ANHANG ZUR AWS-DATENVERARBEITUNG

Dieser Datenverarbeitungszusatz (**„DPA**“) ergänzt die AWS-Kundenvereinbarung, die unter verfügbar ist http://aws.amazon.com/agreement, wie von Zeit zu Zeit zwischen dem Kunden und AWS oder anderen aktualisiert Vereinbarung zwischen dem Kunden und AWS, die die Nutzung der Dienste durch den Kunden regelt (die **„Vereinbarung**“). Diese DPA ist eine Vereinbarung zwischen Ihnen und dem von Ihnen vertretenen Unternehmen (**„Kunde**“, **„Sie**“ oder **„Ihr**“) und Amazon Web Services, Inc. und die AWS-Vertragspartei bzw. die AWS-Vertragsparteien (sofern zutreffend) im Rahmen der Vereinbarung (zusammen **„AWS**“). Sofern in diesem DPA oder in der Vereinbarung nichts anderes definiert ist, sind alle Großgeschriebene Begriffe, die in dieser DPA verwendet werden, haben die ihnen in Abschnitt 17 dieser DPA zugewiesene Bedeutung.

1. Datenverarbeitung.

1.1 Umfang und Rollen. Diese DPA gilt, wenn Kundendaten von AWS verarbeitet werden. In diesem Zusammenhang fungiert AWS als Auftragsverarbeiter für den Kunden, der entweder als Verantwortlicher oder als Verantwortlicher fungieren kann Verarbeiter von Kundendaten.

1.2 Kontrollen durch den Kunden. Der Kunde kann die Servicekontrollen nutzen, um seine Verpflichtungen gemäß den geltenden Datenschutzgesetzen zu unterstützen, einschließlich der Verpflichtung, auf Anfragen von betroffenen Personen zu reagieren. Unter Berücksichtigung der Art der Verarbeitung erklärt sich der Kunde damit einverstanden, dass es unwahrscheinlich ist, dass AWS Kenntnis darüber erlangt, dass die vom Kunden über die Standardvertragsklauseln übermittelten Kundendaten ungenau oder veraltet sind. Sollte AWS jedoch erfahren, dass die über die Standardvertragsklauseln übermittelten Kundendaten ungenau oder veraltet sind, wird AWS den Kunden unverzüglich informieren. AWS wird mit dem Kunden zusammenarbeiten, um ungenaue oder veraltete Kundendaten, die über die Standardvertragsklauseln übermittelt wurden, zu löschen oder zu berichtigen, indem die Servicekontrollen bereitgestellt werden, die der Kunde zur Löschung oder Berichtigung der Kundendaten verwenden kann.

1.3 Einzelheiten zur Datenverarbeitung.

1.3.1 **Gegenstand.** Gegenstand der Datenverarbeitung gemäß dieser Datenverarbeitungsvereinbarung (DPA) sind die Kundendaten.

1.3.2 **Dauer.** Zwischen AWS und dem Kunden wird die Dauer der Datenverarbeitung gemäß dieser Datenverarbeitungsvereinbarung (DPA) vom Kunden festgelegt.

1.3.3 **Zweck.** Der Zweck der Datenverarbeitung gemäß dieser Datenverarbeitungsvereinbarung (DPA) ist die Bereitstellung der vom

Kunden gelegentlich angeforderten Dienste.

1.3.4 **Art der Verarbeitung.** Berechnung, Speicherung und andere Dienste, wie in der Dokumentation beschrieben und vom Kunden gelegentlich initiiert.

1.3.5 **Art der Kundendaten.** Kundendaten, die in den Diensten unter den AWS-Konten des Kunden hochgeladen werden.

1.3.6 **Kategorien der betroffenen Personen.** Die betroffenen Personen könnten Kunden, Mitarbeiter, Lieferanten und Endnutzer des Kunden umfassen.

1.4 Einhaltung der Gesetze. Jede Partei wird alle Gesetze, Vorschriften und Regelungen einhalten, die für sie in der Erfüllung dieses DPA gelten und verbindlich sind, einschließlich der geltenden Datenschutzgesetze.

2. Kundenanweisungen. Die Parteien vereinbaren, dass dieses DPA und die Vereinbarung (einschließlich der Anweisungen des Kunden über Konfigurationstools wie das AWS-Management-Console und APIs, die von AWS für die Dienste bereitgestellt werden) die dokumentierten Anweisungen des Kunden bezüglich der Verarbeitung der Kundendaten durch AWS darstellen (**„Dokumentierte Anweisungen**“). AWS wird die Kundendaten nur gemäß den dokumentierten Anweisungen verarbeiten (die, wenn der Kunde als Verarbeiter handelt, auf den Anweisungen seiner Verantwortlichen basieren könnten). Zusätzliche Anweisungen außerhalb des Rahmens der dokumentierten Anweisungen (sofern vorhanden) erfordern eine vorherige schriftliche Vereinbarung zwischen AWS und dem Kunden, einschließlich der Vereinbarung über zusätzliche Gebühren, die der Kunde an AWS für die Durchführung solcher Anweisungen zahlen muss. Der Kunde ist berechtigt, dieses DPA und die Vereinbarung zu kündigen, wenn AWS Anweisungen des Kunden, die außerhalb des Rahmens oder abweichend von den in diesem DPA gegebenen oder vereinbarten Anweisungen liegen, nicht befolgt. Unter Berücksichtigung der Art der Verarbeitung stimmt der Kunde zu, dass es unwahrscheinlich ist, dass AWS eine Meinung darüber bilden kann, ob dokumentierte Anweisungen gegen die geltenden Datenschutzgesetze verstoßen. Falls AWS eine solche Meinung bildet, wird es den Kunden umgehend informieren, in welchem Fall der Kunde berechtigt ist, seine dokumentierten Anweisungen zurückzuziehen oder zu ändern.

