[AVVQKM017A]

vom 04.06.2021 / MMU

Vereinbarung

zwischen

……..

…..

- im Folgenden Auftraggeber -

und

Quickkonnect UG (haftungsbeschränkt)
Franz Joseph Straße 14
80801 München
- im Folgenden Auftragnehmer –

1. Gegenstand und Dauer des Auftrags

1. Gegenstand

Der Gegenstand des Auftrags ergibt sich aus den Nutzungsbedingungen zum Einsatz der QkMountain Software, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

Gegenstand des Auftrags zum Datenumgang ist die Durchführung des Betriebs der QkMountain Lösung durch den Auftragnehmer entsprechend der Leistungsvereinbarung.

2. Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

1. Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Daten werden für die Nutzung der QKMountain Plattform durch den Auftraggeber verarbeitet. Die Funktionen der QKMountain Lösung ergeben sich aus der Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Die Verlagerung in Drittländer zum Einsatz der in Ziffer 6 benannten Unterauftragnehmer ist von dem Auftraggeber genehmigt.

2. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

Personenstammdaten

Mitarbeiterstammdaten, einschließlich Sozialdaten

Kundendaten

Planungs- und Steuerungsdaten

Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

Daten der Ansprechpartner in Hotels und Partner

Standorte der Skilehrer (während der Buchung)

Buchungsrelevante Photos und Videos von Kunden für die Kunden. Dies wird an niemanden weitergeleitet außer diejenigen, die in den Medien aufgenommen wurden.

3. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Mitarbeiter

Kunden

Ansprechpartner in Hotels und bei Partnern

3. Technisch-organisatorische Maßnahmen

1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des

Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer werden Herr Florian Messerer und Herr von Halem benannt. florian@qkinnovations.com , cedric@qkinnovations.com .

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen

und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in **Anlage 1**].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

2. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung

des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Obono	Österreich	Beleg Erstellung mit QR-Code
Elda	Österreich	Automatische Weiterleitung and Versicherungsträger
Amazon Web Services	USA	Hosting der Anwendungsplattform

b) Der Wechsel der bestehenden Unterauftragnehmer

ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

3. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/ des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

5. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche ver-

traglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

   aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

   eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich

an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

3. Der Auftragnehmer hat keinerlei Zurückbehaltungsrechte an den überlassenen

personenbezogenen Daten und den zugehörigen Datenträgern. Der Auftraggeber kann ihre Herausgabe jederzeit verlangen.

4. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage – Technisch-organisatorische Maßnahmen

Datenverarbeitung beim Auftragnehmer

In unserem Büro steht die Sicherheit an erster Stelle, weshalb wir strenge Regeln eingeführt haben, die unser Team befolgt. Dazu gehört u. a., dass wir unsere Passwörter alle vier Wochen ändern und eine Zwei-Faktor-Authentifizierung für alle verwendeten Webdienste und Konten durchführen, um unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport zu verhindern. Darüber hinaus verwenden wir Sicherheitsdienste wie Cloudflare auf jeder von uns entwickelten Webseite, die Hacking verhindern und verdächtiges Verhalten melden.

Wir unterhalten ein Incident-Response-Management und eine Auftragskontrolle.

Schließlich sind alle unsere Produkte, Dienste, Backups auf den Servern von Amazon Web Services (AWS) in Frankfurt und Irland gehostet. AWS hat die höchsten Standards für Datenschutz und Datensicherheit.

Datenverarbeitung bei AWS

1. Informationssicherheitsprogramm. AWS unterhält ein Informationssicherheitsprogramm (einschließlich der Einführung und Durchsetzung interner Richtlinien und Verfahren), das dazu dient, (a) dem Kunden dabei zu helfen, seine Daten vor versehentlichem oder unrechtmäßigem Verlust, Zugriff oder Offenlegung zu schützen, (b) vernünftigerweise vorhersehbare und interne Risiken für die Sicherheit und den unbefugten Zugriff auf das AWS-Netzwerk zu identifizieren und (c) Sicherheitsrisiken zu minimieren, unter anderem durch Risikobewertung und regelmäßige Tests. AWS wird einen oder mehrere Mitarbeiter benennen, die das Informationssicherheitsprogramm koordinieren und dafür verantwortlich sind. Das Informationssicherheitsprogramm wird die folgenden Maßnahmen umfassen:

1.1 Netzwerksicherheit.

Das AWS-Netzwerk ist für Mitarbeiter, Auftragnehmer und alle anderen Personen, die für die Erbringung der Services erforderlich sind, elektronisch zugänglich. AWS wird Zugriffskontrollen und Richtlinien unterhalten, um zu verwalten, welcher Zugriff auf das AWS-Netzwerk von jeder Netzwerkverbindung und jedem Benutzer erlaubt ist, einschließlich der Verwendung von Firewalls oder funktional gleichwertiger Technologie und Authentifizierungskontrollen. AWS unterhält Pläne für Abhilfemaßnahmen und Reaktionen auf Vorfälle, um auf potenzielle Sicherheitsbedrohungen zu reagieren.

