DIERKS + COMPANY

Q+A für AWS-Kunden Healthcare

Q&A zur Speicherung und Verarbeitung von Sozial- und Gesundheitsdaten in der AWS-Cloud durch Kunden im Healthcare-Bereich

Cloud geht nicht – gibt's nicht.

Prof. Dr. Dr. Christian Dierks
Ira Mießler, LL.M.

Datum:
09.03.2023

DIERKS + COMPANY

Amazon Web Services EMEA SARL (AWS) ist Anbieter einer Palette, Cloud-basierter Services, Speicher, Datenbanken, Analyse, Netzwerke, Mobile, Entwicklertools, Verwaltungstools, IoT-Sicherheits- und Unternehmenswerkzeuge, bei deren Nutzung die zu verarbeitenden Daten auch Personenbezug haben können. Für Anwender im Healthcare-Bereich wie z. B. Krankenkassen und Krankenhäuser, sind die von AWS angebotenen Cloud Services von Interesse. Wesentliche Rechtsgrundlagen der Kundenbeziehung sind das *AWS Customer Agreement*, die *Service Terms* und das *AWS GDPR DATA PROCESSING ADDENDUM (DPA)* sowie das *Supplementary Addendum* zum DPA. AWS bietet im Rahmen eines *Shared Responsibility* Modells[1] verschiedene Sicherheitsmaßnahmen zum Schutz der Daten ihrer Kunden, die sich an den Bedürfnissen des Kunden ausrichten können.

Die folgende Aufstellung soll Krankenkassen und anderen Anwendern im Healthcare-Bereich, die den Einsatz von AWS Services erwägen, die wichtigsten Fragen im Hinblick auf einen datenschutzkonformen Einsatz von AWS-Services beantworten. Sie soll etwaige Einzelfallbewertungen unterstützen.

Der Begriff der **Cloud** (auch Cloud-Dienste oder Cloud-Computing) wird nicht immer einheitlich verwendet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat – aufbauend auf der Definition der US-amerikanischen Standardisierungsstelle NIST (*National Institute of Standards and Technology*), die auch von der ENISA (*European Network and Information Security Agency*) genutzt wird – folgende Definition für den Begriff „Cloud Computing" festgelegt: *„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software"*. Wesentlich ist, dass Unternehmen durch Auslagerung in die „Cloud" insbesondere IT-Ressourcen nicht mehr selbst vorhalten müssen, sondern auf spezialisierte Anbieter zurückgreifen und so die Kostenbasis für den IT-Bereich reduzieren, die Agilität, Sicherheit und Innovationsfähigkeit steigern können.[2] In einem reinen IaaS-Angebot z. B. nutzt ein Krankenhaus IT-Infrastrukturen des Cloud-Anbieters, d. h. im Wesentlichen Gebäude, Server, Virtualisierungsschichten und Storagekomponenten. Die vom Cloud-Anbieter eingesetzten Komponenten werden von ihm automatisiert und einheitlich für alle Kunden verwaltet und aktualisiert.

---

1 AWS betreibt ein Modell der gemeinsamen Verantwortung, das Sicherheits- und Compliance-Verantwortlichkeiten zwischen AWS und Kunden basierend auf der Funktionsweise von AWS-Services und dem Grad der Kontrolle, den jede Partei im Rahmen der AWS-Services hat, aufteilt. Im Rahmen des Modells der gemeinsamen Verantwortung ist AWS für die Bereitstellung sicherer Infrastruktur und Dienste (Sicherheit "DER" Cloud), während Kunden für die Architektur und Sicherung ihrer Anwendungen und Lösungen verantwortlich sind, die sie in der AWS Cloud bereitstellen möchten (Sicherheit „IN" der Cloud).

2 Vgl. Dahmen, BKR, 2019, 533, 536.

DIERKS + COMPANY

1. Fragen zum regulatorischen Kontext

1.1 Ist es in Deutschland erlaubt, Gesundheits- und Sozialdaten in der Cloud zu speichern bzw. zu verarbeiten?

Kurzantwort: Ja – es sind jedoch Besonderheiten zu beachten.

Erläuterung:

Um diese Frage zu beantworten, ist eine kurze Erklärung zu den unterschiedlichen Begriffen erforderlich.

Gesundheitsdaten sind eine besondere Kategorie personenbezogener Daten nach Art. 9 Abs. 1 DSGVO. Gemäß Art. 4 Nr. 15 DSGVO sind Gesundheitsdaten „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen". Der Begriff ist weit auszulegen und umfasst nicht nur „medizinische Daten".[3]

Sozialdaten sind personenbezogene Daten (vgl. Art. 4 Nr. 1 DSGVO), die von einer in § 35 SGB I genannten Stelle (z. B. Leistungsträger) im Hinblick auf ihre Aufgaben verarbeitet werden, vgl. § 67 Abs. 2 S. 1 SGB X.

Von Gesundheits- und Sozialdaten zu unterscheiden sind jedoch andere im Healthcare-Bereich verarbeitete Daten, die z. B. keinen Gesundheits- oder Sozialbezug aufweisen. Hierzu gehören etwa Daten, die bereits keinen Personenbezug aufweisen (z. B. Einkaufsdaten) oder Daten, die sich zwar auf Personen nicht jedoch auf Patienten oder Versicherte beziehen (z. B. Daten von Mitarbeitenden). Für solche Daten gelten die Anforderungen des Gesundheitsdatenschutzes nicht. Die an diese Daten zu stellenden Anforderungen werden in diesem Q&A nicht betrachtet.

Ein Verbot der Speicherung, also Verarbeitung, von Gesundheits- oder Sozialdaten in der Cloud, kennen die gesetzlichen Vorschriften nicht. Krankenkassen müssen bei der Beauftragung von Cloud-Dienstleistern jedoch die Vorschriften des Art. 9 Abs. 2 lit. b DSGVO i. V. m. den Vorschriften der Sozialgesetzbücher sowie die Einhaltung des Art. 28 DSGVO (siehe dazu Frage 1.2ff.) und des Kapitels V der DSGVO (vgl. hierzu Abschnitt 3) beachten. Aus im Einzelfall anzuwendenden (landes- und) gesundheitsrechtlichen Spezialvorschriften können sich möglicherweise Einschränkungen in der Wahl der Dienstleister ergeben.

1.2 Erfüllt das DPA von AWS die Anforderungen des Art. 28 DSGVO?

Kurzantwort: Ja.

---

[3] Weichert, in Kühling/Buchner, DSGVO, 2. Aufl. 2020, Art. 4 Nr. 15 Rn. 1.

DIERKS + COMPANY

Erläuterung:

Auftraggeber können daher durch die den Abschluss des AWS Customer Agreements einschließlich des AWS GDPR Data Processing Addendums die gesetzlichen Anforderungen an einen Auftragsverarbeitungsvertrag mit einem Cloud-Provider erfüllen.

Der Auftragsverarbeitungsvertrag (*AWS GDPR Data Processing Addendum,* DPA), den AWS mit ihren Kunden bei Abschluss des *AWS Customer Agreements* abschließt, enthält alle Regelungen, die ein Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DSGVO enthalten muss. Im Einzelnen:

- Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen (Art. 28 Abs. 3 S. 1 DSGVO) sind in Ziffer 1.3 des DPA geregelt.
- Die Gebundenheit von AWS als Auftragsverarbeiter an die Weisungen des Verantwortlichen gemäß Art. 28 Abs. 3 S. 2 lit. a DSGVO findet sich in Ziffer 2. des DPA.
- Ziffern 3. und 4. regeln die Vertraulichkeit der Verarbeitung gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO.
- Zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 28 Abs. 3 S. 2 lit. c DSGVO verpflichtet sich AWS unter Verweis auf die AWS Security Standards in Ziffer 5. des DPA; daneben stehen dem Kunden gemäß Ziffer 8. des DPA weitere optionale Sicherheitsfeatures zur Verfügung.
- Regelungen zur Beauftragung weiterer Auftragnehmer finden sich in Einklang mit Art. 28 Abs. 2, Abs. 3 S. 2 lit. d, Abs. 4 DSGVO in Ziffer 6. des DPA. AWS bietet eine Übersichtsseite mit den in Anspruch genommenen „Sub-Processors" sowie ihren Aufgaben in Bezug auf bestimmte Services. Diese Webseite bietet Kunden auch die Möglichkeit, E-Mail-Benachrichtigungen zu abonnieren, wenn sich die Liste der Sub-Processors ändert. Kunden werden daher über alle Subunternehmen informiert, die Zugang zu kundeneigenen Inhalten haben, die auf AWS hochgeladen werden.
- Gemäß Ziffer 7. des DPA wird AWS den Kunden bei der Durchsetzung der Rechte der betroffenen Personen gemäß Art. 28 Abs. 3 S. 2 lit. e DSGVO unterstützen.
- In Ziffer 9. des DPA ist die Unterstützungspflicht von AWS im Falle einer Verletzung des Schutzes personenbezogener Daten aus Art. 28 Abs. 3 S. 2 lit. f geregelt. Die weitere sich hieraus ergebende Pflicht, den Kunden bei einer Datenschutzfolgenabschätzung zu unterstützen, findet sich in Ziffer 10.4 des DPA.
- Ziffer 14 regelt Rückgabe oder Löschung aller Daten nach Beendigung des Vertragsverhältnisses im Einklang mit Art. 28 Abs. 3 S. 2 lit. g DSGVO.
- Ziffern 10. und 11. ermöglichen dem Kunden den Nachweis und die Überprüfung der Einhaltung der Pflichten aus Art. 28 gemäß Art. 28 Abs. 3 S. 2 lit. h DSGVO.

Darüber hinaus hat AWS bereits die im September 2021 veröffentlichten neuen Standardvertragsklauseln (*Controller to Processor* und *Processor to Processor*) in ihr DPA übernommen, sofern diese Anwendung finden sollten.