3. Vertraulichkeit der Kundendaten. AWS wird keine Kundendaten einsehen, verwenden oder an Dritte weitergeben, es sei denn, dies ist erforderlich, um die Dienste aufrechtzuerhalten oder bereitzustellen, oder um gesetzliche Anforderungen oder eine gültige und verbindliche Anordnung einer Behörde (wie eine Vorladung oder gerichtliche Anordnung) zu erfüllen. Wenn eine Behörde AWS zur Herausgabe von Kundendaten auffordert, wird AWS versuchen, die Behörde anzuweisen, die Daten direkt beim Kunden anzufordern. Im Rahmen dieses Versuchs kann AWS der Behörde die grundlegenden

Kontaktdaten des Kunden mitteilen. Wenn AWS gesetzlich gezwungen ist, Kundendaten an eine Behörde weiterzugeben, wird AWS dem Kunden eine angemessene Benachrichtigung über die Aufforderung geben, damit der Kunde eine Schutzanordnung oder ein anderes angemessenes Rechtsmittel anstreben kann, es sei denn, AWS ist gesetzlich daran gehindert.

4. **Vertraulichkeitsverpflichtungen des AWS-Personals.** AWS beschränkt ihr Personal darauf, Kundendaten nur mit Genehmigung von AWS zu verarbeiten, wie in den Sicherheitsstandards beschrieben. AWS legt geeignete vertragliche Verpflichtungen gegenüber ihrem Personal fest, einschließlich relevanter Verpflichtungen hinsichtlich Vertraulichkeit, Datenschutz und Datensicherheit.

5. Sicherheit der Datenverarbeitung

5.1 AWS hat die technischen und organisatorischen Maßnahmen für das AWS-Netzwerk gemäß den Sicherheitsstandards und diesem Abschnitt umgesetzt und wird diese aufrechterhalten. Insbesondere hat AWS die folgenden technischen und organisatorischen Maßnahmen umgesetzt und wird diese aufrechterhalten:

(a) Sicherheit des AWS-Netzwerks, wie in Abschnitt 1.1 der Sicherheitsstandards dargelegt;
(b) Physische Sicherheit der Einrichtungen, wie in Abschnitt 1.2 der Sicherheitsstandards dargelegt;
(c) Maßnahmen zur Kontrolle der Zugriffsrechte für autorisiertes Personal auf das AWS-Netzwerk, wie in Abschnitt 1.3 der Sicherheitsstandards dargelegt;
(d) Prozesse zum regelmäßigen Testen, Bewerten und Evaluieren der Wirksamkeit der von AWS implementierten technischen und organisatorischen Maßnahmen, wie in Abschnitt 2 der Sicherheitsstandards beschrieben.

5.2 Der Kunde kann sich entscheiden, technische und organisatorische Maßnahmen zum Schutz der Kundendaten zu implementieren. Solche technischen und organisatorischen Maßnahmen umfassen die folgenden, die der Kunde von AWS gemäß der Dokumentation oder direkt von einem Drittanbieter erhalten kann:

(a) Pseudonymisierung und Verschlüsselung zur Gewährleistung eines angemessenen Sicherheitsniveaus;
(b) Maßnahmen, die es dem Kunden ermöglichen, Daten angemessen zu sichern und zu archivieren, um im Falle eines physischen oder technischen Vorfalls die Verfügbarkeit und den Zugriff auf die

Kundendaten zeitnah wiederherzustellen;

(c) Prozesse zur regelmäßigen Prüfung, Bewertung und Überprüfung der Wirksamkeit der vom Kunden umgesetzten technischen und organisatorischen Maßnahmen.

