA-Datenübertragungsbewertung zu erfüllen.

> **Schritt 2:** Verifizieren Sie das Übertragungswerkzeug, auf welchem die Übertragung basiert (beispielsweise SCCs).

Wenn Kunden die AWS-Services anweisen, Kundendaten außerhalb des EWR zu übertragen, gemäß dem Abschnitt Übersicht über die Transfers von Kundendaten in diesem Dokument, verwendet AWS die SCCs, um solche Übertragungen zu validieren. Sowohl das Schrems-II-Urteil als auch die EDSA-Empfehlungen bestätigen, dass SCCs ein gültiger Mechanismus zum Übertragen personenbezogener Daten sind, welche der DSGVO außerhalb des EWR unterliegen. AWS-Kunden können darum weiterhin auf die SCCs vertrauen, welche in dem AWS-DSGVO-Zusatz (AWS GDPR DPA) für die Übertragung von Kundendaten in Übereinstimmung mit der DSGVO enthalten sind.

Bewertung der Gesetze und Praktiken des Empfängerlandes

Dieser Abschnitt hilft Ihnen, Schritt 3 der EDSA-Datenübertragungsbewertung zu erfüllen.

> **Schritt 3:** Bewerten Sie die Gesetze oder Praktiken der Drittländer, welche die Wirksamkeit der geeigneten Sicherheitsmaßnahmen des Übertragungswerkzeugs beeinträchtigen können, unter anderem anhand der Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien für Überwachungsmaßnahmen.

Mit AWS können Sie aus einer Reihe von AWS-Services wählen, die Sie „on demand" bereitstellen und konfigurieren können, um Ihre eigenen Produkt- und Serviceangebote zu entwickeln. AWS gibt Ihnen zu jeder Zeit die vollständige Kontrolle über Ihre Kundendaten durch einfache aber mächtige Werkzeuge, die es Ihnen ermöglichen, zu bestimmen, wo Ihre Kundendaten gespeichert sind und um Ihre Kundendaten bei der Übertragung und im Ruhezustand zu sichern. Sie sind am besten in der Lage, die Gesetze zu identifizieren, die für Kundendaten gelten, denn Sie bestimmen, wie, wo und warum Sie Kundendaten verarbeiten, welche Sie mit AWS-Services nutzen.

Wenn Sie Fragen zu den US-Überwachungsgesetzen, einschließlich Abschnitt 702 des Foreign Intelligence Surveillance Act 1978 (FISA), haben, lesen Sie die *Informationen über die USA Datenschutzsicherheitsmaßnahmen für SCCs und andere EU-Rechtsgrundlagen für Datenübermittlungen zwischen der EU und den USA nach Schrems II*, ein „Whitepaper", das das US-Handelsministerium, das US-Justizministerium und das Office of the Director of National Intelligence im September 2020 gemeinsam herausgegeben haben und in dem die Grenzen und Sicherheitsmaßnahmen in Bezug auf ihren Datenzugriff als Reaktion auf das Schrems-II-Urteil im Einzelnen aufgeführt sind.

Das „Whitepaper" besagt, dass für viele Unternehmen das Problem des Zugriffs auf ihre personenbezogenen Daten im Namen der nationalen Sicherheit unwahrscheinlich ist, weil diese Daten für die nationalen Sicherheitsbehörden nicht von Interesse wären. Das „Whitepaper" besagt, dass:

- Unternehmen, die mit „gewöhnlichen Geschäftsinformationen wie Mitarbeiter-, Kunden- oder Verkaufsdaten hantieren, keinen Grund haben, zu befürchten, dass US-Geheimdienste versuchen würden, diese Daten zu sammeln."
- „Die theoretische Möglichkeit, dass US-Geheimdienste ohne das Wissen des Unternehmens einseitig auf Daten zugreifen könnten, die aus der EU übertragen werden, unterscheidet sich nicht von der theoretischen Möglichkeit, dass staatliche Geheimdienste, inklusive jene der EU-Mitgliedstaaten, oder eine

private Einrichtung, die rechtswidrig handelt, auf diese Daten zugreifen könnten." Das „Whitepaper" sagt auch, dass solch ein Zugriff auf Daten überall auf der Welt stattfinden könnte, nicht nur in den USA.