DIERKS + COMPANY

1.3 Entsprechen die Vertraulichkeitsverpflichtungen von AWS und ihren Unterverarbeitern den gesetzlichen Anforderungen?

Kurzantwort: Ja.

Erläuterung:

Nach Art. 28 Abs. 3 S. 2 lit. b DSGVO muss der Auftragsverarbeiter gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Vorgaben zu Art, Inhalt und Form enthält das Gesetz nicht. Gemäß Ziffer 3 des DPA werden Kundendaten vertraulich behandelt. Mitarbeiter von AWS werden gemäß Ziffer 4 des DPA zur Vertraulichkeit verpflichtet. Gemäß Ziffer 6.2 (ii) des DPA verpflichtet sich AWS, dass Unterverarbeitern die gleichen vertraglichen Verpflichtungen auferlegt werden, denen AWS gemäß DPA unterliegt. Dies gilt auch für die Vertraulichkeitsverpflichtung. Weitere Maßnahmen stützen die Vertraulichkeit zusätzlich: Gemäß Annex 1 zum DPA, den AWS Security Standards, wird der Zugang zu Kundendaten durch AWS-Mitarbeiter oder Unterverarbeiter u. a. durch ID-Kontrollen und Rechte-Rollen-Konzepte für Datenzugriff limitiert und überprüft. Die von AWS getroffenen Maßnahmen sind folglich ausreichend, um die gesetzlichen Anforderungen an Vertraulichkeitsverpflichtungen aus Art. 28 Abs. 3 S. 2 lit. b DSGVO zu erfüllen.

1.4 Decken die vertraglichen Vereinbarungen mit AWS den § 203 StGB ab?

Kurzantwort: Ja. Eine ausdrückliche Verpflichtung auf die Geheimhaltungspflicht nach § 203 StGB ist nicht erforderlich.

Erläuterung:

Seit der umfassenden Reform des Berufsgeheimnisschutzgesetzes Ende 2017 ist die rechtssichere Einbeziehung von Outsourcing-Dienstleistern in die Abläufe von Betrieben von Berufsgeheimnisträgern möglich. Sind die so mitwirkenden Personen zur Geheimhaltung verpflichtet, ist die (erforderliche) Kenntnisnahme – die „Offenbarung" – von Berufsgeheimnissen durch diese mitwirkenden Personen nicht strafbar für den Berufsgeheimnisträger, § 203 Abs. 3 S. 2 StGB. Setzt der Kunde die ihm zur Verfügung stehenden Verschlüsselungsmethoden mit hinreichendem Schutzniveau ein und verhindert so, dass AWS die ggf. einem Berufsgeheimnis unterfallenden Daten des Kunden zur Kenntnis nehmen kann, ist eine Übermittlung kein Offenbaren im Sinne der Vorschrift. § 203 StGB kommt dann nicht zur Anwendung. Daneben verpflichtet AWS sich und ihre Mitarbeiter gemäß Ziffer 3 und 4 des DPA zur Vertraulichkeit und gibt diese Vertraulichkeitsverpflichtung an ihre Unterverarbeiter weiter. So kann die Kette der Vertraulichkeitsverpflichtungen gemäß § 203 Abs. 4 StGB ordnungsgemäß aufrechterhalten werden. Dies gilt auch, wenn eine „weitere sonstige mitwirkende Person" im Sinne des § 203 Abs. 3 S. 2 StGB ihren Sitz im Ausland hat. Für bestimmte Berufsgeheimnisträger, z. B. Rechtsanwälte oder Steuerberater, gelten neben der Pflicht, mitwirkende Personen zur Verschwiegenheit zu verpflichten, zusätzliche Belehrungspflichten aus dem Berufsrecht.

DIERKS + COMPANY

Diese bestehen jedoch nicht für Krankenkassen und deren Mitarbeiter. Für sie genügt mithin die von AWS im Rahmen des DPA bestehende Vertraulichkeitsverpflichtung, sofern überhaupt eine Offenbarung von Geheimnissen im Sinne des § 203 StGB erfolgt.

1.5 Kann ich bei der Nutzung von AWS die Anforderungen des § 80 SGB X erfüllen?

Kurzantwort: Ja.

Erläuterung:

§ 80 SGB X regelt die Auftragsverarbeitung im Sinne des Art. 28 DSGVO von Sozialdaten (vgl. Frage 1.1). Die Nutzung der AWS Services wäre eine solche Auftragsverarbeitung. Verantwortliche, die Sozialdaten verarbeiten, müssen daher vorab ihre Anzeigepflicht nach § 80 Abs. 1 SGB X erfüllen.

Weiter verlangt § 80 Abs. 2 SGB X, dass die Verarbeitung von Sozialdaten im Auftrag nur innerhalb Deutschlands, in einem anderen Mitgliedstaat der EU, in einem nach § 35 Abs. 7 SGB I gleichgestellten Staat oder in einem Drittland erfolgt, für das ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt. Je nach der vom Kunden gewählten Architektur und den ausgewählten AWS-Services ist es möglich, AWS Services in einer Weise zu nutzen, bei der die Datenverarbeitung innerhalb der EU erfolgt. AWS ermöglicht den Kunden u. a. zu wählen, in welcher Region der Service und die Auftragsverarbeitung durchgeführt werden soll. Überdies hat AWS eine Übersicht erarbeitet, anhand derer Kunden feststellen können, ob ihre Nutzung eines einzelnen AWS-Services die Übertragung von Kundendaten (die personenbezogenen Daten, die Kunden in ihr AWS-Konto hochgeladen haben) beinhaltet. Zusätzlich bietet AWS technische Lösungen (wie z. B. *AWS Service Control Policies*) an, die die Sperrung der Nutzung von AWS-Diensten in Regionen außerhalb des EWR ermöglichen. Die (Auftrags-) Verarbeitung der Sozialdaten kann damit in Einklang mit § 80 Abs. 2 SGB X erfolgen. Dem zulässigen Einsatz von AWS im Rahmen der Verarbeitung von Sozialdaten widerspricht auch nicht, dass AWS in Einzelfällen mit Herausgabeverlangen von Drittlandsbehörden konfrontiert wird: Hierbei handelt es sich nicht um die Verarbeitung von Sozialdaten *im Auftrag*, sodass bereits die Anwendbarkeit des § 80 Abs. 2 SGB X auf eine Verarbeitung zum Zwecke der Herausgabe fraglich ist. Darüber hinaus findet sich der Wortlaut des § 80 Abs. 2 SGB X in § 4 Abs. 3 der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) wieder (vgl. hierzu Frage 1.7).[4] Zu § 4 Abs. 3 DiGAV vertritt das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) ausdrücklich, dass der Einsatz von Dienstleistern, die eine Niederlassung in der EU haben, grundsätzlich möglich ist, selbst wenn diese einen Mutterkonzern in einem Drittland haben.[5] Aufgrund der Parallelität der Regelungen muss der Einsatz von Dienstleistern mit Mutterkonzernen in Drittländern bei Erfüllung der vom BfArM aufgestellten Anforderungen daher auch nach § 80 Abs. 2 SGB X rechtlich zulässig sein. Dies gilt auch

---

[4] Vgl. Referentenentwurf des Bundesministeriums für Gesundheit zu § 4 DiGAV, abrufbar unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/DiGAV_RefE.pdf

[5] Vgl. DiGA-Leitfaden (Stand 18.03.2022), Ziff. 3.3.

DIERKS + COMPANY

für AWS, denn AWS erfüllt die vom BfArM aufgestellten Anforderungen an Dienstleister mit einem Mutterkonzern in den USA (vgl. hierzu Frage 3.3).

Schließlich darf AWS als nicht-öffentliche Stelle gemäß § 80 Abs. 3 SGB X nur beauftragt werden, wenn beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten erheblich kostengünstiger besorgt werden können. Die Prüfung dieser Voraussetzungen obliegt dem Verantwortlichen. AWS ist bereit, ihre Kunden hierbei zu unterstützen.

1.6 Können Gesundheitsanwendungen, die auf AWS laufen, auch nach der MDR zertifiziert werden?

Kurzantwort: Sofern die Voraussetzungen der MDR vorliegen, ist eine solche Zertifizierung möglich.

Erläuterung:

Nach der *Medical Devices Regulation* (MDR) ist Software zu zertifizieren, wenn sie die Kriterien einer *Medical Device Software (MDSW)* und sämtliche Anforderungen der MDR erfüllt. Es wird stets die Anwendung des Kunden zertifiziert und nicht die AWS Services. Das Zertifizierungsverfahren erfordert in aller Regel die Beteiligung einer Benannten Stelle, weil die MDSW zumeist in die Risikoklasse IIa oder höher fallen wird. Die MDR bildet den rechtlichen Rahmen für alle Medizinprodukte. Sie enthält allgemeine Anforderungen an IT-Sicherheit und Datenschutz, die dem Einsatz von AWS nicht entgegenstehen. AWS bietet Kunden die Tools, um die regulatorischen Anforderungen zu erfüllen. Es obliegt sodann dem Kunden, hiermit die Voraussetzungen für eine Zertifizierung seiner Anwendung zu schaffen. Für Digitale Gesundheitsanwendungen gelten daneben noch weitere Anforderungen, u. a. aus § 33a SGB V, der DiGAV sowie einer Reihe von BSI-Standards und ISO-Normen. Vgl. hierzu auch Frage 1.7.

1.7 Kann ich AWS Services im Einklang mit den Anforderungen des § 4 DiGAV nutzen?

Kurzantwort: Ja.

Erläuterung:

AWS ermöglicht es Kunden, digitale Gesundheitsanwendungen auf AWS zu erstellen und auszuführen, die den Anforderungen der der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) genügen. Anbieter einer digitalen Gesundheitsanwendung sind u. a. gemäß § 4 Abs. 1 DiGAV verpflichtet, die gesetzlichen Anforderungen an Datenschutz und Datensicherheit zu gewährleisten. Die Einschränkungen der Verarbeitung nach § 4 Abs. 2 DiGAV sind von den Verantwortlichen einzuhalten.