6. Unterauftragsverarbeitung

6.1 **Autorisierte Unterauftragsverarbeiter.** Der Kunde erteilt allgemeine Genehmigung für die Nutzung von Unterauftragsverarbeitern durch AWS zur Durchführung von Verarbeitungsaktivitäten an Kundendaten im Auftrag des Kunden (**„Unterauftragsverarbeiter**“) gemäß diesem Abschnitt. Auf der AWS-Website (derzeit veröffentlicht unter https://aws.amazon.com/compliance/sub-processors/) sind die aktuell von AWS eingesetzten Unterauftragsverarbeiter aufgeführt. Mindestens 30 Tage bevor AWS einen Unterauftragsverarbeiter einsetzt, wird AWS die entsprechende Website aktualisieren und dem Kunden ein Verfahren zur Verfügung stellen, um eine Benachrichtigung über diese Aktualisierung zu erhalten. Um gegen einen Unterauftragsverarbeiter Einspruch zu erheben, kann der Kunde: (i) die Vereinbarung gemäß den Bedingungen kündigen; (ii) die Nutzung des Dienstes einstellen, für den AWS den Unterauftragsverarbeiter engagiert hat; oder (iii) die relevanten Kundendaten in eine andere Region verschieben, in der AWS den Unterauftragsverarbeiter nicht engagiert hat.

6.2 **Verpflichtungen der Unterauftragsverarbeiter.** Wenn AWS einen Unterauftragsverarbeiter gemäß Abschnitt 6.1 autorisiert:

(i) AWS wird den Zugriff des Unterauftragsverarbeiters auf die Kundendaten auf das notwendige Minimum beschränken, um die Dienstleistungen gemäß der Dokumentation bereitzustellen oder aufrechtzuerhalten, und AWS wird den Unterauftragsverarbeiter daran hindern, auf Kundendaten für andere Zwecke zuzugreifen;

(ii) AWS wird eine schriftliche Vereinbarung mit dem Unterauftragsverarbeiter eingehen und, soweit der Unterauftragsverarbeiter dieselben Datenverarbeitungsdienste erbringt, die AWS im Rahmen dieses DPA bereitstellt, wird AWS dem Unterauftragsverarbeiter dieselben vertraglichen Verpflichtungen auferlegen, die AWS unter diesem DPA hat;

(iii) AWS bleibt verantwortlich für die Einhaltung der Verpflichtungen aus diesem DPA und für alle Handlungen oder Unterlassungen des Unterauftragsverarbeiters, die dazu führen, dass AWS gegen eine der Verpflichtungen von AWS aus diesem DPA verstößt.

7. AWS Unterstützung bei Anfragen von betroffenen Personen. Unter Berücksichtigung der Art der Verarbeitung sind die Service Controls die technischen und organisatorischen

Maßnahmen, durch die AWS den Kunden bei der Erfüllung seiner Verpflichtungen zur Beantwortung von Anfragen von betroffenen Personen gemäß den geltenden Datenschutzgesetzen unterstützt. Wenn eine betroffene Person eine Anfrage an AWS stellt, wird AWS diese Anfrage umgehend an den Kunden weiterleiten, sobald AWS festgestellt hat, dass die Anfrage von einer betroffenen Person stammt, für die der Kunde verantwortlich ist. Der Kunde autorisiert AWS in seinem Namen und im Namen seiner Verantwortlichen, wenn der Kunde als Auftragsverarbeiter tätig ist, AWS, auf Anfragen von betroffenen Personen zu antworten und zu bestätigen, dass AWS die Anfrage an den Kunden weitergeleitet hat. Die Parteien stimmen darin überein, dass die Nutzung der Service Controls durch den Kunden und die Weiterleitung von Anfragen betroffener Personen durch AWS an den Kunden gemäß diesem Abschnitt den Umfang und die Reichweite der erforderlichen Unterstützung des Kunden darstellen.

8. Optionale Sicherheitsfunktionen. AWS stellt viele Service Controls zur Verfügung, die der Kunde nach Wahl nutzen kann. Der Kunde ist verantwortlich für (a) die Implementierung der in Abschnitt 5.2 beschriebenen Maßnahmen, soweit dies angebracht ist, (b) die ordnungsgemäße Konfiguration der Services, (c) die Nutzung der Service Controls, um die Verfügbarkeit und den Zugriff auf die Kundendaten im Falle eines physischen oder technischen Vorfalls zeitnah wiederherzustellen (zum Beispiel durch Backups und routinemäßige Archivierung der Kundendaten), und (d) die Ergreifung solcher Maßnahmen, die der Kunde für angemessen hält, um die Sicherheit, den Schutz und die Löschung der Kundendaten aufrechtzuerhalten, einschließlich der Nutzung von Verschlüsselungstechnologie zum Schutz der Kundendaten vor unbefugtem Zugriff und Maßnahmen zur Kontrolle der Zugriffsrechte auf die Kundendaten.

9. Sicherheitsvorfallbenachrichtigung.

9.1 **Sicherheitsvorfall.** AWS wird (a) den Kunden unverzüglich benachrichtigen, nachdem AWS von dem Sicherheitsvorfall Kenntnis erlangt hat, und (b) geeignete Maßnahmen ergreifen, um den Sicherheitsvorfall zu beheben, einschließlich Maßnahmen zur Minderung der durch den Sicherheitsvorfall verursachten nachteiligen Auswirkungen.