1.2 Physische Sicherheit

1.2.1 Physische Zugangskontrollen. Die physischen Komponenten des AWS-Netzwerks sind in nicht näher bezeichneten Einrichtungen (die "Einrichtungen") untergebracht. Physische Schrankenkontrollen werden eingesetzt, um den unbefugten

Zutritt zu den Einrichtungen sowohl an den Außengrenzen als auch an den Gebäudezugängen zu verhindern. Das Passieren der physischen Barrieren in den Einrichtungen erfordert entweder eine elektronische Zugangskontrolle (z. B. Kartenzugangssysteme usw.) oder eine Validierung durch menschliches Sicherheitspersonal (z. B. vertraglich vereinbarter oder interner Wachdienst, Empfangspersonal usw.). Mitarbeitern und Auftragnehmern werden Lichtbildausweise zugewiesen, die getragen werden müssen, während sich die Mitarbeiter und Auftragnehmer in einer der Einrichtungen aufhalten. Besucher müssen sich beim zuständigen Personal anmelden, sich ausweisen, erhalten einen Besucherausweis, den sie tragen müssen, wenn sie sich in den Einrichtungen aufhalten, und werden beim Besuch der Einrichtungen ständig von autorisierten Mitarbeitern oder Auftragnehmern begleitet.

1.2.2 Beschränkter Zugang für Mitarbeiter und Auftragnehmer. AWS gewährt denjenigen Mitarbeitern und Auftragnehmern Zugang zu den Einrichtungen, die einen legitimen geschäftlichen Grund für diese Zugangsrechte haben. Wenn ein Mitarbeiter oder Auftragnehmer kein geschäftliches Bedürfnis mehr für die ihm zugewiesenen Zugriffsrechte hat, werden die Zugriffsrechte unverzüglich entzogen, auch wenn der Mitarbeiter oder Auftragnehmer weiterhin ein Mitarbeiter von AWS oder seinen Verbundenen Unternehmen ist.

1.2.3 Physische Sicherheitsvorkehrungen. Alle Zugangspunkte (mit Ausnahme der Haupteingangstüren) werden in einem gesicherten (verschlossenen) Zustand gehalten. Die Zugangspunkte zu den Einrichtungen werden durch Videoüberwachungskameras überwacht, die alle Personen aufzeichnen, die die Einrichtungen betreten. AWS unterhält außerdem elektronische Einbruchserkennungssysteme, die darauf ausgelegt sind, unbefugten Zutritt zu den Einrichtungen zu erkennen, einschließlich der Überwachung von Schwachstellen (z. B. Haupteingangstüren, Notausstiegstüren, Dachluken, Türen von Verladerampen usw.) mit Türkontakten, Glasbruchvorrichtungen, Bewegungserkennung im Inneren oder anderen Vorrichtungen, die darauf ausgelegt sind, Personen zu erkennen, die versuchen, sich Zutritt zu verschaffen.

ISO/IEC 27001:2013:

ISO/IEC 27001:2013 ist ein Sicherheitsmanagement-Standard, der Best Practices für das Sicherheitsmanagement und umfassende Sicherheitskontrollen in Anlehnung an die ISO/IEC 27002 Best Practice Guidance festlegt. Die Grundlage dieser Zertifizierung ist die Entwicklung und Implementierung eines strengen Sicherheitsprogramms, das die Entwicklung und Implementierung eines Informationssicherheits-Managementsystems (ISMS) umfasst, das definiert, wie AWS die Sicherheit auf Dauer in einer ganzheitlichen, umfassenden Weise verwaltet. Dieser weithin anerkannte internationale Sicherheitsstandard legt fest, dass AWS Folgendes tut:

- Wir bewerten systematisch unsere Informationssicherheitsrisiken und berücksichtigen dabei die Auswirkungen von Bedrohungen und Schwachstellen.
- Wir entwerfen und implementieren eine umfassende Reihe von Informationssicherheitskontrollen und andere Formen des Risikomanagements, um Sicherheitsrisiken für Kunden und Architekturen zu begegnen.
- Wir verfügen über einen übergreifenden Managementprozess, um sicherzustellen, dass die Informationssicherheitskontrollen fortlaufend unseren Anforderungen entsprechen.

AWS verfügt über Zertifizierungen für die Einhaltung von ISO/IEC 27001:2013, 27017:2015 und 27018:2014. Diese Zertifizierungen werden von unabhängigen Dritt-Auditoren durchgeführt. Unsere Konformität mit diesen international anerkannten Standards und Verfahrensregeln ist ein Beweis für unser Engagement für die Informationssicherheit auf jeder Ebene unserer Organisation und dafür, dass das AWS-Sicherheitsprogramm mit branchenführenden Best Practices übereinstimmt.

SO/IEC 27018:2019:

SO/IEC 27018:2019 ist ein Verhaltenskodex, der sich auf den Schutz von personenbezogenen Daten in der Cloud konzentriert. Er basiert auf der ISO/IEC-Informationssicherheitsnorm 27002 und bietet eine Implementierungsanleitung für ISO/IEC 27002-Kontrollen, die für personenbezogene Daten (PII) in der öffentlichen Cloud gelten. Sie bietet auch eine Reihe zusätzlicher Kontrollen und zugehöriger Anleitungen, die dazu gedacht sind, die Anforderungen an den Schutz von PII in der Public Cloud zu erfüllen, die nicht durch die bestehenden ISO/IEC 27002-Kontrollen abgedeckt sind.

AWS hat sog. zusätzliche Maßnahmen zur Ergänzung der Standarddatenschutzklauseln nach den Vorgaben des Schrems 2 Urteils des Europäischen Gerichtshofs implementiert.