1.7.1 Einsatz von Auftragsverarbeitern gemäß § 4 Abs. 3 DiGAV

Nach § 4 Abs. 3 der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) ist im Rahmen einer digitalen Gesundheitsanwendung eine Verarbeitung im Auftrag nur innerhalb Deutschlands, in einem anderen Mitgliedstaat der EU, in einem nach § 35 Abs. 7 SGB I gleichgestellten Staat oder in einem

Drittland zulässig, für das ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt. Teilweise wird vertreten, dass die Einschränkungen des § 4 Abs. 3 DiGAV nicht zuletzt aufgrund der fehlenden Konkretisierung der Datenkategorien und des Schutzzwecks gegen Art. 49 Abs. 5 DSGVO verstoßen und die Norm europarechtswidrig ist.[6] Ungeachtet dessen ist es jedoch möglich, AWS Services so zu konfigurieren und zu nutzen, dass die Verarbeitung nur innerhalb in der EU erfolgt. AWS ermöglicht den Kunden u. a. zu wählen, in welcher Region der Service und die Auftragsverarbeitung durchgeführt werden soll. So können Kunden vertraglich z. B. Frankfurt am Main als Serverstandort vereinbaren. Da manchen AWS-Services die Übermittlung von Daten außerhalb der EU / des EWR inhärent ist, können Kunden ihre AWS-Architektur so konfigurieren, dass diese Services deaktiviert sind, und hiermit § 4 Abs. 3 DiGAV erfüllen. AWS unterstützt ihre Kunden dabei, zu verstehen, welche Services eine ausschließliche Verarbeitung innerhalb der EU / des EWR ermöglichen. **Speziell für DiGA-Kunden ermöglicht AWS zahlreiche Maßnahmen, um sie bei der Einrichtung technischer Leitplanken zur Einhaltung der rechtlichen Rahmenbedingungen zu unterstützen.** AWS hat für seine Kunden u. a. eine Übersicht erarbeitet, aus der sich ergibt, welche Services die Verarbeitung ausschließlich in der EU / dem EWR ermöglichen. AWS stellt überdies auch Anleitungen für technische Lösungen zur Verfügung, die Kunden bei der Sperrung der Nutzung von AWS-Services in Regionen außerhalb des EWR unterstützen. Die (Auftrags-) Verarbeitung der Gesundheits- und Sozialdaten bei der Nutzung von AWS Services kann damit im Einklang mit § 4 Abs. 3 DiGAV erfolgen. Dem zulässigen Einsatz von AWS im Rahmen der Verarbeitung von Daten im Zusammenhang mit DiGAs widerspricht auch nicht, dass AWS in Einzelfällen mit Herausgabeverlangen von Drittlandsbehörden konfrontiert wird: Zunächst ist zweifelhaft, ob die Übermittlung in ein Drittland aufgrund eines solchen Herausgabeverlangens noch die Verarbeitung „im Rahmen einer digitalen Gesundheitsanwendung" bzw. die Verarbeitung *im Auftrag* ist und damit unter den Anwendungsbereich des § 4 Abs. 3 DiGAV fällt. Darüber hinaus kommt das BfArM im Lichte des § 4 Abs. 3 DiGAV zwar zu dem Ergebnis, dass bei einer DiGA die Verarbeitung in einem Drittland nicht aufgrund von Standardvertragsklauseln nach Art. 46 DSGVO möglich ist und wegen des Schrems-II-Urteils des EuGH und der Unwirksamkeit des sog. *Privacy Shields* eine Auftragsverarbeitung nicht in den USA stattfinden darf. Es vertritt jedoch unter ausdrücklicher Nennung von AWS, dass der Einsatz von Dienstleistern, die eine Niederlassung in der EU haben, auch unter den Einschränkungen des § 4 Abs. 3 DiGAV möglich ist, selbst wenn diese einen Mutterkonzern im Ausland haben, sofern Auftraggeber und Dienstleister bestimmte Anforderungen erfüllen. Dies gilt auch für AWS, denn AWS erfüllt die vom BfArM im DiGA-Leitfaden aufgestellten Anforderungen an Dienstleister mit einem Mutterkonzern in den USA (vgl. hierzu Frage 3.3f.). AWS-Services können daher in zulässigerweise auch unter Beachtung der Einschränkungen des § 4 Abs. 3 DiGAV genutzt werden.

1.7.2 Verschwiegenheitsverpflichtung gemäß § 4 Abs. 5 DiGAV

Gemäß § 4 Abs. 5 der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) ist der Hersteller einer digitalen Gesundheitsanwendung verpflichtet, alle für ihn tätigen Personen mit Zugang zu

---

[6] Hofer/Sachs/Sonnenschein, MPR 2020, 227f.

DIERKS + COMPANY

personenbezogenen Daten von Versicherten auf Verschwiegenheit zu verpflichten. Macht der Kunde von den ihm zur Verfügung stehenden Verschlüsselungsmethoden Gebrauch und verhindert so, dass AWS Zugang zu den entsprechenden Daten erhält, kann eine Verschwiegenheitsverpflichtung entbehrlich sein. Ungeachtet dessen verpflichtet sich AWS gemäß DPA zur Vertraulichkeit und dazu, dass Unterverarbeiter die gleichen vertraglichen Verpflichtungen auferlegt werden, denen AWS gemäß DPA unterliegt (vgl. Frage 1.2). Dies gilt folglich auch für die Vertraulichkeitsverpflichtung, sodass eine Kette der Vertraulichkeit besteht. Die Anlage 1 Nr. 36 zur DiGAV verlangt, dass Daten ausschließlich an Auftragsverarbeiter weitergegeben werden, die über eine ausreichende Vertrauenswürdigkeit und Haftbarkeit verfügen, angemessene Mechanismen zum Schutz übernommener Daten realisieren und mit dem Hersteller der DiGA in einem verpflichtenden vertraglichen Verhältnis stehen, das eine Abschwächung der dem Versicherten gegenüber gemachten Zusagen ausschließt. Auch diesen Anforderungen kann beim Einsatz von AWS genüge getan werden. Neben der Verpflichtung zur Vertraulichkeit hält AWS weitere Maßnahmen zum Schutz der Daten vor. Gemäß Annex 1 zum DPA, den AWS Security Standards, wird der Zugang zu Kundendaten durch AWS-Mitarbeiter oder Unterverarbeiter u. a. durch ID-Kontrollen und Rechte-Rollen-Konzepte für einen Datenzugriff limitiert und überprüft. Die Sicherheit der Datenverarbeitung wird zudem durch die Maßnahmen nach Art. 32 DSGVO gewährleistet, siehe hierzu Abschnitt 2. AWS haftet nach dem Regime der DSGVO. Die vertragliche Haftung ergibt sich im Übrigen aus Ziffern 10, 11 des *AWS Customer Agreements*.

1.8 Erfüllt AWS die Sicherheitsanforderungen nach Art. 32 DSGVO?

Ja. AWS ist bereit, die für die Bedürfnisse des Kunden im Rahmen des *Shared Responsibilty* Modells erforderlichen Maßnahmen nach Art. 32 DSGVO zu erfüllen. Auch die nach § 22 Abs. 2 BDSG zu treffenden Maßnahmen können mithilfe von AWS gewährleistet werden. Siehe hierzu Abschnitt 2.

1.9 Welches Vertragsrecht und welcher Gerichtsstand gilt, wenn ich AWS nutze?

Kurzantwort: Luxemburgisches Recht und Luxemburg. Eine Kundenvereinbarung nach deutschem Recht oder einen deutschen Gerichtsstand zu vereinbaren, ist im Kontext des Sozialrechts und im Zusammenhang mit digitalen Gesundheitsanwendungen nicht vorgeschrieben und böte auch keinen Vorteil.

Erläuterung:

AWS stellt eine standardisierte Reihe von Services bereit, die für alle Kunden weltweit einheitlich funktionieren. Daher ist es für AWS wichtig, Sicherheit und Einheitlichkeit im Hinblick auf das auf Verträge anwendbare Recht zu gewährleisten. AWS Services werden von Kunden weltweit genutzt. Es ist für AWS – wie auch für jeden anderen globalen Anbieter von IT-Dienstleistungen –nicht mit vertretbarem Aufwand skalierbar, ihre Verträge jeweils an die Details der lokalen Rechtsordnungen der Länder anzupassen, in denen AWS Services genutzt werden. Nur so kann AWS ihre Ressourcen in die sinnvolle Erweiterung und Sicherheit ihrer Services einbringen und dem hohen Standard gerecht werden, den sich AWS für ihre Services setzt. Die so gewährte Einheitlichkeit und Klarheit bei der

Auslegung und Anwendung der Vertragsbestimmungen kommen allen Kunden zugute. Die Wahl des anwendbaren Rechts und des Gerichtsstands betrifft nur Streitigkeiten aus und im Zusammenhang mit den geschlossenen Verträgen. Ungeachtet der Wahl des auf die Verträge anzuwendenden Rechts, wird AWS durch direkt auf sie anzuwendendes europäisches und deutsches Recht gebunden, soweit sie in Deutschland agiert, vgl. Art. 3 DSGVO und § 1 Abs. 4 BDSG.

AWS EMEA Sarl ist eine juristische Person mit Sitz in Luxemburg. Aus diesem Grund ist es sinnvoll, auch die vertraglichen Bestimmungen einheitlich nach luxemburgischem Recht zu gestalten und Luxemburg als Gerichtsstand zu vereinbaren. Die Wahl des Ortes des Gerichtsstands ist nicht willkürlich und weist Bezug zu einer der Vertragsparteien auf. Durch die Harmonisierung vieler relevanter Rechtsvorschriften in der EU entsteht deutschen Kunden kein rechtlicher Nachteil dadurch, dass Luxemburg als Gerichtsstand vereinbart wird. Die für den Kunden relevanten Vorschriften des Sozialrechts und gegebenenfalls betreffend die digitalen Gesundheitsanwendungen regeln die Wahl des Gerichtsstands und des Vertragsrechts nicht und stehen der Vereinbarung von luxemburgischem Recht und Luxemburg als Gerichtsstand nicht entgegen.