9.2 **AWS-Unterstützung**. Um dem Kunden zu ermöglichen, einen Sicherheitsvorfall an Aufsichtsbehörden oder betroffene Personen zu melden (je nach Anwendbarkeit), wird AWS mit dem Kunden zusammenarbeiten und ihn unterstützen, indem AWS in der Benachrichtigung gemäß Abschnitt 9.1(a) Informationen über den Sicherheitsvorfall bereitstellt, die AWS dem Kunden offenlegen kann, unter Berücksichtigung der Art der Verarbeitung, der verfügbaren Informationen bei AWS und etwaiger Einschränkungen bei der Offenlegung der Informationen, wie z.B. Vertraulichkeit. Unter Berücksichtigung der Art der Verarbeitung stimmt der Kunde zu, dass er am besten in der Lage ist, die voraussichtlichen Folgen eines Sicherheitsvorfalls zu bestimmen.

9.3 **Fehlgeschlagene Sicherheitsvorfälle.** Der Kunde stimmt zu, dass:

(i) ein fehlgeschlagener Sicherheitsvorfall nicht unter diesen Abschnitt 9 fällt. Ein fehlgeschlagener Sicherheitsvorfall ist ein Vorfall, der zu keinem unbefugten Zugriff auf Kundendaten oder auf die Ausrüstung oder Einrichtungen von AWS, die Kundendaten speichern, führt. Dazu können unter anderem Pings und andere Broadcast-Angriffe auf Firewalls oder Edge-Server, Port-Scans, erfolglose Anmeldeversuche, Denial-of-Service-Angriffe, Paket-Sniffing (oder anderer unbefugter Zugriff auf Verkehrsdaten, der nicht über die Header hinausgeht) oder ähnliche Vorfälle gehören.

(ii) Die Verpflichtung von AWS, einen Sicherheitsvorfall gemäß diesem Abschnitt 9 zu melden oder darauf zu reagieren, wird nicht als Anerkennung einer Schuld oder Haftung von AWS im Zusammenhang mit dem Sicherheitsvorfall ausgelegt oder betrachtet.

9.4 **Kommunikation.** Benachrichtigungen über Sicherheitsvorfälle, sofern vorhanden, werden von AWS auf einem oder mehreren Wegen an die Administratoren des Kunden übermittelt, einschließlich per E-Mail. Es liegt in der alleinigen Verantwortung des Kunden, sicherzustellen, dass die Administratoren des Kunden stets aktuelle Kontaktinformationen in der AWS-Managementkonsole pflegen und eine sichere Übertragung gewährleistet ist.

9.5 **Benachrichtigungspflichten.** Wenn AWS den Kunden über einen Sicherheitsvorfall informiert oder der Kunde auf andere Weise von einer unbeabsichtigten oder unrechtmäßigen Zerstörung, Verlust, Veränderung, unbefugten Offenlegung oder unbefugtem Zugriff auf Kundendaten Kenntnis erhält, ist der Kunde verantwortlich für (a) die Feststellung, ob sich daraus Benachrichtigungs- oder andere Verpflichtungen nach geltendem Datenschutzrecht ergeben, und (b) die notwendigen Maßnahmen zur Erfüllung dieser Verpflichtungen zu treffen. Dies schränkt die Verpflichtungen von AWS gemäß diesem Abschnitt 9 nicht ein.

10. AWS-Zertifizierungen und -Prüfungen.

10.1 **AWS ISO-Zertifizierung und SOC-Berichte.** Neben den in diesem DPA enthaltenen Informationen wird AWS auf Anfrage des Kunden und vorausgesetzt, dass die Parteien eine anwendbare NDA (Geheimhaltungsvereinbarung) abgeschlossen haben, die folgenden Dokumente und Informationen zur Verfügung stellen:

(i) die Zertifikate für die ISO 27001-Zertifizierung, die ISO 27017-Zertifizierung, die ISO 27018-Zertifizierung und die ISO 27701-Zertifizierung (oder die Zertifikate oder andere Dokumente, die die

Einhaltung solcher alternativer Standards nachweisen, die weitgehend äquivalent zu ISO 27001, ISO 27017, ISO 27018 und ISO 27701 sind); und

(ii) den System and Organization Controls (SOC) 1-Bericht, den System and Organization Controls (SOC) 2-Bericht und den System and Organization Controls (SOC) 3-Bericht (oder die Berichte oder andere Dokumente, die die von AWS implementierten Kontrollen beschreiben und die SOC 1, SOC 2 und SOC 3 ersetzen oder weitgehend äquivalent sind).

10.2 **AWS-Audits.** AWS beauftragt externe Prüfer, um die Angemessenheit seiner Sicherheitsmaßnahmen zu überprüfen, einschließlich der Sicherheit der physischen Rechenzentren, von denen AWS die Dienstleistungen bereitstellt. Dieses Audit: (a) wird mindestens einmal jährlich durchgeführt; (b) wird gemäß ISO 27001-Standards oder anderen alternativen Standards, die weitgehend äquivalent zu ISO 27001 sind, durchgeführt; (c) wird von unabhängigen Drittsicherheitsfachleuten nach Auswahl und auf Kosten von AWS durchgeführt; und (d) führt zur Erstellung eines Prüfberichts (**„Bericht**“), der AWSs vertrauliche Informationen darstellt.