- Es gibt individuelle Rechtsbehelfe, auch für EU-Bürger, für Verstöße gegen FISA-Abschnitt 702 durch Maßnahmen, auf die das Gericht im Schrems-II-Urteil nicht eingegangen ist, einschließlich FISA-Bestimmungen, die private Klagen auf Schadenersatz und Strafschadensersatz ermöglichen.
- Der FISA-Abschnitt 702 wurde um zusätzliche Datenschutzsicherheitsmaßnahmen ergänzt, einschließlich der Änderungen von 2018, mit denen Folgendes hinzugefügt wurde: (i) Abfrageverfahren (zusätzlich zu den Verfahren zur gezielten Erfassung und Minimierung); (ii) Bereitstellungen zur Verbesserung der Aufsicht durch das Privacy and Civil Liberties Oversight Board; (iii) Anforderungen an Datenschutz- und Bürgerrechtsbeauftragte für zusätzliche relevante Agenturen; (iv) erweiterter Schutz von Hinweisgebern für Auftragnehmer; und (v) Transparenzanforderungen, einschließlich Bestimmungen zur Offenlegung der Anzahl der Ziele des FISA Abschnitts 702.

Unabhängig von den geltenden Gesetzen prüft AWS jede Anfrage der Strafverfolgungsbehörden einzeln und unabhängig, egal aus welchem Land diese stammt. Amazon hat in der Vergangenheit immer wieder förmlich Einspruch gegen behördliche Anfragen nach Kundendaten erhoben, die es für zu weitreichend oder anderweitig unangemessen hält. AWS wird solche Anfragen weiterhin gründlich prüfen, auch solche, die im Widerspruch zu lokalen Gesetzen wie der DSGVO stehen, und in begründeten Fällen Einspruch erheben.

AWS ergreift außerdem zusätzliche Maßnahmen, um die Wirksamkeit der SCCs zu unterstützen, und stellt diese zur Verfügung, wie im Abschnitt Zusätzliche Maßnahmen dieses Whitepapers beschrieben. Zu diesen zusätzlichen Maßnahmen gehört die Zusatzvereinbarung zur AWS GPDR DPA, in der sich AWS vertraglich verpflichtet, Anfragen von Strafverfolgungsbehörden abzulehnen, wie im Abschnitt Vertragliche Maßnahmen dieses Whitepapers näher erläutert wird.

Die EDSA-Empfehlungen ermöglichen es AWS-Kunden auch, die praktischen Erfahrungen von AWS „mit einschlägigen früheren Fällen von Zugangsanfragen von Behörden" außerhalb des EWR zu berücksichtigen.

Um AWS-Kunden bei der Bewertung dieser früheren Anfragen zu helfen, veröffentlicht AWS auf der Webseite für Informationsanfragen der Strafverfolgungsbehörden („Law Enforcement Information Requests") regelmäßig Berichte über die Art und den Umfang der Anfragen von Strafverfolgungsbehörden, die bei AWS eingehen. Die in den Berichten über die Informationsanfragen enthaltenen Informationen zeigen, dass AWS nur sehr selten Kundendaten als Reaktion auf staatliche Informationsanfragen offenlegt.

Zusätzliche Maßnahmen

Dieser Abschnitt hilft Ihnen, Schritt 4, 5 und 6 der EDSA-Datenübertragungsbewertung zu erfüllen.