1.10 Gelten die Anforderungen an die Speicherung von Gesundheits- und Sozialdaten für alle Daten, die eine Krankenkasse in der Cloud speichert?

Kurzantwort: Nein.

Erläuterung:

Gesundheitsdaten (vgl. Frage 1.1) sind als besondere Kategorien personenbezogener Daten i. S. d. Art. 9 Abs. 1 DSGVO besonders schützenswert. Die erhöhten Anforderungen an den Schutz der besonderen Kategorien personenbezogener Daten gelten nur für diejenigen Daten, die dem Begriff unterfallen. Für andere Daten gelten andere, regelmäßig geringe Anforderungen.

Sozialdaten sind definitionsgemäß alle personenbezogenen Daten, die eine in § 35 Abs. 1 SGB I genannte Stelle im Hinblick auf ihre Aufgaben nach dem SGB verarbeitet. Sozialdaten sind also alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, vgl. Art. 4 Nr. 1 DSGVO. Verarbeitet eine Krankenkasse die personenbezogenen Daten ihrer Versicherten, handelt es sich hierbei um Sozialdaten, für die die gesetzlichen Anforderungen des Sozialdatenschutzes gelten.

Nicht unter den (Sozial- oder Gesundheits-) Datenschutz fallen anonymisierte oder stark aggregierte Daten. Auf diese Daten finden auch die Regelung der DSGVO keine Anwendung.

Die Beurteilung, welche der Daten des Verantwortlichen personenbezogene, Sozial- und/oder Gesundheitsdaten sind, muss der Verantwortliche vornehmen.

DIERKS + COMPANY

1.11 Gelten die datenschutzrechtlichen Anforderungen auch für pseudonymisierte Daten und anonymisierte Daten?

Kurzantwort: Nein in Bezug auf anonymisierte Daten und ja in Bezug auf pseudonymisierte Daten.

Erläuterung:

Personenbezogene Daten sind gemäß Art. 4 Nr. 5 DSGVO **pseudonymisiert**, wenn sie in einer Weise verarbeitet werden, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert oder logisch getrennt aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Daten können zum Beispiel pseudonymisiert werden, indem in Datensätzen Vor- und Nachname durch eine Buchstabenzahlenkombination ausgetauscht werden. Pseudonymisierte Daten sind immer noch personenbezogene Daten, die dem Schutz der DSGVO und der weiteren datenschutzrechtlichen Bestimmungen unterfallen.

Der Begriff der **anonymisierten Daten** ist nicht in der DSGVO definiert. Anonymisieren ist das Verändern personenbezogener Daten derart, dass die hinter den Einzelangaben über persönliche oder sachliche Verhältnisse stehende betroffene Person nicht bzw. nicht mehr identifiziert werden kann. Durch eine Anonymisierung kann der Gehalt eines Datensatzes erhalten bleiben, lässt aber keine Zuordnung der Aussage zu einer bestimmten oder bestimmbaren Person mehr zu. Daten sind jedoch nicht bereits dann anonym, wenn ein Identifizierungsdatum fehlt. Kann dieses noch aufgefunden und können die Daten re-identifiziert werden, liegt allenfalls Pseudonymisierung, nicht aber Anonymisierung vor.[7] Während nach alter Rechtslage (vgl. § 3 Abs. 6 BDSG 2003) schon von einer Anonymisierung ausgegangen wurde, wenn die Daten nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können, dürfte dies angesichts der stetig zunehmenden Möglichkeiten an technischen Mitteln, scheinbar anonyme Daten doch einzelnen Personen zuzuordnen, nach der aktuellen Rechtslage nicht mehr genügen. Die sicherste Methode der Anonymisierung ist die Aggregierung von Daten, also das Zusammenführen mehrerer personenbezogener Daten zu einem Gruppendatensatz, aus dem heraus nicht mehr festgestellt werden kann, wem innerhalb dieses Datenkollektivs welche Einzeldaten zuzuordnen sind. Anonymisierte Daten sind keine personenbezogenen Daten i. S. d. DSGVO. Die Grundsätze des Datenschutzrechtes gelten daher nicht für (tatsächlich) anonyme Daten (vgl. auch ErwGrund 26 der DSGVO). Bereits aus dem Grundsatz der Datenminimierung (vgl. Art. 5 Abs. 1 lit. c DSGVO) folgt, dass personenbezogene Daten nur in dem Maße verarbeitet werden sollen, in dem es für die Zwecke der Verarbeitung notwendig ist. Können die Verarbeitungszwecke mit anonymisierten Daten erreicht werden, sollte auf die Verarbeitung personenbezogener Daten verzichtet werden.

---

[7] Ernst, in Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 4 Rn. 49.

DIERKS + COMPANY

2. Fragen zur Sicherheit der Verarbeitung

2.1 Ermöglicht AWS geeignete Maßnahmen für die Sicherheit der Verarbeitung (Art. 32 DSGVO, § 22 BDSG) bzw. hat AWS ausreichende „TOM", um die Sicherheit der Verarbeitung zu gewährleisten?

Kurzantwort: Ja.

Erläuterung:

Verantwortliche und Auftragsverarbeiter haben gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Welche Maßnahmen im Einzelfall zu treffen sind, hängt von den sich aus der Verarbeitung ergebenden Risiken und dem Schutzbedarf der verarbeiteten Daten ab.[8] Seit den Empfehlungen des *European Data Protection Boards* (EDPB) als Folge der sog. Schrems-II-Entscheidung des EuGH (vgl. Abschnitt 3) haben (zusätzliche) vertragliche, organisatorische und technische Maßnahmen als Garantien bei der Datenverarbeitung, insbesondere der Datenübermittlung, an Bedeutung gewonnen. Als vertragliche Maßnahme hat AWS nicht nur ihr *DPA* angepasst, sondern es auch um das *Supplementary Addendum* zum DPA ergänzt, um den neuen Anforderungen gerecht zu werden. Die im Rahmen der Nutzung der verschiedenen AWS-Services eingesetzten (organisatorischen und technischen) Maßnahmen wählt im Rahmen des *Shared Responsibilty* Modells der Kunde. Die zahlreichen Tools, die AWS im Zusammenhang mit der DSGVO anbietet, können im *GDPR Center* eingesehen werden. So können die Kunden etwaig erforderliche zusätzliche Maßnahmen i. S. d. Schrems-II-Entscheidung einrichten.

Typische Beispiele für von ihren Kunden angewandte technische und organisatorische Maßnahmen sind laut AWS: Verschlüsselung personenbezogener Daten (Client- und Serverseitig), Zugriffskontrollen, Verfügbarkeitsgarantien (Nutzung mehrerer Verfügbarkeitszonen und Regionen), Back-up Angebote sowie *AWS Security Services*. Die Konfigurierung der Verschlüsselung legt der Kunde im Rahmen der Nutzung des *Key Management Systems* (KMS) oder der *High Security Module* (HSM) eigenständig fest. So kann die Verschlüsselung der Daten nur vom Kunden selbst aufgehoben, also entschlüsselt werden. Die virtuelle Infrastruktur wird ebenfalls autonom vom Kunden konfiguriert. Weitere Sicherheitsservices von AWS sind: *Amazon Inspector, Amazon GuardDuty, AWS CloudTrail, AWS Trusted Advisor*. Hinzu kommen im Rahmen des *Shared Responsibilty* Modells kundenseitige Maßnahmen wie beispielsweise ein differenziertes Berechtigungskonzept, Zugriffskontrollen und Client- sowie Server-seitige Verschlüsselung. Bei der Nutzung von *Elastic Compute EC2*, *Kubernetes*, *Relational Data Base Service* ermöglicht AWS *Confidential Computing:* Der von AWS entwickelte Virtualisierungs- und Isolationsansatz von *Nitro System* ermöglicht es den Kunden, sensible Daten zu isolieren und AWS von der Verarbeitung auszuschließen. So können Kunden die für die Verarbeitung ihrer Daten erforderlichen Maßnahmen bestimmen und konfigurieren, um ein angemessenes

---

[8] Jandt, Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 32 Rn. 31.

Schutzniveau im Sinne des Art. 32 DSGVO zu gewährleisten. Auf diese Weise können Kunden auch angemessene und spezifische Maßnahmen treffen, die den Anforderungen des § 22 Abs. 2 BDSG genügen. Welche Maßnahmen Kunden treffen müssen oder wollen, ist im Einzelfall abhängig von dem aus der Datenverarbeitung entstehenden Risiko und dem festgestellten erforderlichen Schutzniveau der Daten.

2.2 Welche Maßnahmen ergreift AWS, um meine Daten vor Angriffen von innen und von außen zu schützen?

Kurzantwort: AWS verpflichtet sich zur Einhaltung ihrer Security Standards und ist überdies nach verschiedenen IT-Sicherheitsstandards zertifiziert.

Erläuterung:

Das DPA von AWS beinhaltet einen Annex 1 *AWS Security Standard*, in dem AWS Angaben zu ihrem *Information Security Programm* macht. Gemäß den *AWS Security Standards* wird der Zugang zu Kundendaten durch AWS-Mitarbeiter oder Unterverarbeiter u. a. durch ID-Kontrollen und Rechte-Rollen-Konzepte für Datenzugriff limitiert und überprüft.

Daneben ist AWS nach verschiedenen Sicherheitsstandards zertifiziert. AWS als Level 1-Diensteanbieter ist beispielsweise nach dem *Payment Card Industry Data Security Standard* (**PCI DSS**) Datensicherheitsstandard zertifiziert. Dieses Zertifikat ist besonders für Kunden von Bedeutung, die vertrauliche Authentifizierungsdaten (Sensitive Authentication Data, SAD) speichern, verarbeiten oder übertragen. Für diese Kunden stellt AWS die *Attestation of Compliance* (AOC, Bestätigung der Compliance) und *Responsibility Summary* (Zusammenfassung der Verantwortlichkeiten) des PCI DSS zur Verfügung.