10.3 **Auditberichte.** Auf schriftliche Anfrage des Kunden und vorausgesetzt, dass die Parteien eine geltende Vertraulichkeitsvereinbarung (NDA) abgeschlossen haben, wird AWS dem Kunden eine Kopie des Berichts zur Verfügung stellen, damit der Kunde die Einhaltung der Verpflichtungen von AWS gemäß dieser DPA angemessen überprüfen kann.

10.4 **Datenschutz-Folgenabschätzung und Vorabkonsultation.** Unter Berücksichtigung der Art der Verarbeitung und der Informationen, die AWS zur Verfügung stehen, wird AWS den Kunden bei der Erfüllung der Verpflichtungen im Hinblick auf Datenschutz-Folgenabschätzungen und Vorabkonsultationen unterstützen, indem AWS die Informationen bereitstellt, die AWS gemäß diesem Abschnitt 10 zur Verfügung stellt.

11. Kunden-Audits. Der Kunde kann ein Audit, einschließlich einer Inspektion, durchführen, die er gemäß den geltenden Datenschutzgesetzen oder den Standardvertragsklauseln auf eigene Rechnung und im Namen seiner Verantwortlichen (wenn der Kunde als Auftragsverarbeiter handelt) verlangen oder anordnen kann, indem er AWS anweist, das im Abschnitt 10 beschriebene Audit durchzuführen. Wenn der Kunde diese Anweisung bezüglich des Audits ändern möchte, hat er das Recht, eine Änderung der Anweisung durch die Übermittlung einer schriftlichen Mitteilung an AWS zu beantragen, wie im Vertrag vorgesehen. Wenn AWS sich weigert, einer Anweisung des Kunden bezüglich Audits, einschließlich Inspektionen, zu folgen, ist der Kunde berechtigt, den Vertrag gemäß den

Vertragsbedingungen zu kündigen.

12. Übermittlungen personenbezogener Daten.

12.1 **Regionen.** Der Kunde kann den Ort oder die Orte festlegen, an denen die Kundendaten innerhalb des AWS-Netzwerks verarbeitet werden (jeweils eine **„Region**"), einschließlich Regionen im EWR. Sobald der Kunde seine Auswahl getroffen hat, wird AWS die Kundendaten nicht aus den vom Kunden ausgewählten Regionen übertragen, es sei denn, dies ist erforderlich, um die vom Kunden initiierten Dienste bereitzustellen oder um gesetzlichen Anforderungen oder gültigen und verbindlichen Anordnungen einer Behörde nachzukommen.

12.2 **Anwendung der Standardvertragsklauseln.** Vorbehaltlich Abschnitt 12.3 gelten die Standardvertragsklauseln nur für Kundendaten, die dem GDPR unterliegen und die in ein Drittland (jeweils eine „Datenübertragung") übertragen werden, entweder direkt oder über eine Weiterübertragung.

12.2.1 Wenn der Kunde als Verantwortlicher handelt, gelten die Klauseln für die Übertragung von Verantwortlichem an Auftragsverarbeiter für eine Datenübertragung.

12.2.2 Wenn der Kunde als Auftragsverarbeiter handelt, gelten die Klauseln für die Übertragung von Auftragsverarbeiter an Auftragsverarbeiter für eine Datenübertragung. Unter Berücksichtigung der Art der Verarbeitung stimmt der Kunde zu, dass es unwahrscheinlich ist, dass AWS die Identität der Verantwortlichen des Kunden kennt, da AWS keine direkte Beziehung zu den Verantwortlichen des Kunden hat. Daher wird der Kunde die Verpflichtungen von AWS gegenüber den Verantwortlichen des Kunden gemäß den Klauseln für Auftragsverarbeiter übernehmen.

12.3 **Alternative Übertragungsmechanismen.** Die Standardvertragsklauseln finden keine Anwendung auf eine Datenübertragung, wenn AWS verbindliche Unternehmensregeln für Auftragsverarbeiter oder einen anerkannten alternativen Compliance-Standard für rechtmäßige Datenübertragungen eingeführt hat.

13. Kündigung des DPA. Dieses DPA bleibt in Kraft, bis die Vereinbarung beendet wird (das „Kündigungsdatum").

14. Rückgabe oder Löschung von Kundendaten. Bis zum Kündigungsdatum und für 90 Tage nach dem Kündigungsdatum wird AWS, vorbehaltlich der Bedingungen der Vereinbarung, die Kundendaten zurückgeben oder löschen, wenn der Kunde die

Servicekontrollen verwendet, um eine solche Rückgabe oder Löschung anzufordern. Spätestens am Ende dieses 90-Tage-Zeitraums wird der Kunde alle AWS-Konten, die Kundendaten enthalten, schließen.

15. Rückgabe oder Löschung von Kundendaten. Bis zum Kündigungsdatum und für 90 Tage nach dem Kündigungsdatum wird AWS, vorbehaltlich der Bedingungen der Vereinbarung, die Kundendaten zurückgeben oder löschen, wenn der Kunde die Servicekontrollen verwendet, um eine solche Rückgabe oder Löschung anzufordern. Spätestens am Ende dieses 90-Tage-Zeitraums wird der Kunde alle AWS-Konten, die Kundendaten enthalten, schließen.

