Auftragsverarbeitungsvertrag

Einführung
Die Parteien sind sich darüber einig, dass dieser Auftragsverarbeitungsvertrag ("**AVV**") die Rechte und Pflichten jeder Partei in Bezug auf die Verarbeitung und Sicherheit der personenbezogenen Daten des Kunden im Zusammenhang mit der von INCREASE YOUR SKILLS GmbH bereitgestellten Software und den Leistungen festlegt. Der AVV wird durch Verweis in die Allgemeinen Geschäftsbedingungen (AGB) aufgenommen. Die Parteien sind sich darüber hinaus einig, dass, sofern kein separater, von den Parteien unterzeichneter AVV existiert, dieser AVV die Verarbeitung und Sicherheit der personenbezogenen Daten des Kunden regelt.
Die Bestimmungen der AVV-Bedingungen ersetzen alle entgegenstehenden Bestimmungen der INCREASE YOUR SKILLS-Datenschutzerklärung, die andernfalls für die Verarbeitung personenbezogener Daten des Kunden gelten könnten. Aus Gründen der Klarheit und in Übereinstimmung mit den unten definierten Standardvertragsklauseln 2021 gilt, dass soweit diese Anwendung finden, die Standardvertragsklauseln 2021 Vorrang vor allen anderen Bestimmungen dieses AVV haben.

AUFTRAGSVERARBEITUNGSVERTRAG GÜLTIG AB 26. JANUAR 2024

1. Parteien

1.1 Kunde ist in den AGB definiert ("**Kunde**") und

1.2 **INCREASE YOUR SKILLS GmbH** (eingetragen unter HRB 33627 beim Amtsgericht Leipzig) mit Sitz in der Katharinenstraße 21, 04109 Leipzig, Deutschland ("**Anbieter**").

2. Allgemeines

2.1 Der Kunde und der Anbieter haben einen Vertrag geschlossen, der es erforderlich machen kann, dass der Anbieter personenbezogene Daten im Auftrag des Kunden verarbeitet.

2.2 Dieser Auftragsverarbeitungsvereinbarung ("AVV") legt die zusätzlichen Bedingungen und Regelungen fest, unter denen der Anbieter personenbezogene Daten bei der Erbringung seiner Leistungen im Rahmen des Vertrages verarbeiten wird. Dieser AVV enthält die obligatorischen Klauseln, die gemäß Art. 28 Abs. 3 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) sowie der korrespondieren gesetzlichen Regelungen im Vereinigten Königreich für Verträge zwischen dem für die Verarbeitung Verantwortlichen (Controller) und dem Auftragsverarbeiter (Processor) erforderlich sind.

2.3 Dieser AVV unterliegt den Bedingungen des Vertrags und ist Bestandteil des Vertrags. Die in diesem AVV verwendeten Begriffe haben die ihnen zugewiesene Bedeutung. Begriffe, die in diesem AVV nicht anderweitig definiert sind, haben die Bedeutung, die ihnen in den AGB des Vertrags gegeben wurde.

2.4 Etwaige Anhänge sind Teil dieses AVV dessen integraler Bestandteil. Jede Bezugnahme auf diesen AVV schließt seine Anhänge mit ein.

2.5 Im Falle eines Widerspruchs zwischen einer Bestimmung dieses AVV und einer oder mehrerer Bestimmungen des Vertrags haben in Bezug auf das Datenschutzrecht die Regelungen dieses AVV Vorrang.

3. Begriffsbestimmungen

Die folgenden Begriffe in diesem AVV haben die folgende Bedeutung:

“Datenschutzgesetze”	bezeichnet alle anwendbaren Gesetze und Vorschriften, die sich auf die Verarbeitung personenbezogener Daten zu irgendeinem Zeitpunkt während der Laufzeit dieses AVV beziehen, insbesondere (i) die Datenschutz-Grundverordnung (DSGVO, EU 2016/679, ("**DSGVO**"); (ii) die UK General Data Protection Regulation ("UK GDPR") in der Fassung des Data Protection Act 2018; (3) die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG, wie sie von den EU-Mitgliedstaaten umgesetzt wurde, sowie alle Nachfolgeregelungen und Umsetzungsrechtsakte und sonstigen Vorschriften, Leitfäden und Verhaltenskodizes in Bezug auf Datenschutz, in der jeweils aktuellen Fassung.
“Personenbezogene Daten des Kunden”	bezeichnet personenbezogene Daten, die vom Anbieter ausschließlich für die Zwecke der Erbringung von **Leistungen** und im Auftrag des Kunden verarbeitet werden.
“EWR”	bezeichnet den Europäischen Wirtschaftsraum, also die Mitgliedstaaten der Europäischen Union sowie Island, Liechtenstein und Norwegen.
“Standardvertragsklausel”	bezeichnet die Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten aus der Europäischen Union an Auftragsverarbeiter in Drittländern (Übermittlung von Daten an den für die Verarbeitung Verantwortlichen), die im Anhang des Beschlusses 2021/914/EU der Kommission vom 4. Juni 2021 enthalten sind und mit dem Nachtrag des Vereinigten Königreichs vom 21. März 2022 angenommen wurden.
“Unterauftragsverarbeiter”	ist ein vom Anbieter beauftragter Auftragnehmer, der im Rahmen der Leistungserbringung personenbezogene Daten verarbeitet.
"Verantwortlicher", "betroffene Person", "Auftragsverarbeiter", "Verarbeitung", "personenbezogene Daten",	haben die Bedeutung, die ihnen in der DSGVO sowie in den einschlägigen Datenschutzgesetzen im Vereinigten Königreich gegeben wird.

"Verletzung des Schutzes personenbezogener Daten"	

4. Verarbeitung von personenbezogenen Daten

4.1 Die Parteien erkennen an und vereinbaren, dass im Sinne der Datenschutzgesetze und im Hinblick auf die Verarbeitung personenbezogener Daten des Kunden der Anbieter der Auftragsverarbeiter und der Kunde der Verantwortliche ist.

4.2 Der Kunde garantiert und sichert zu, dass: (i) die Übermittlung personenbezogener Daten des Kunden an den Anbieter in jeder Hinsicht mit den Datenschutzgesetzen übereinstimmt (insbesondere im Einklang mit den Regeln über die Erhebung und Verwendung der Daten steht); und (ii) die Betroffenen der personenbezogenen Daten des Kunden nach Treu und Glauben und durch angemessene Hinweise über die Verarbeitung informiert wurden (und alle etwaig erforderlichen Zustimmungen dieser Betroffenen sowie alle relevanten Erlaubnisse und Genehmigungen eingeholt und aufrechterhalten wurden), soweit dies nach den Datenschutzgesetzen in Verbindung mit allen Verarbeitungsaktivitäten erforderlich ist, die vom Anbieter und seinen Unterauftragsverarbeitern in Übereinstimmung mit diesem Vertrag durchgeführt werden;

4.3 Der Anbieter verpflichtet sich, personenbezogene Daten des Kunden nur (i) soweit dies für die Erbringung der Leistungen erforderlich ist, (ii) in Übereinstimmung mit schriftlichen Anweisungen des Kunden und (iii) in Übereinstimmung mit den Anforderungen der Datenschutzgesetze zu verarbeiten.

4.4 Der Kunde hat bei der Nutzung der Leistungen die personenbezogenen Daten in Übereinstimmung mit den Anforderungen der Datenschutzgesetze zu verarbeiten. Der Kunde stellt sicher, dass alle Anweisungen an den Anbieter in Bezug auf die Verarbeitung von personenbezogenen Daten des Kunden den Datenschutzgesetzen entsprechen.

4.5 Die Anweisungen des Kunden an den Anbieter in Bezug auf den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Arten der personenbezogenen Daten und die Kategorien der betroffenen Personen sind in **Anhang A** beschrieben. Zur Vermeidung von Zweifeln erkennen die Parteien an und sind sich darüber einig, dass vorbehaltlich der Ziffer 5, die in diesem AVV und in **Anhang A** aufgeführten Verarbeitungsanweisungen eine vollständige und abschließende Auflistung der Anweisungen des Kunden an den Anbieter darstellen.

4.6 Der Anbieter hat den Kunden unverzüglich zu benachrichtigen, wenn eine vom Kunden erteilte Anweisung nach vernünftiger Einschätzung des Anbieters wahrscheinlich gegen die Datenschutzgesetze verstoßen würde.