AWS-Regionen wie Frankfurt, Irland, London, Paris, Mailand, Stockholm und Singapore erfüllen außerdem die Anforderungen des *Cloud Computing Compliance Criteria Catalogue* (C5) des Bundesamtes für Sicherheit in der Informationstechnik (BSI). C5 ist ein Kriterienkatalog, der die Mindestanforderungen an die Informationssicherheit für Cloud-Dienste beschreibt, die nicht unterschritten werden sollten. Der Kunde ist in der Verantwortung zu prüfen, ob die Mindestkriterien für seinen konkreten Anwendungsfall ausreichen oder durch weitergehende Maßnahmen ergänzt werden müssen. Mehr zu C5 findet sich beim BSI und bei AWS.

Daneben sind Services von AWS u. a. nach **ISO/IEC 27001:2013** zertifiziert.[9] ISO/IEC 27001:2013 ist ein Sicherheitsstandard, der bewährte Sicherheitsmanagementverfahren und umfassende Sicherheitskontrollen gemäß festgelegten Leitlinien festlegt. Zur Entwicklung und Implementierung eines strengen Sicherheitsprogramms zählt auch die Entwicklung und Implementierung eines

---

[9] Darüber hinaus sind AWS-Services nach IT-Sicherheitsstandards 27017:2015, 27018:2019, ISO/IEC 9001:2015 und CSA STAR CCM v3.0.1 zertifiziert.

Informationssicherheits-Managementsystems (ISMS). Eine aktuelle Liste der AWS-Services, die unter die Zertifizierungen fallen, findet sich hier.

Weitere Ausführungen gibt es in den von AWS und der AWS-Community erstellten technischen Inhalten über die Cloud. Zu diesen Inhalten gehören technische Whitepaper, technische Handbücher, Referenzmaterial sowie Referenzarchitekturdiagramme, die hier abrufbar sind.

2.3 Wie helfen mir die AWS Zertifikate, die Sicherheit der Verarbeitung nachzuweisen?

Kurzantwort: Sie können als zusätzlicher Nachweis für die Sicherheit der Verarbeitung dienen.

Erläuterung:

Eine Zertifizierung mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung datenschutzrechtlicher Anforderungen, vgl. Art. 42 Abs. 4 DSGVO. Doch sie kann als Nachweis für die Einhaltung der Vorschriften der DSGVO verwendet werden und damit die Kontrolle von eingesetzten Dienstleistern erleichtern.[10] Ob die gemäß ISO dokumentierten Maßnahmen ausreichen, um im Einzelfall ein hinreichendes Schutzniveau zu begründen, muss der Kunden abhängig von seinem beabsichtigten Einsatz der AWS-Services beurteilen.

Die Kunden sind berechtigt, ISO 27001-Zertifizierungen von (potenziellen) Auftragsverarbeitern von Sozialdaten zu verlangen.[11] AWS hält die Zertifikate auf ihrer Webseite abrufbereit. Kunden von AWS können auf die C5-testierte Infrastruktur von AWS aufbauen, wenn sie sich um ein eigenes C5-Testat bemühen.

2.4 Wenn ich meine Daten bei AWS speichere, wo liegen diese Daten dann und wer hat darauf Zugriff?

Kurzantwort: Der Kunde bestimmt, wo die Daten gespeichert werden und wer darauf zugreifen kann.

Erläuterung:

Die Kunden bestimmen die Region, in der die Daten des Kunden oder seiner Endnutzer gespeichert werden sollen. AWS wird diese Daten nicht ohne Zustimmung des Kunden in eine andere als die vereinbarte Region bewegen. Gemäß Ziffer 12.1, 2. und 3. des DPA sowie gemäß Ziffer 3.2 des *AWS Customer Agreements* wird AWS diese Kundendaten nicht außerhalb der vom Kunden ausgewählten AWS-Region verarbeiten, es sei denn, dies ist zum Zweck der Erbringung der vom Kunden genutzten Services oder aufgrund von dokumentierten Anweisungen des Kunden erforderlich oder wenn dies zur Einhaltung des Gesetzes oder einer wirksamen und rechtskräftigen Anordnung einer staatlichen Stelle erforderlich ist. In ihrem *Supplementary Addendum* verpflichtet sich AWS ergänzend u.a., Anfragen

---

[10] Conrad/Streitz, in Auer-Reinsdorff/Conrad, Hdb IT- und Datenschutzrecht, 3. Aufl. 2019, § 33 Rn. 363.
[11] BKartA, B. v. 19.7.2019 – VK 1-39/19.

von Behörden abzulehnen und anzufechten, insbesondere wenn die Anfragen europäischem oder nationalem Recht widersprechen (vgl. Frage 3.3.1). Darüber hinaus verpflichtet sich AWS, gegen etwaige Verfügungen vorzugehen, die ihr untersagen, den Kunden zu informieren. Die Pflicht, sich an geltendes Recht zu halten, trifft jeden Anbieter (siehe auch Frage 3.3.2). Durch Zugriffskontrollen und Verschlüsselung kontrollieren die Kunden, wem der Zugriff auf die Inhalte der Kundendaten oder der Daten der Endnutzer (technisch) möglich ist.

Auf der Webseite von AWS findet sich eine Übersicht der verfügbaren Regionen. Der Kunde kann insbesondere ausdrücklich Frankfurt als AWS-Region auswählen. Der Kunde kann zudem die Architektur so wählen und die Services von AWS so nutzen, dass im Rahmen der Durchführung der Dienste keine Datenverarbeitungen außerhalb der EU / des EWR erforderlich sind. AWS verarbeitet die Daten in der Form und in dem Umfang, wie es erforderlich ist, um die gewünschte Nutzung des Kunden zu erfüllen. Der Kunde hat es also in der Hand, die Services so zu nutzen, dass die Verarbeitung im Einklang mit einschlägigen Vorgaben erfolgt. Die von AWS ermöglichten Maßnahmen genügen auch bei einer Datenverarbeitung unter Anwendbarkeit des § 80 SGB X oder § 4 DiGAV den dort geregelten Anforderungen zum Ort der Verarbeitung (vgl. Fragen 1.5 und 1.7). Dies gilt auch mit Blick auf die Verbindung zum Mutterkonzern von AWS in den USA (vgl. Abschnitt 3).

2.5 Wenn ich meine Daten in AWS verschlüssele, kann AWS die Daten trotzdem lesen?

Kurzantwort: Nein.

Erläuterung:

Verschlüsselte Daten in AWS können ausschließlich vom Kunden selbst entschlüsselt und gelesen werden. Der Kunde entscheidet über die Art der Verschlüsselungen. Es liegt in seinem Verantwortungsbereich, ob die Daten verschlüsselt werden, wie diese Verschlüsselung konfiguriert ist und ob er dazu einen eigenen Schlüssel nutzen möchte und diesen importiert.

Das BfArM gibt im DiGA-Leitfaden im Kontext digitaler Gesundheitsanwendungen bei Auftragsverarbeitern mit US-Verbindungen hierzu folgende Vorgabe: „*Sofern die personenbezogenen Daten nach dem Stand der Technik im Sinne von Artikel 25 und 32 DSGVO verschlüsselt sind und die Schlüssel vom DiGA-Hersteller in der EU selbst verwaltet oder gespeichert werden (beispielsweise Customer-Managed Encryption Keys, CMEK), dürfen Dienstleister mit Niederlassung in der EU, aber einem Mutterkonzern in den USA, herangezogen werden.*“ Diese Anforderungen können bei der Nutzung von AWS Services erfüllt werden:

Der Kunde kann den *Key Management Service* (KMS) von AWS in verschiedenen Varianten einsetzen. Wenn der Kunde die volle Kontrolle über die Verwaltung seiner Schlüssel haben möchte, einschließlich der Möglichkeit, den Zugriff auf Schlüssel über Konten oder Services hinweg freizugeben, kann er seinen eigenen Kunden-Masterschlüssel (CMKs) in AWS KMS erstellen. AWS KMS ist so aufgebaut, dass niemand, auch kein Mitarbeiter von AWS, CMKs des Kunden im Klartext abrufen kann. Der Service verwendet Hardwaresicherheitsmodule (HSMs), die entweder bereits unter dem internationalen

DIERKS + COMPANY

Computersicherheitsstandard FIPS 140-2 validiert wurden oder aktuell validiert werden. Die Klartext-CMKs verlassen nie die HSMs und werden nicht auf die Festplatte geschrieben, sondern lediglich für die Dauer der jeweiligen vom Kunden angeforderten kryptografischen Vorgänge im temporären Speicher der HSMs verwendet. AWS KMS-Schlüssel werden nie außerhalb der AWS-Regionen übertragen, in denen sie erstellt wurden.

2.6 Was sind Instance-Metadaten, wie sind sie rechtlich einzuordnen und (wie) werden sie von AWS verarbeitet?

Kurzantwort: Auch Instance-Metadaten können bedingt durch die Nutzung durch den Kunden personenbezogene Daten sein. Sie werden der Nutzung des Kunden entsprechend von AWS verarbeitet.

Erläuterung:

Instance-Metadaten sind Daten über eine Instance, mit denen ausgeführte Instanzen konfiguriert und verwaltet werden können. Instance-Metadaten sind in Kategorien unterteilt (z. B. Hostname, Ereignisse und Sicherheitsgruppen). Bei jedem Start einer Instance wird ein Instance-Identitätsdokument generiert, das Informationen über die Instance selbst liefert. Der Kunde kann die Attribute einer Instance mithilfe des Instance-Identitätsdokuments validieren. Die Instance-Identitätsdokumente können mithilfe von gehashten und verschlüsselten Signaturen authentifiziert werden. Das Instance-Identitätsdokument kann nur während der laufenden Instance abgerufen werden. Wie der Zugriff auf die Instance-Metadaten erfolgen soll, kann der Kunde selbst konfigurieren. Ob der Kunde beim Starten einer Instance auch Instance-Benutzerdaten angibt und verarbeiten lässt und wenn ja, welche, kann der Kunde selbst entscheiden.