16. Vollständige Vereinbarung; Konflikte. Diese DPA nimmt die Standardvertragsklauseln durch Verweis auf. Sofern nicht durch diese DPA geändert, bleibt die Vereinbarung in vollem Umfang in Kraft und Wirkung. Bei einem Konflikt zwischen der Vereinbarung und dieser DPA haben die Bedingungen dieser DPA Vorrang, es sei denn, die Servicebedingungen haben Vorrang vor dieser DPA. Nichts in diesem Dokument ändert oder modifiziert die Standardvertragsklauseln.

17. Definitionen. Sofern in der Vereinbarung nicht anders definiert, haben alle in dieser DPA verwendeten großgeschriebenen Begriffe die unten angegebenen Bedeutungen:

„API“ bedeutet eine Programmierschnittstelle.

„Anwendbares Datenschutzrecht“ bedeutet alle Gesetze und Vorschriften, die für die Verarbeitung von Kundendaten durch eine Partei gelten und verbindlich sind, einschließlich, soweit zutreffend, der DSGVO.

„**AWS-Netzwerk**“ bedeutet die Server, Netzwerkgeräte und Host-Software-Systeme (zum Beispiel virtuelle Firewalls), die unter der Kontrolle von AWS stehen und zur Bereitstellung der Dienste verwendet werden.

„**Verbindliche interne Datenschutzvorschriften**“ hat die im DSGVO festgelegte Bedeutung.

„Verantwortlicher“ hat die im DSGVO festgelegte Bedeutung.

„**Verantwortlicher-zu-Auftragsverarbeiter-Klauseln**“ bedeutet die Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern für Datenübermittlungen, die durch den Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021 genehmigt wurden und derzeit unter https://d1.awsstatic.com/Verantwortlicher_zu_Auftragsverarbeiter_SCCs.pdf erfügbar sind.
„Kundendaten“ bedeutet die personenbezogenen Daten, die in die Dienste unter den AWS-Konten des Kunden hochgeladen werden.

„Dokumentation“ bezeichnet die jeweils aktuelle Dokumentation für die Dienste, die unter http://aws.amazon.com/documentation (und allen von AWS benannten Nachfolgestellen) verfügbar ist.

„EEA“ steht für den Europäischen Wirtschaftsraum (European Economic Area).
„GDPR“ steht für die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und über den freien Verkehr solcher Daten sowie zur Aufhebung der Richtlinie 95/46/EG (Allgemeine Datenschutzverordnung).

„**Personenbezogene Daten**“ bezeichnet personenbezogene Daten, persönliche Informationen, persönlich identifizierbare Informationen oder einen anderen gleichwertigen Begriff (jeweils gemäß der anwendbaren Datenschutzgesetzgebung definiert).

„Verarbeitung“ hat die Bedeutung, die ihr in der DSGVO (GDPR) zugewiesen wird, und „verarbeiten“, „Verarbeitungen“ und „verarbeitet“ werden entsprechend interpretiert.

„Auftragsverarbeiter“ hat die Bedeutung, die ihm in der DSGVO (GDPR) zugewiesen wird.

„**Auftragsverarbeiter-zu-Auftragsverarbeiter-Klauseln**“ bezeichnet die Standardvertragsklauseln zwischen Auftragsverarbeitern für Datenübertragungen, die von der Europäischen Kommission in der Durchführungsentscheidung (EU) 2021/914 vom 4. Juni 2021 genehmigt wurden und derzeit unter https://d1.awsstatic.com/Auftragsverarbeiter_zu_Auftragsverarbeiter_SCCs.pdf zu finden sind.

„Region“ hat die Bedeutung, die in Abschnitt 12.1 dieser DPA angegeben ist.

„Sicherheitsvorfall“ bedeutet eine Verletzung der Sicherheit von AWS, die zur unbeabsichtigten oder rechtswidrigen Zerstörung, Verlust, Veränderung, unbefugten Offenlegung oder unbefugtem Zugriff auf Kundendaten führt.

„Sicherheitsstandards“ bedeutet die Sicherheitsstandards, die diesem DPA als Annex 1 beigefügt sind.

„Service Controls“ (Dienstkontrollen) bedeutet die Kontrollen, einschließlich Sicherheitsfunktionen und -merkmale, die die Dienste bereitstellen, wie in der Dokumentation beschrieben.
„Standardvertragsklauseln“ (Standard Contractual Clauses) bezeichnet (i) die Verantwortlicher-zu-Auftragsverarbeiter-Klauseln oder (ii) die Auftragsverarbeiter-zu Auftragsverarbeiter-Klauseln, je nach Anwendbarkeit gemäß den Abschnitten 12.2.1 und 12.2.2.

„**Drittland**“ bezeichnet ein Land außerhalb des EWR, das von der Europäischen Kommission nicht als Land mit einem angemessenen Schutzniveau für personenbezogene Daten anerkannt ist (wie im GDPR beschrieben).