> **Schritt 4:** Wenn die Rechtsvorschriften oder Praktiken der Drittländer bedeuten, dass die Verwendung des Übertragungswerkzeugs allein kein im Wesentlichen gleichwertiges Schutzniveau bieten würde, sind die ergänzenden vertraglichen, technischen oder organisatorischen Maßnahmen zu identifizieren, die erforderlich sind, um das Schutzniveau der übertragenen Daten auf den EWR-Standard der wesentlichen Gleichwertigkeit zu bringen.
>
> **Schritt 5:** Befolgen Sie jeden formellen Verfahrensschritt, welche die Anwendung Ihrer ergänzenden Maßnahme erfordern könnte.
>
> **Schritt 6:** Bewerten Sie in angemessenen Abständen das Schutzniveau der Daten neu, welche die Exporteure an Drittländer übertragen und überwachen Sie, ob es Entwicklungen gab oder Entwicklungen geben wird, die dies beeinflussen könnten.

Die EDSA-Empfehlungen enthalten eine nicht erschöpfende Liste zusätzlicher Maßnahmen, die AWS und seine Kunden ergreifen können, je nach dem Ergebnis der im Abschnitt Überblick über die EDSA-Empfehlungen dieses Whitepapers beschriebenen Bewertung der Datenübertragung durch die Kunden.

Diese zusätzlichen Sicherheitsmaßnahmen fallen unter die folgenden drei Kategorien:

- ***Technische Maßnahmen***, wie Verschlüsselung und Logging.
- ***Vertragliche Schutzmaßnahmen,*** einschließlich Verpflichtungen in Bezug auf Datenanfragen von Strafverfolgungsbehörden, wie sie AWS in der AWS-Zusatzvereinbarung macht
- ***Organisatorische Maßnahmen,*** bestehend aus internen Richtlinien und Standards, Maßnahmen zur Minimierung der Datenerfassung und -speicherung sowie der Annahme von Verhaltenskodizes

In diesem Abschnitt werden die wichtigsten technischen, vertraglichen und organisatorischen Zusatzmaßnahmen dargelegt, die AWS ergreift und zur Verfügung stellt, um Kundendaten zu schützen und die Wirksamkeit der SCCs zu unterstützen. AWS wird dieses Dokument im Zuge der der Weiterentwicklung der zusätzlichen Maßnahmen aktualisieren.

Technische Maßnahmen

Kontrolle durch den Kunden

Sie haben vollständige Kontrolle über Ihre Kundendaten durch einfache, aber leistungsstarke AWS-Services und -Werkzeuge, mit denen Sie bestimmen können, wo die Kundendaten gespeichert werden, wie sie gesichert werden und wer Zugriff hat.

Modell der geteilten Verantwortung

AWS arbeitet mit einem Modell der geteilten Verantwortung, bei dem die Verantwortung für die Sicherheit und die Einhaltung der Vorschriften zwischen AWS und den Kunden aufgeteilt wird. Dies geschieht auf der Grundlage der Funktionsweise der AWS-Services und dem Grad der Kontrolle, den jede Partei über die AWS-Dienste hat. Im Rahmen des Modells der geteilten Verantwortung ist AWS für die Bereitstellung einer sicheren Infrastruktur und sicherer Services verantwortlich (Sicherheit „VON“ der Cloud), während die Kunden für die Entwicklung und Sicherung ihrer Anwendungen und Lösungen verantwortlich sind, die sie in der AWS Cloud bereitstellen möchten (Sicherheit „IN“ der Cloud).

Für die Sicherheit der Cloud setzt AWS verantwortungsbewusste und hoch entwickelte technische und physische Kontrollen und Prozesse ein, die den unbefugten Zugriff auf oder die Offenlegung von Kundendaten verhindern sollen (wie durch die auf der AWS-Compliance-Programm-Website beschriebenen Compliance-Programme dargelegt).

Für die Sicherheit in der Cloud stellt AWS Produkte, Werkzeuge und Services zur Verfügung, die Sie für die Entwicklung und Sicherung Ihrer Anwendungen und Lösungen nutzen können. Im weiteren Verlauf dieses Abschnitts stellt AWS Beispiele für solche Schlüssel-Produkte, -Werkzeuge und -Services vor. Unter AWS Well-Architected finden Sie weitere Informationen zu diesen Produkten, Werkzeugen und Services.