2.7 Haben Support- bzw. Serviceteams (von außerhalb der EU) Zugriff auf Kundendaten in meinen Account oder können diese einsehen?

Kurzantwort: Der Kunde kann selbst bestimmen, ob und in welchem Umfang Supportteams von AWS Einsicht in Kundendaten nehmen. Grundsätzlich benötigt AWS für Erbringung von Wartung und Support keinen Zugang zu Kundendaten. Der Kunde entscheidet selbst darüber, ob er AWS im Supportfall ausnahmsweise temporär Zugriff gewähren möchte. Der jeweilige Support-Techniker erhält mit diesem Zugriffsrecht jedoch kein Recht zur Nutzung der kryptografischen Schlüssel. Daher wird das AWS-Supportteam keine Einsicht in Kundendaten erhalten, wenn der Kunde diese verschlüsselt hat.

Erläuterung:

Support- oder Service-Teams von AWS greifen unabhängig von ihrem Standort nicht ohne ausdrückliche Aufforderung des Kunden auf Kundendaten zu. Ist z. B. aufgrund eines technischen Problems der Einsatz eines Supportteams gefragt, hält AWS bei Abschluss eines entsprechenden Support-Vertrags einen persönlichen, lokalen Ansprechpartner für ihre Kunden bereit. AWS sieht drei

DIERKS + COMPANY

Varianten der Problemlösung vor: (i) Der Kunde löst das Problem selbstständig, (ii) AWS-Supportteams leisten Hilfestellung im Regelfall, ohne auf Kundensysteme zuzugreifen, und (iii) AWS-Supportteams leisten in Ausnahmefällen Hilfestellung mit streng reguliertem Zugriff auf Kundensysteme, sofern der Kunde sein ausdrückliches Einverständnis erteilt. Der Kunde steuert, ob er im Zusammenhang mit dem jeweiligen Supportfall Kundendaten mit AWS teilt oder nicht, z. B., indem er Kundendaten in das Support-Ticket aufnimmt, Kundendaten per E-Mail oder Bildschirmfreigabe teilt oder auf andere Weise Zugriff auf die AWS-Umgebungen gewährt, die Kundendaten enthalten. Wenn der Kunde ein Support-Ticket öffnet, kann es notwendig sein, bestimmte Metadaten-Tags oder andere Metadaten zu verarbeiten, z. B. Ressourcenkennungen (Service-Attribute). Wenn der Kunde nicht möchte, dass AWS bei der Verarbeitung von Metatags oder ähnlichen Service-Attributen zum Nachweis des Supports personenbezogene Daten verarbeitet, kann der Kunde wählen, keine personenbezogenen Daten bei der Erstellung solcher Service-Attribute zu verwenden. Im Rahmen des regulären Supports (ii) müssen AWS-Supportteams zur Behebung von Problemen von lediglich auf AWS-Ressourcen (z. B. EC2-Instanzen) nicht jedoch auf die darin gespeicherten Kundeninhalte und -daten zugreifen. Denn etwaige Probleme werden nicht in der Kundenapplikation, sondern in der darunterliegenden Infrastruktur behoben. Für Supportleistungen ist es daher nicht notwendig, dass AWS auf Kundendaten zugreift. Für den unwahrscheinlichen Fall, dass ein Kunde dem AWS-Supportteam ausnahmsweise Einsicht in seine Kundendaten gewährt (iii), kontrolliert der Kunde hier selbst, welche (personenbezogenen) Daten für die Supportteams sichtbar sind. Zwar werden nach seiner expliziten Freigabe dem Supportteam temporäre AWS-interne Genehmigungen erteilt, um die erforderliche Hilfestellung zu leisten. Das Supportteam kann jedoch auch dann nur Informationen sehen, die der Kunde nicht verschlüsselt hat. Verschlüsselte Informationen sind nicht sichtbar. Ist es für die Supportleistung erforderlich, verschlüsselte Daten einzusehen, ist dies nur unter Mitarbeit des Kunden möglich.

2.8 Ist on premise-Speicherung sicherer als Speicherung bei AWS?

Kurzantwort: Nein, professionelle Cloud-Anbieter sind in der Regel sicherer als On-Premise-Lösungen.

Erläuterung:

Eine *On-Premise*-Lösung ist der Gegensatz zu einer Cloud. Bei *On-Premise* befinden sich Daten nicht auf extern gehosteten Servern, sondern werden im unternehmenseigenen Netzwerk administriert. Um bei *On-Premise-Lösungen* ein Daten- und IT-Sicherheitsniveau professioneller Cloud-Anbieter zu erreichen und aufrechtzuerhalten, ist unternehmensseitig in der Regel ein erheblicher Kosten- und Personalaufwand erforderlich. Die Architektur der Datenzentren von AWS ist weltweit identisch. So können als notwendig erkannte Sicherheitsverbesserungen sofort weltweit ausgerollt und das Sicherheitsniveau stets auf einem aktuellen Stand gehalten werden. AWS tätigt jährlich Ausgaben in Milliardenhöhe und beschäftigt Tausende von Mitarbeitern, um die Sicherheit ihrer Datenzentren

aufrechtzuerhalten. Ein solches Sicherheitsniveau ist im Rahmen einzelner On-Premise-Lösungen kaum zu erreichen.[12]

2.9 Kann ich AWS Rechenzentren auch für KRITIS-Anwendungen nutzen oder ist AWS KRITIS-zertifiziert?

Kurzantwort: Ja, man kann AWS Dienste für KRITIS-Anwendungen benutzen, AWS ist selbst nach ISO 27001 zertifiziert, um die vom BSI aufgestellten Anforderungen an eine KRITIS zu nachzuweisen.

Erläuterung:

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Nach § 8a Abs. 1 BSI-Gesetz (BSIG) müssen Betreiber kritischer Infrastrukturen organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse treffen. Der branchenspezifische Sicherheitsstandard (B3S), an dem u. a. auch AWS mitgewirkt hat, ist als Rahmenwerk aufgebaut und orientiert sich am Inhalt der ISO / IEC 27000-Familie.

Der Betrieb eines Informationssicherheits-Managementsystems (ISMS) z. B. nach ISO / IEC 27001:2013 ist für die Absicherung der Kritischen Infrastrukturen und deren Schutzziele erforderlich. Dies gilt auch, wenn die Leistungen (teilweise) durch Dritte erbracht werden. Für kritische Dienstleistungen relevante IT-Dienstleistungen, die von Dritten erbracht werden, müssen wirksame Verträge bzw. Dienstleistungsvereinbarungen nachweisbar sein. Prüfmöglichkeiten sind in Abhängigkeit von der Bedeutung der jeweiligen IT-Dienstleistung als möglicher Vertragsbestandteil vorzusehen. Eine Zertifizierung der für den Betrieb der relevanten IT-Systeme und Dienstleistungen nach ISO / IEC 27001 ist als Nachweis für die Erfüllung des §8a Abs. 1 BSIG hinreichend, solange der Gegenstand der Zertifizierung die für die kritische Dienstleistung relevanten Prozesse und Systeme umfasst. Auch ein bestandenes C5-Testat (vgl. Frage 2.2f.) wird vom BSI als Nachweis nach § 8a BSIG akzeptiert.

AWS ist als Erbringer einer kritischen Dienstleistung im Sektor Informationstechnik und Telekommunikation nach § 5 BSI-KritisV, nämlich der Bereitstellung von virtualisierten Servern im großen Umfang, selbst verpflichtet, die vorgenannten Nachweise gegenüber dem BSI zu erbringen und zu zeigen, dass AWS gegen Cyber-Angriffe adäquat gerüstet ist.

AWS macht für den Nachweis des Kunden ihre ISO 27001-Zertifizierung und *Statement of Applicability* verfügbar und verpflichtet sich gemäß Ziffer 10.2 des DPA vertraglich, mindestens diese Standards

---

[12] Der Nachrichtendienst Heise Online hat die Sicherheitskonzepte der bei Cloud-Plattformen in einem Bericht vom 02.11.2021 näher beleuchtet: https://www.heise.de/hintergrund/Cloud-Sicherheit-Konzepte-von-Amazon-Microsoft-und-Google-auf-dem-Pruefstand-6233294.html.

einzuhalten. Eine ggf. bestehende Pflicht des Kunden zur Dokumentation und Aufbau eines eigenen ISMS entfällt hierdurch jedoch nicht. Der Kunde muss außerdem berücksichtigen, ob für ihn weitere spezifische Branchenstandards gelten, die über B3S hinaus gehen.

3. Fragen zur Übermittlung in Drittländer

3.1 Ist es nach der DSGVO und aufgrund des sog. Schrems-II-Urteils des EuGHs verboten, AWS zu nutzen?

Kurzantwort: Nein. An der Möglichkeit, AWS Services im Einklang mit der DSGVO und deutschen Datenschutzbestimmungen zu nutzen, hat sich durch Schrems II nichts geändert.

Erläuterung:

Die sog. Schrems-II-Entscheidung des EuGH bezog sich auf Datenübermittlungen in sog. Drittländer. Der Einsatz von AWS bedeutet nicht automatisch, dass es zu Übermittlungen in die USA kommt, also in ein Drittland (vgl. hierzu Fragen 1.5, 1.7 und 2.4). Die Entscheidung hat im Zusammenhang mit AWS daher nur eingeschränkte Relevanz. Das EuGH-Urteil enthält kein Verbot, die Services von AWS zu nutzen. Es enthält auch kein Verbot, Daten in Drittländer zu übermitteln oder in Drittländern ansässige Dienstleister zu beauftragen. In seiner Entscheidung erklärt der EuGH allein den sog. EU-US-*Privacy-Shield* für unwirksam. In der Folge lässt sich die Zulässigkeit einer Datenübermittlung in ein Drittland bzw. der Einsatz von Auftragsverarbeitern in einem Drittland nicht mehr mit dem *Privacy Shield* begründen. Die Datenübermittlung ist jedoch nicht in jedem Fall unzulässig. Hierfür gelten weiterhin die Anforderungen des Kapitel V der DSGVO. So kann eine Datenübermittlung unter Verwendung der Standardvertragsklauseln und weiterer geeigneter Garantien weiterhin DSGVO-konform erfolgen. AWS ist so aufgestellt, dass diese Garantien erfüllt sein können. Dies führen wir in diesem Abschnitt 3 aus.

