Unterstützung von Kunden im Rahmen der DiGAV

FAQs

6.10.2021

Notices

Sind die AWS-Dienste DSGVO-konform?
Alle AWS-Dienste können in Übereinstimmung mit der DSGVO verwendet werden. Das bedeutet, dass Kunden nicht nur von allen Maßnahmen profitieren, die AWS bereits ergreift, um die Sicherheit der AWS-Services aufrechtzuerhalten, sondern auch, dass Kunden AWS-Dienste als wichtigen Teil ihrer DSGVO-Compliance-Pläne einsetzen können. Weitere Details finden Sie in unserem DSGVO-Zentrum.

Verlangt die DiGAV, dass personenbezogene Daten nur innerhalb des EWR verarbeitet werden dürfen?
Kunden, die eine Erstattungsfähigkeit nach dem Digitalen-Versorgungs-Gesetz (DVG) und der Digitalen-Gesundheits-Anwendungs-Verordnung (DiGAV) anstreben, müssen nachweisen, dass die personenbezogenen Daten innerhalb des EWR oder in Ländern mit einem Angemessenheitsbeschluss der EU-Kommission verarbeitet werden.

Können AWS-Dienste DiGAV-konform genutzt werden?
Ja. Je nach der vom Kunden gewählten Architektur und den ausgewählten AWS-Diensten ist es möglich, AWS-Dienste in Übereinstimmung mit den DiGAV-Anforderungen zu nutzen. AWS bestimmt nicht den Standort der Kundendaten und verarbeitet Daten nur auf der Grundlage der dokumentierten Weisungen seiner Kunden. Die Kunden behalten die vollständige Kontrolle und Besitz an ihren Daten, wenn sie die Region wählen, in der sich ihre Daten physisch befinden. AWS-Kunden, die an der Entwicklung oder dem Betrieb von Anwendungen unter der DiGAV interessiert sind, können AWS-Regionen und -Dienste auswählen - einschließlich in der Region AWS Europe (Frankfurt am Main) in Deutschland-, um die Anforderungen der DiGAV zu erfüllen.

Welche AWS-Dienste kann ich nutzen, um Daten nur innerhalb des EWR zu verarbeiten?
Kunden finden Informationen zu den Datenschutzfunktionen der AWS-Dienste, um festzustellen, welche AWS-Dienste ohne Datenübertragung aus der/den vom Kunden ausgewählten AWS-Region(en) genutzt werden können. Durch die Auswahl von AWS-Diensten, die keine Kundendaten übertragen und die ordnungsgemäße Konfiguration dieser Dienste für die Nutzung aus AWS-Regionen, die sich innerhalb des EWR befinden, können Kunden die Verarbeitung von Daten ausschließlich im EWR ermöglichen. Um eine angemessene Konfiguration zu gewährleisten, können technische Maßnahmen (SCPs und andere) eingerichtet werden, die die Nutzung von AWS-Ressourcen in Regionen außerhalb des EWR blockieren. Bitte beachten Sie den DiGAV Blueprint.

Wie kann ich AWS-Dienste nutzen, sodass personenbezogene Daten nicht außerhalb des EWR verarbeitet werden?
Kunden wählen die AWS-Region aus, in der ihre Kundendaten gespeichert werden sollen. AWS wird diese Kundendaten nicht außerhalb der vom Kunden gewählten AWS-Region verarbeiten, es sei denn, dies ist zur Aufrechterhaltung oder Bereitstellung der AWS-Dienste oder zur Einhaltung von Gesetzen oder einer verbindlichen Anordnung einer staatlichen Stelle erforderlich. Des Weiteren, verbieten wir - und unsere Systeme sind auf die Verhinderung ausgelegt - den Fernzugriff von AWS-Mitarbeitern auf Kundendaten zu jeglichem Zweck, einschließlich der Wartung der Dienste, es sei denn, der Zugriff wird vom Kunden angefordert, ist zur Verhinderung von Betrug und Missbrauch oder zur Einhaltung von Gesetzen erforderlich.