Verschlüsselung

Die Verschlüsselung (inklusive der Verwaltung von Verschlüsselungsschlüsseln) ist eine wichtige technische zusätzliche Maßnahme, die in den EDSA-Empfehlungen beschrieben wird. AWS bietet fortschrittliche Verschlüsselungs-Services und -Werkzeuge, welche Sie verwenden können, um ihre Kundendaten zu schützen.

Sie können Ihre eigenen Verschlüsselungsschlüssel aus einer Reihe von nativen AWS-Lösungen oder Lösungen von Drittanbietern heraus verwalten. AWS Key Management Service (KMS) ist ein verwalteter Service, der Ihnen die Erstellung und Kontrolle Ihrer Verschlüsselungsschlüssel erleichtert und zum Schutz der Sicherheit Ihrer Schlüssel FIPS-140-2-zertifizierte Hardware-Sicherheitsmodule (HSMs) einsetzt.

Alle Anfragen zur Verwendung von Schlüsseln in AWS KMS werden in AWS CloudTrail protokolliert, sodass Kunden nachvollziehen können, wer welchen Schlüssel in welchem Kontext und wann verwendet hat. Die in AWS CloudTrail protokollierten Ereignisdaten können nicht geändert werden. AWS KMS ist so konzipiert, dass weder AWS (einschließlich AWS-Mitarbeiter) noch Drittanbieter von AWS die Möglichkeit haben, die Primärschlüssel der Kunden in einem unverschlüsselten Format abzurufen, anzuzeigen oder weiterzugeben.

Das AWS Nitro System

Das AWS Nitro System ist die Basis-Plattform für alle modernen Amazon Elastic Compute Cloud (Amazon EC2) Instanzen und bietet zusätzliche Vertraulichkeit und Datenschutz für Kundenanwendungen. Mit eigens entwickelter Hardware, Firmware und Software bietet das AWS Nitro System einzigartige und branchenführende Sicherheit und Isolation, indem Virtualisierungsfunktionen für Speicher- und Netzwerkzugriffe auf dedizierte Hardware und zugehörige Firmware ausgelagert werden.

Das AWS Nitro System ist außerdem so entwickelt, dass kein AWS-Mitarbeiter Zugang hat. Mit dem AWS Nitro System gibt es für kein System und keine Person die Möglichkeit, sich bei EC2-Servern (der zugrunde liegenden Host-Infrastruktur) anzumelden, den Speicher von EC2-Instanzen zu lesen oder auf Daten zuzugreifen, die im Instance-Speicher und in verschlüsselten Amazon Elastic Block Store (Amazon EBS) Volumes gespeichert sind.

Vertragliche Maßnahmen

AWS-DSGVO-Zusatzvereinbarung zur Datenverarbeitung (AWS GDPR DPA)

In der AWS-DSGVO-Zusatzvereinbarung zur Datenverarbeitung (auf englisch: „AWS GDPR Data Processing Addendum“, kurz „AWS GDPR DPA“) geht AWS vertragliche Verpflichtungen über die Maßnahmen ein, die ergriffen und verfügbar gemacht werden, um Kundendaten zu schützen. Beispielsweise verpflichtet sich AWS vertraglich:

(i) Zur Implementierenung technischer Maßnahmen zum Schutz des AWS-Netzwerks

(ii) Zum Unterstützen der Kunden bei der Einhaltung ihrer Sicherheitsverpflichtungen gemäß DSGVO durch Anbieten von Werkzeugen und Funktionalitäten

(iii) Zur Bereitstellung von Drittanbieter-Zertifizierungen und (Revisions-) Prüfungs-Berichten, damit Kunden die Einhaltung der AWS GDPR DPA durch AWS überprüfen können

Zusatzvereinbarung

AWS hat eine weitere Zusatzvereinbarung zur AWS GDPR DPA veröffentlicht, welche vertragliche Verpflichtungen enthält, die Kunden als ergänzende vertragliche Maßnahmen gemäß der EDSA-Empfehlungen nutzen können. In dieser Zusatzvereinbarung verpflichtet sich AWS:

(i) alle angemessenen Anstrengungen zu unternehmen, um staatliche Stellen, die Kundendaten anfordern, an den jeweiligen Kunden zu verweisen

(ii) den betreffenden Kunden unverzüglich über die Anfrage zu informieren, sofern dies gesetzlich zulässig ist

(iii) zu weit gehende oder unangemessene Anfragen anzufechten, einschließlich der Fälle, in denen die Anfrage im Widerspruch zu EU-Recht steht

AWS verpflichtet sich außerdem, dass AWS, wenn es nach Ausschöpfung der vorgenannten Schritte weiterhin gezwungen ist, Kundendaten offen zu legen, nur die Mindestmenge an Kundendaten offen legt, die zur Erfüllung der Anfrage erforderlich ist.

Um Kunden bei der Bewertung der Gesetze von Empfängerländern zu unterstützen (siehe Bewertung der Gesetze und Praktiken des Empfängerlandes in diesem Whitepaper), garantiert AWS, dass es keinen Grund zu der Annahme hat, dass die für AWS oder seine Unterverarbeiter geltende Gesetzgebung, auch in einem Land, in das Kundendaten übertragen werden, AWS daran hindert, seine Verpflichtungen gemäß der AWS GDPR oder der Zusatzvereinbarung zu erfüllen.

AWS verpflichtet sich außerdem dazu, jede Änderung der Rechtsvorschriften, die sich wesentlich auf die Erfüllung der Verpflichtungen von AWS auswirken könnte, unverzüglich zu melden. Weitere Informationen finden Sie unter AWS und EU-Datenübertragung: Verstärkte Verpflichtungen zum Schutz von Kundendaten.

Organisatorische Maßnahmen

Prozesse

AWS verfügt über interne Prozesse für den Umgang mit behördlichen Anfragen nach Kundendaten, und unabhängig von der Quelle der Anfrage oder den geltenden Gesetzen prüft AWS jede behördliche Anfrage einzeln und unabhängig in Übereinstimmung mit seinen Strafverfolgungsrichtlinien und den Verpflichtungen in der AWS-Zusatzvereinbarung. AWS schränkt Anfragen von Strafverfolgungsbehörden auf Kundendaten aus allen Ländern, einschließlich der Vereinigten Staaten, rigoros ein oder lehnt sie gänzlich ab, wenn sie zu weit gefasst sind oder AWS einen angemessenen Grund dafür hat.

Berichte zu Informationsanforderungen

AWS weiß, dass Transparenz für seine Kunden wichtig ist. Deshalb veröffentlicht AWS auf der Webseite für Informationsanfragen der Strafverfolgungsbehörden regelmäßig einen Bericht über die Art und den Umfang der bei AWS eingehenden behördlichen Informationsanfragen (IRR). Mit dem Bericht für Juli-Dezember 2020 hat AWS als organisatorische Zusatzmaßnahme ein neues IRR-Format eingeführt, das mehr Informationen liefert über die Arten von Anfragen von staatlichen Stellen, die AWS erhält, sowie über die Herkunftsländer dieser Anfragen.

Um dieses neue IRR-Format zu verwenden, siehe den Amazon-Bericht zu Informationsanfragen. Die in den IRR bereitgestellten Informationen zeigen, dass die Offenlegung von Kundendaten durch AWS als Reaktion auf staatliche Auskunftsanfragen sehr selten ist.

Weitere Ressourcen

Damit Sie besser verstehen, wie Sie Ihre Datenschutzanforderungen erfüllen können, sollten Sie die auf der AWS-Website veröffentlichten Whitepapers zu Risiken, Compliance und Sicherheit, Bewährte Methoden, Checklisten und Orientierungshilfen lesen. Dieses Material kann auf den Websites AWS Compliance und AWS Cloud-Sicherheit gefunden werden.

Dokumentversionen

Datum	Beschreibung
7. September 2021	Erstveröffentlichung