Die Ausführungen gelten nicht nur für „normale“ personenbezogene Daten, sondern auch für besondere Kategorien personenbezogener Daten wie Gesundheits- oder Sozialdaten.

3.2 Wenn ich als Speicherregion von AWS Frankfurt am Main oder eine andere europäische Region wähle, werden meine Daten dann trotzdem in die USA übermittelt?

Kurzantwort: Grundsätzlich nicht. Der Kunde hat die Kontrolle darüber, wohin seine Daten übermittelt werden.

Erläuterung:

AWS speichert und verarbeitet Daten ihrer Kunden grundsätzlich in der Region, die der Kunde ausgewählt hat (vgl. Frage 2.4). Wenige AWS Services beinhalten eine mögliche Übertragung von Kundendaten aus der gewählten Region heraus für Zwecke der Weiterentwicklung und Verbesserung der Services. Der Kunde kann die entsprechenden Services so einstellen, dass eine Übertragung nicht

erfolgt, oder die Services nicht einsetzen. Bei wenigen anderen Services ist die Übertragung von Kundendaten inhärent, weil sie wesentlicher Bestandteil des Services ist. Der Kunde kann daher wählen, ob und wofür er einen solchen Service einsetzt.

AWS hat eine Übersicht veröffentlicht, aus der ersichtlich ist, welche Services eine Übertragung von Kundendaten beinhalten können. AWS sperrt für den Kunden weder Regionen noch Services, denen eine Datenverarbeitung außerhalb der EU inhärent ist. Möchte der Kunde eine (regelmäßige) Drittlandsübermittlung im Rahmen der Nutzung der Services vermeiden, kann er die entsprechenden Services sperren. AWS hat hierfür Anleitungen zur Unterstützung ihrer Kunden veröffentlicht.

Obwohl AWS nicht ausschließen kann, dass sie Behördenanfragen aus Drittländern erhält und trotz der weitreichenden Verpflichtungen aus ihrem *Supplementary Addendum* Daten herausgeben muss, führt dieses theoretische Risiko nicht dazu, dass es unzulässig ist, AWS als Auftragsverarbeiter zu nutzen (vgl. Frage 3.3f).

Eine vom Kunden eingesetzte Verschlüsselung seiner Kundendaten ist für solche Fälle der effektive Schutz für Kunden, denn ohne entsprechende Entschlüsselungsschlüssel sind verschlüsselte Kundeninhalte nicht lesbar (vgl. auch Frage 2.5, 2.7, 3.4).

3.3 Können mit AWS die Anforderungen des BfArM an den Einsatz von Cloud-Anbietern durch DiGA-Hersteller erfüllt werden?

Kurzantwort: Ja. Durch die bestehenden vertraglichen Regelungen und individuelle Konfigurationen kann ein DiGA-Hersteller die Anforderungen erfüllen. Dem steht auch der CLOUD Act nicht entgegen.

Erläuterung:

3.3.1 Anforderungen des BfArM

Das BfArM verlangt im DiGA-Leitfaden von DiGA-Herstellern und ihren Auftragsverarbeitern *„hinreichende Gewähr für die Unterbindung einer Datenübertragung […] an das Mutterunternehmen“*. Neben der Verschlüsselung durch den Kunden (vgl. Frage 2.5) muss der jeweilige Dienstleister zusichern,

- dass keine Datentransfers in die USA und auch keine Datenverarbeitungen in den USA durchgeführt werden;
  - ➢ Der Kunde kann diese Anforderungen dadurch erfüllen, dass er seine Architektur und die AWS Services so konfiguriert und nutzt, dass die Auftragsdatenverarbeitung ausschließlich innerhalb der EU / des EWR erfolgt. Im Regelbetrieb kann eine Drittlandsübermittlung somit ausgeschlossen werden.
- dass auch im Fall von Herausgabeverlangen von US-Behörden keine Daten zur Verfügung gestellt und auch nicht an das Mutterunternehmen herausgegeben werden;
  - ➢ Als Antwort auf diese Anforderung sichert AWS in ihrem *Supplementary Addendum* zum DPA zu, Anfragen von Behörden abzulehnen und die Behörde an den Kunden direkt zu verweisen.

DIERKS + COMPANY

Weiterhin kann der Kunde die Erfüllung dieser Anforderung sicherstellen, indem er alle Daten verschlüsselt, sodass zu keinem Zeitpunkt unverschlüsselte Daten herausgegeben werden können.

- dass sie in jedem Fall eines Herausgabeverlangens den Rechtsweg beschreiten und ausschöpfen;
  - AWS verpflichtet sich in ihrem *Supplementary Addendum* zum DPA, jede überzogene oder unangemessene Anfrage anzufechten („*challenge any overboard or inappropriate Request*"), insbesondere wenn die Anfragen europäischem oder nationalem Recht widersprechen. Mit dieser Verpflichtung genügt AWS der Anforderung des BfArM.
- unverzüglich über das Bestehen des Verlangens sowie über die Abhilfemaßnahmen und mögliche Rechtsstreitigkeiten sowie deren Verfahrensstand und Fortschritt zu informieren.
  - Diese Anforderung erfüllt AWS, indem sie sich dazu verpflichtet, den Kunden unverzüglich über etwaige Anfragen zu informieren, soweit dies rechtlich zulässig ist. Darüber hinaus verpflichtet sich AWS, gegen etwaige Verfügungen vorzugehen, die ihr untersagen, den Kunden zu informieren.

Die Anforderungen des BfArM an die Einbindung von Cloud-Dienstleistern mit Konzernverbindungen in ein Drittland können beim Einsatz von AWS also erfüllt werden.

3.3.2 Zulässigkeit einer Drittlandsübermittlung

Das BfArM weist darauf hin, dass selbst im Fall eines höchstrichterlichen rechtskräftigen Urteils, das eine Herausgabepflicht bestätigt, Art. 48 DSGVO zu beachten ist, wonach ein Datentransfer nur erfolgen darf, wenn die Herausgabepflicht auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt ist. Als Ermächtigung für den Datentransfer i. S. d. Art. 48 DSGVO kann eine Ausnahme nach Art. 49 DSGVO in Betracht kommen.[13] Im Fall einer rechtskräftigen Herausgabeverpflichtung könnte die Übermittlung aufgrund Art. 49 Abs. 1 S. 1 lit. d oder S. 2 DSGVO zulässig sein:

Die Übermittlung von Daten in Drittstaaten wie die USA wäre gemäß Art. 49 Abs. 1 S. 1 lit. d DSGVO „*aus wichtigen Gründen des öffentlichen Interesses*" aufgrund von Anordnungen der US-Geheimdienste und der US-Strafverfolgungsbehörden unter dem Rechtsrahmen der zugrundeliegenden Gesetze zulässig. Ausweislich des Erwägungsgrundes 112 hat der Verordnungsgeber an „*den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten*" gedacht, einschließlich der „*Verringerung und/oder Beseitigung des Dopings im Sport*". Wenn bereits die Dopingbekämpfung die Übermittlung personenbezogener Daten ohne völkerrechtliche Grundlage an Drittländer ohne angemessenes Datenschutzniveau erlaubt, sollte dies erst recht für die Terrorismusbekämpfung

---

[13] Schröder, in: Kühling/Buchner (Hr.), DS-GVO BDSG, 3. Aufl. 2020, Art. 48 DSGVO Rn. 17.

gelten, zumal es in dieser Hinsicht einen starken Gleichklang zwischen den Interessen der EU und der USA gibt. Ferner sind diverse Straftaten im Zusammenhang mit internationalem Terrorismus nach deutschem Strafrecht unabhängig vom Tatort strafbar, sodass deren Verhinderung und Aufklärung im deutschen öffentlichen Interesse liegen. Es ist daher datenschutzrechtlich geboten, diese Fälle unter Art. 49 Abs. 1 Satz 1 lit. d DSGVO zu subsumieren.

Als weitere Rechtsgrundlage käme zudem Art. 49 Abs. 1 S. 2 DSGVO in Betracht. Diese kann sich ggf. aus dem CLOUD Act ergeben. Nach dem ***Clarifying Lawful Overseas Use of Data Act*** **(CLOUD Act)**, dort insbesondere der Vorschrift 18 U.S.C. § 2713, können US-Behörden unter bestimmten Voraussetzungen die Herausgabe von Daten verlangen, auch wenn diese außerhalb der USA gespeichert werden. Der CLOUD Act ändert respektive konkretisiert den *US Stored Communications Act* und bezweckt, die Zahl der Verfahren zu reduzieren, für die bislang ein internationales Rechtshilfeverfahren in Strafsachen notwendig war. Die Herausgabepflicht soll laut Angaben des US-Justizministeriums zur Beweiserlangung bei *„serious crime and terrorism“* dienen. Der CLOUD Act findet Anwendung im Rahmen der Strafverfolgung. Er enthält keine Befugnisse für Geheimdienste und dient nicht der Wirtschaftsspionage, Massenüberwachung, Vorratsspeicherung oder für *„fishing expeditions“*. Das Herausgabeverlangen erfordert in jedem Fall einen Beschluss des zuständigen US-Gerichts. Die im Kontext des CLOUD Act relevanten Instrumente sind *Warrant* (z. B. Durchsuchungsbefehle) und *Subpoena* (z. B. Herausgabeverfügungen). Der CLOUD-Act ist laut einer Handreichung des US-Justizministeriums *„encryption neutral“*. Das bedeutet, dass AWS nicht gerichtlich gezwungen werden kann, Daten zu entschlüsseln. AWS verarbeitet Daten nur nach Anweisung des Kunden (vgl. Frage 1.3).