Einer kleinen Anzahl von AWS-Diensten ist die Übermittlung von Kundendaten inhärent - zum Beispiel, um diese Dienste zu entwickeln und zu verbessern (wobei die Kunden die Möglichkeit haben, der Datenübermittlung zu widersprechen) oder weil die Übermittlung ein wesentlicher Bestandteil des Dienstes ist (z. B. bei einem Content Delivery Dienst). Welche AWS-Dienste ohne die Übermittlung von

Daten aus der/den vom Kunden ausgewählten AWS-Region(en) genutzt werden, entnehmen Sie bitte den Datenschutzfunktionen der AWS-Dienste. Durch die Auswahl von AWS-Dienste, die keine Kundendaten übertragen sowie die Auswahl von AWS-Regionen, die sich innerhalb des EWR befinden, können Kunden eine reine EWR-Datenverarbeitung ermöglichen.

Welche Dokumentation kann ich verwenden, um gegenüber Aufsichtsbehörden oder Kunden nachzuweisen, dass Daten innerhalb des EWR verarbeitet werden, wenn ich AWS-Dienste verwende?
Es liegt in der Verantwortung des Kunden, AWS-Dienste korrekt zu konfigurieren, um eine Datenverarbeitung in einer Region außerhalb des EWR zu vermeiden. AWS stellt Werkzeuge zur Verfügung, um dies sicherzustellen, wie im DiGAV Blueprint beschrieben, der für diese Maßnahmen auf die Dienst-Dokumentation verweist.

Welche Infrastruktur stellt AWS innerhalb des EWR zur Verfügung?
Einen Überblick über die globale AWS-Infrastruktur und Regionen, Edge-Standorte und andere Infrastrukturen innerhalb des EWR finden Sie hier.

Kann der AWS-Support genutzt werden, wenn eine reine EWR-Verarbeitung beabsichtigt ist?
Ja. Wir verbieten den Fernzugriff von AWS-Mitarbeitern auf Kundendaten zu jeglichem Zweck, einschließlich der Servicewartung, und unsere Systeme sind so konzipiert, dass dies verhindert wird, es sei denn, der Zugriff wird vom Kunden angefordert, ist zur Verhinderung von Betrug und Missbrauch oder zur Einhaltung von Gesetzen erforderlich.

Das Deutsche Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) verlangt von internationalen Cloud-Anbietern wie AWS Zusagen zum Umgang mit ausländischen Strafverfolgungsanfragen (z. B. nach dem CLOUD Act). Bietet AWS solche Zusagen an?
Ja. Der Schutz von Kundendaten hat für uns höchste Priorität. AWS hat vor kurzem unsere Verpflichtung zum Schutz von Kundendaten vor Anfragen von Strafverfolgungsbehörden innerhalb und außerhalb des EWR durch ein Supplementary Addendum zu unserem AWS GDPR DPA verstärkt.
Wir wissen, dass Transparenz für unsere Kunden wichtig ist. Deshalb veröffentlichen wir regelmäßig auf der Webseite für Informationsanfragen von Amazon einen Bericht über die Art und den Umfang der Informationsanfragen, die wir erhalten und wie AWS darauf reagiert.Weitere Informationen über den CLOUD Act und die Auswirkungen für AWS-Kunden finden Sie hier.

Welche Unterauftragsverarbeiter verwendet AWS zur Datenverarbeitung?
Eine Liste der AWS-Unterauftragsverarbeiter finden Sie hier.

Der BfArM-Leitfaden empfiehlt bei der Nutzung von Cloud-Anbietern die Verschlüsselung mit Customer Managed Encryption Keys (CMEK oder CMK). Wie kann dies bei AWS umgesetzt werden?
AWS bietet eine Reihe von fortschrittlichen Verschlüsselungs- und Schlüsselverwaltungsdiensten, die Kunden zum Schutz ihrer Inhalte nutzen können. Kunden können auch aus einer Reihe von unterstützten Verschlüsselungslösungen von Drittanbietern wählen, wenn sie AWS-Dienste nutzen. Verschlüsselte Inhalte sind ohne die entsprechenden Entschlüsselungsschlüssel nutzlos.

Eine Liste der AWS-Dienste, die Verschlüsselung unterstützen, finden Sie in den Datenschutzfunktionen der AWS-Dienste. Schlüsselverwaltungsdienste wie KMS und CloudHSM ermöglichen es Kunden, ihre Verschlüsselungsschlüssel effektiv und sicher zu verwalten. Bitte setzen Sie sich mit Ihrem AWS-Kundenteam in Verbindung (oder kontaktieren Sie uns hier), um eine Anleitung für eine CMEK-basierte Verschlüsselungslösung auf AWS zu erhalten.