Annex 1
Sicherheitsstandards

1. **Informationssicherheitsprogramm.** AWS wird ein Informationssicherheitsprogramm aufrechterhalten, das darauf ausgelegt ist, (a) es dem Kunden zu ermöglichen, Kundendaten gegen unbeabsichtigten oder rechtswidrigen Verlust, Zugriff oder Offenlegung abzusichern, (b) vernünftigerweise vorhersehbare Risiken für die Sicherheit und Verfügbarkeit des AWS-Netzwerks zu identifizieren und (c) physische und logische Sicherheitsrisiken für das AWS-Netzwerk zu minimieren, einschließlich durch regelmäßige Risikobewertungen und -tests. AWS wird einen oder mehrere Mitarbeiter benennen, die das Informationssicherheitsprogramm koordinieren und dafür verantwortlich sind.

   Das Informationssicherheitsprogramm von AWS wird folgende Maßnahmen umfassen:

   1.1 Logische Sicherheit.

   A. Zugriffskontrollen. AWS wird das AWS-Netzwerk nur autorisiertem Personal zugänglich machen und nur, soweit es zur Wartung und Bereitstellung der Dienste erforderlich ist. AWS wird Zugriffskontrollen und -richtlinien aufrechterhalten, um Autorisierungen für den Zugriff auf das AWS-Netzwerk von jedem Netzwerkanschluss und Benutzer zu verwalten, einschließlich der Verwendung von Firewalls oder funktional äquivalenter Technologie sowie Authentifizierungskontrollen. AWS wird Zugriffskontrollen aufrechterhalten, die darauf abzielen, (i) unautorisierten Zugriff auf Daten zu beschränken und (ii) die Daten jedes Kunden von den Daten anderer Kunden zu trennen.

   B. Eingeschränkter Benutzerzugang. AWS wird (i) den Benutzerzugang zum AWS-Netzwerk gemäß den Grundsätzen der minimalen Berechtigung basierend auf den Aufgaben der Mitarbeiter einrichten und einschränken, (ii) eine Überprüfung und Genehmigung vor der Gewährung von Zugriff auf das AWS-Netzwerk über die minimalen Berechtigungen, einschließlich Administrator-Konten, verlangen; (iii) eine mindestens vierteljährliche Überprüfung der Zugriffsberechtigungen für das AWS-Netzwerk erfordern und, falls erforderlich, die Zugriffsberechtigungen zeitnah widerrufen, und (iv) eine Zwei-Faktor-Authentifizierung für den Zugriff auf das AWS-Netzwerk von entfernten Standorten verlangen.

C. **Schwachstellenbewertung.** AWS wird regelmäßige externe Schwachstellenbewertungen und Penetrationstests des AWS-Netzwerks durchführen und identifizierte Probleme untersuchen sowie deren Behebung zeitnah verfolgen.

D. **Anwendungssicherheit.** Vor der öffentlichen Einführung neuer Dienste oder wesentlicher neuer Funktionen von Diensten wird AWS Sicherheitsüberprüfungen der Anwendungen durchführen, die darauf abzielen, Sicherheitsrisiken zu identifizieren, zu mindern und zu beheben.

E. **Änderungsmanagement.** AWS wird Kontrollen aufrechterhalten, die darauf ausgelegt sind, Änderungen an bestehenden AWS-Netzwerkressourcen zu protokollieren, zu genehmigen, zu testen, zu genehmigen und zu dokumentieren, und wird die Einzelheiten der Änderungen in seinen Änderungsmanagement oder Bereitstellungstools dokumentieren. AWS wird Änderungen gemäß seinen Änderungsmanagement-Standards testen, bevor sie in die Produktion überführt werden. AWS wird Prozesse aufrechterhalten, die darauf abzielen, unautorisierte Änderungen am AWS-Netzwerk zu erkennen und identifizierte Probleme bis zur Behebung nachzuverfolgen.

F. **Datenintegrität.** AWS wird Kontrollen aufrechterhalten, die darauf abzielen, die Datenintegrität während der Übertragung, Speicherung und Verarbeitung innerhalb des AWS-Netzwerks zu gewährleisten. AWS wird dem Kunden die Möglichkeit bieten, Kundendaten aus dem AWS-Netzwerk zu löschen.

G. **Business Continuity und Notfallwiederherstellung.** AWS wird ein formelles Risikomanagementprogramm aufrechterhalten, das darauf ausgelegt ist, die Kontinuität seiner kritischen Geschäftsabläufe zu unterstützen („Business Continuity Program“). Das Business Continuity Program umfasst Prozesse und Verfahren zur Identifizierung, Reaktion und Wiederherstellung nach Ereignissen, die die Bereitstellung der Dienste durch AWS verhindern oder wesentlich beeinträchtigen könnten (ein „BCP-Ereignis“). Das Business Continuity Program umfasst einen dreiphasigen Ansatz, den AWS zur Verwaltung von BCP-Ereignissen befolgen wird:

(i) **Aktivierungs- und Benachrichtigungsphase**. Wenn AWS Probleme identifiziert, die wahrscheinlich zu einem BCP-Ereignis führen könnten, wird AWS diese Probleme eskalieren, validieren und untersuchen. In dieser Phase wird AWS die Ursachen des BCP-Ereignisses analysieren.