Die gerichtlich angeordnete Herausgabepflicht kann sich an alle Anbieter elektronischer Kommunikationsdienstleistungen richten, nicht nur an Anbieter von Cloud-Services, mit Sitz in den USA, die Daten (gegebenenfalls über eine andere juristische Person) im Ausland verarbeiten und auf diese Verarbeitung im Ausland Einfluss haben. Das bedeutet, dass die US-amerikanische Muttergesellschaft von AWS theoretisch einem Herausgabeverlangen ausgesetzt sein kann, das Daten betrifft, die von AWS in der EU verarbeitet werden. Die angegangenen US-Anbieter haben die Möglichkeit eine solche richterliche Anordnung anzufechten, insbesondere wenn die Datenherausgabe eine Verletzung des am Ort der Datenhaltung geltenden nationalen Rechts hervorruft, hier also eine Verletzung von Unionsrecht und nationalem Recht der EU Mitgliedstaaten.

Die Übermittlung aufgrund eines Herausgabeverlangens nach dem CLOUD Act erfolgt somit nur in konkreten Einzelfällen in einem zeitlich begrenzten Umfang für einzelne Betroffene, die aufgrund eines Verdachts ausgewählt werden, an schweren Straftaten oder Angriffen auf die internationale Ordnung beteiligt zu sein. In dieser Konstellation werden die berechtigten Interessen der Betroffenen durchweg nicht überwiegen. Dies würde die Datenübermittlung in Einzelfällen in die USA aufgrund der Anforderungen durch US-Behörden nach dem CLOUD Acts gemäß Art. 49 Abs. 1 S. 2 DSGVO legitimieren.

DIERKS + COMPANY

Für die Anwendbarkeit des CLOUD Acts ist die Art und Weise (On-Premise oder in der Cloud) oder der Ort der Speicherung nicht von Bedeutung, sondern ob Zugriffsberechtigte als Adressaten des CLOUD Acts infrage kommen. Im Übrigen kann der CLOUD Act auch deutsche CSPs oder Anwendungsanbieter betreffen. Aufgrund der weitreichenden Formulierung des CLOUD Act hat dieser einen sehr umfassenden Anwendungsbereich. Er kann daher seinem Wortlaut nach aufgrund der globalen Zusammenhänge und Verflechtungen von Unternehmensstrukturen auch für deutsche oder europäische Anbieter jeglicher elektronischer Kommunikationsdienstleistungen gelten, die anderweitig (konzern-)verbundene Unternehmen in den USA haben oder Geschäftstätigkeiten dort nachgehen, und zwar unabhängig davon, ob sie Cloud-Dienste oder andere Kommunikationsdienstleistungen erbringen. Es ist daher möglich, dass auch Unternehmen, deren Muttergesellschaft ihren Sitz nicht in den USA haben, mit Herausgabeverlangen nach dem CLOUD Act konfrontiert werden.

3.4 Wie geht AWS mit Anfragen zur Informationsherausgabe von US-Behörden um?

Durch das *AWS Customer Agreement* sowie das DPA ziehen sich weitgehende Verpflichtungen von AWS, Kundendaten zu schützen. Insbesondere jedoch im *Supplementary Addendum* zum DPA verpflichtet sich AWS zu einem Maßnahmenbündel für den Fall von Anfragen zur Informationsherausgabe. AWS verpflichtet sich nur wirksame und rechtskräftige Anfragen zu beantworten, überzogene und unangemessene Anfragen anzufechten, insbesondere wenn diese Anfrage mit EU oder nationalem Recht kollidieren, und den Kunden über Anfragen zu informieren, soweit AWS dies nicht untersagt ist und AWS die Untersagung nicht durch angemessene rechtliche Schritte beseitigen kann, vgl. Ziffer 1 des *Supplementary Addendum* zum DPA. Durch diese Verpflichtung hat AWS eine vertragliche Maßnahme als zusätzliche Garantie im Sinne des Art. 46 DSGVO nach den Empfehlungen des *European Data Protection Boards* (EDPB) in der Folge der Schrems-II-Entscheidung des EuGH implementiert.

In vielen Fällen gelingt es AWS mit rechtlichen Gegenmaßnahmen, dass Anträge eingeschränkt oder ganz zurückgezogen werden. AWS veröffentlicht halbjährliche Berichte darüber, wie viele Anfragen AWS erhalten hat und ob und in welchem Umfang sie beantwortet wurden. Hieraus ist u. a. ersichtlich, dass in dem Berichtszeitraum keine der Anfragen zur Offenlegung von Unternehmensinhaltsdaten, die sich außerhalb der Vereinigten Staaten befinden, gegenüber der US-Regierung führte.

3.5 Bietet AWS mir neben den *Standard Contracual Clauses* hinreichend „geeignete Garantien" i. S. d. Schrems-II-Urteils?

Kurzantwort: Ja.

Erläuterung:

Der EuGH verlangt, dass neben den Standardvertragsklauseln geeignete Garantien i. S. d. Art. 46 DSGVO bestehen. Solche weiteren Maßnahmen können sowohl vertraglicher als auch technischer Natur sein (vgl. Empfehlungen des *European Data Protection Boards* (EDPB)).

Als vertragliche Maßnahme hat AWS nicht nur ihr *DPA* (vgl. hierzu Frage 1.2) angepasst, sondern es auch um das *Supplementary Addendum* zum DPA (vgl. hierzu insbesondere Frage 3.3.1) ergänzt, um den neuen Anforderungen gerecht zu werden. Die im Rahmen der Nutzung der verschiedenen AWS-Services eingesetzten (organisatorischen und technischen) Maßnahmen wählt im Rahmen des *Shared Responsibilty* Modells der Kunde. Die zahlreichen Tools, die AWS im Zusammenhang mit der DSGVO anbietet, können z. B. im GDPR Center und im DiGA-Leitfaden eingesehen werden. Insbesondere die Möglichkeit zur (kundenseitigen) Verschlüsselung der Daten stellt eine hinreichende (technische) Garantie dar (vgl. Abschnitt 2 zur Verschlüsselung und anderen Sicherheitsmaßnahmen).

So hat der französische *Conseil d'Etat* bereits vor Erlass der Empfehlungen des EDPB in zwei Entscheidungen im Nachgang zum Schrems-II-Urteil im Zusammenhang mit Auftragsverarbeitern mit Konzernverbindungen in die USA eine Verschlüsselung der Daten als hinreichende Garantie genügen lassen.[14] Diese Auffassung teilt auch das BfArM im Zusammenhang mit digitalen Gesundheitsanwendungen. Demnach ist unter Erfüllung der Voraussetzungen des § 4 Abs. 2 DiGAV auch der Einsatz von Dienstleistern wie AWS zulässig, die eine Konzernverbindung in die USA haben, wenn der DiGA-Hersteller zusätzliche technische, organisatorisch und vertraglicher Maßnahmen trifft (vgl. Frage 3.3f.). Das OLG Karlsruhe hat mit Beschluss vom 07.09.2022 erklärt, dass öffentliche Krankenhäuser einen Anbieter für digitales Entlassmanagement beauftragen dürfen, der die luxemburgischen Tochtergesellschaft eines US-amerikanischen Unternehmens als Hosting-Anbieterin einbindet, da bei entsprechenden vertraglichen Zusicherungen nicht davon auszugehen ist, dass Daten vertragswidrig in die USA übermittelt werden würden.[15]

AWS bietet mithin geeignete Garantien, die die Anforderungen des Art. 46 DSGVO nach dem Verständnis des EuGH erfüllen.

3.6 Ist es sinnvoll, Musterfragebögen für US-Anbieter oder Anbieter mit US-Bezug durch AWS ausfüllen zu lassen?

Kurzantwort: Nein.

Erläuterung:

Musterfragebögen sind nicht auf die konkrete Nutzung des Kunden der verschiedenen AWS-Services zugeschnitten. Bei AWS haben Kunden die Möglichkeit, aus einer Reihe von On-Demand-Services zu

---

[14] Beschluss N° 444937 vom 13,10.2020, abrufbar unter https://www.conseil-etat.fr/actualites/actualites/health-data-hub-et-protection-de-donnees-personnelles-des-precautions-doivent-etre-prises-dans-l-attente-d-une-solution-perenne, Entscheidung N° 450163 vom 12.03.2021, abrufbar unter https://www.conseil-etat.fr/en/news/the-urgent-applications-judge-does-not-suspend-the-partnership-between-the-ministry-of-health-and-doctolib-for-the-management-of-covid-19-vaccinati.

[15] Oberlandesgericht Karlsruhe, Beschluss vom 7.9.2022, Aktenzeichen: 15 Verg 8/22, https://oberlandesgericht-karlsruhe.justiz-bw.de/pb/,Lde/Startseite/Medien/Kein+Ausschluss+aus+Vergabeverfahren+wegen+Einbindung+der+luxemburgischen+Tochtergesellschaft+eines+US-amerikanischen+Unternehmens+als+Hosting-Anbieterin.

DIERKS + COMPANY

wählen, die von den Kunden bereitgestellt und konfiguriert werden können, um ihre Produkte/Serviceangebote zu erstellen. So liegt die Kontrolle darüber, wie Kundendaten gespeichert und gesichert werden, beim Kunden. Zudem hat AWs keinen Einblick darin, welche Daten der Kunde verarbeiten lässt. Aus diesen Gründen ist der Kunde deutlich besser in der Lage, die Fragebögen zu beantworten, sofern diese auf die konkrete Nutzung überhaupt anwendbar sind. Im Hinblick auf den US-Bezug hält AWS außerdem die Maßnahmen nach Frage 3.4f. vor.

***