(ii) **Wiederherstellungsphase.** AWS weist die zuständigen Teams an, Maßnahmen zu ergreifen, um die normale Systemfunktionalität wiederherzustellen oder die betroffenen Dienste zu stabilisieren.

(iii) **Rekonstitutionsphase.** Die AWS-Leitung überprüft die ergriffenen Maßnahmen und bestätigt, dass die Wiederherstellungsbemühungen abgeschlossen sind und die betroffenen Teile der Dienste und des AWS-Netzwerks wiederhergestellt wurden. Nach dieser Bestätigung führt AWS eine Nachanalyse des BCP-Ereignisses durch.

H. Vorfallmanagement. AWS wird Korrekturmaßnahmenpläne und Notfallpläne für die Reaktion auf potenzielle Sicherheitsbedrohungen für das AWS-Netzwerk aufrechterhalten. Die Notfallpläne von AWS enthalten definierte Prozesse zur Erkennung, Minderung, Untersuchung und Meldung von Sicherheitsvorfällen. Die Notfallpläne umfassen die Verifizierung von Vorfällen, Angriffsanalysen, Eindämmung, Datensammlung und Problemlösung. AWS wird ein AWS-Sicherheitsbulletin (ab dem Datum des Inkrafttretens, http://aws.amazon.com/security/security-bulletins/) führen, das sicherheitsrelevante Informationen veröffentlicht und kommuniziert, die die Dienste betreffen könnten, und Anleitungen zur Minderung der identifizierten Risiken bereitstellt.

I. Ausserbetriebnahme von Speichermedien. AWS wird einen Prozess zur Ausserbetriebnahme von Speichermedien aufrechterhalten, der vor der endgültigen Entsorgung der zur Speicherung von Kundendaten verwendeten Medien durchgeführt wird. Vor der endgültigen Entsorgung werden Speichermedien, die zur Speicherung von Kundendaten verwendet wurden, entmagnetisiert, gelöscht, gesäubert, physisch zerstört oder auf andere Weise gemäß branchenüblichen Standards saniert, um sicherzustellen, dass die Kundendaten nicht von dem betreffenden Speichermedium wiederhergestellt werden können.

1.2 Physische Sicherheit.

A. Zugangskontrollen. AWS wird (i) physische Schutzmaßnahmen implementieren und aufrechterhalten, die darauf abzielen, unbefugten physischen Zugang, Beschädigung oder Störung des AWS Netzwerks zu verhindern, (ii) geeignete Kontrollgeräte verwenden, um den physischen Zugang zum AWS Netzwerk nur autorisierten Personen mit einem berechtigten geschäftlichen Bedarf zu gestatten, (iii) den physischen Zugang zum AWS Netzwerk mit Hilfe von Eindringungserkennungssystemen überwachen, die darauf ausgelegt sind, Sicherheitsvorfälle zu überwachen, zu erkennen und geeignete Personen zu alarmieren, (iv) den physischen Zugang zum AWS Netzwerk protokollieren und regelmäßig auditieren und (v) regelmäßige Überprüfungen durchführen, um die Einhaltung dieser Standards zu validieren.

B. Verfügbarkeit. AWS wird (i) redundante Systeme für das AWS Netzwerk

implementieren, die darauf ausgelegt sind, die Auswirkungen eines Fehlers auf das AWS Netzwerk zu minimieren, (ii) das AWS Netzwerk so gestalten, dass es Hardwarefehler antizipieren und tolerieren kann, und (iii) automatisierte Prozesse implementieren, die darauf abzielen, den Datenverkehr der Kunden im Falle eines Hardwarefehlers von dem betroffenen Bereich wegzuleiten.

1.3 AWS-Mitarbeiter.

A. Mitarbeiterschulung zur Sicherheit. AWS wird Programme zur Schulung der Mitarbeiter in Bezug auf die Informationssicherheitsanforderungen von AWS implementieren und aufrechterhalten. Die Schulungsprogramme zur Sicherheitsbewusstsein werden mindestens einmal jährlich überprüft und aktualisiert.

B. Hintergrundüberprüfungen. Wo gesetzlich erlaubt und soweit von den zuständigen Regierungsbehörden verfügbar, wird AWS verlangen, dass jeder Mitarbeiter einer Hintergrundüberprüfung unterzogen wird, die für die jeweilige Position und das Zugriffslevel auf das AWS-Netzwerk angemessen und erforderlich ist.

2. Fortlaufende Bewertung. AWS wird regelmäßige Überprüfungen des Informationssicherheitsprogramms für das AWS-Netzwerk durchführen. AWS wird das Informationssicherheitsprogramm nach Bedarf aktualisieren oder ändern, um auf neue Sicherheitsrisiken zu reagieren und neue Technologien zu nutzen.