4.7 Der Anbieter darf die personenbezogenen Daten des Kunden nicht verarbeiten, übertragen, modifizieren, ergänzen oder verändern oder die personenbezogenen Daten des Kunden an Dritte weitergeben oder deren Weitergabe an Dritte gestatten, sofern dies nicht durch die Bestimmungen dieses AVV gestattet ist.

4.8 Das Personal des Anbieters, das mit der Verarbeitung der personenbezogenen Daten des Kunden befasst ist, wird über die Vertraulichkeit der personenbezogenen Daten des Kunden informiert und erhält eine angemessene Schulung zu den datenschutzrechtlichen Pflichten und Verantwortlichkeiten. Das eingesetzte Personal unterliegt einer angemessenen Vertraulichkeitsverpflichtung.

4.9 In Anbetracht der Art der Verarbeitung personenbezogener Daten im Rahmen der erbrachten Leistungen muss der Anbieter gemäß Artikel 32 DSGVO geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit der Verarbeitung zu gewährleisten,

einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Änderung oder Beschädigung, unbefugter Offenlegung oder unbefugtem Zugriff auf die personenbezogenen Daten des Kunden. Die Parteien erkennen an und vereinbaren, dass die in diesem AVV und insbesondere in **Anhang B** aufgeführten Sicherheitsmaßnahmen die geeigneten technischen und organisatorischen Maßnahmen darstellen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Der Anbieter kann die technischen und organisatorischen Maßnahmen jederzeit ohne Vorankündigung ändern, solange er ein vergleichbares oder besseres Sicherheitsniveau sicherstellt. Einzelne Maßnahmen können durch neue Maßnahmen ersetzt werden, die dem gleichen Zweck dienen, ohne das Sicherheitsniveau zum Schutz personenbezogener Daten zu mindern.

4.10 Der Anbieter unterstützt den Kunden durch geeignete technische und organisatorische Maßnahmen, soweit dies unter Berücksichtigung der Art der Verarbeitung der personenbezogenen Daten des Kunden möglich ist, bei der Erfüllung der datenschutzrechtlichen Verpflichtungen des Kunden im Rahmen der Datenschutzgesetze, insbesondere im Zusammenhang mit der Geltendmachung von Rechten durch betroffene Personen, der Datenschutz-Folgenabschätzungen (im Zusammenhang mit der Nutzung der Leistungen des Anbieters durch den Kunden) sowie der Kommunikation mit Aufsichtsbehörden (jeweils in Verbindung mit einer Datenschutz-Folgenabschätzung im Zusammenhang mit den Leistungen des Anbieters).

4.11 Wenn betroffene Personen, zuständige Behörden oder sonstige Dritte vom Anbieter Informationen über die Verarbeitung personenbezogener Daten des Kunden verlangen, wird der Anbieter diese Anfragen an den Kunden weiterleiten, es sei denn Datenschutzgesetze verbieten eine solche Information; in diesem Fall wird der Anbieter den Kunden vorab über entgegenstehenden gesetzlichen Verpflichtung informieren, sofern dies dem Anbieter zumutbar und gestattet ist.

5. Unterauftragsverarbeiter

5.1 Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass der Anbieter im Zusammenhang mit der Erbringung von Leistungen die in **Anhang C** näher beschriebenen Unterauftragsverarbeiter einsetzen darf, bei denen es sich um verbundene Unternehmen des Anbieters und/oder Dritte handeln kann.

5.2 Der Kunde nimmt zur Kenntnis, dass der Anbieter die allgemeine Erlaubnis hat, neue Unterauftragsverarbeiter zu beauftragen, ohne eine weitere schriftliche, spezifische Erlaubnis des Kunden einzuholen. Voraussetzung hierfür ist, dass der Anbieter den Kunden dreißig (30) Tage vor der Verarbeitung der personenbezogenen Daten des Kunden schriftlich über die Identität des neuen Unterauftragsverarbeiters informiert.

5.3 Möchte der Kunde dem Einsatz des betreffenden Unterauftragsverarbeiter widersprechen, so hat er dies innerhalb von zehn (10) Werktagen nach Erhalt der Benachrichtigung durch den Anbieter schriftlich mitzuteilen. Erhebt der Kunde keine Einwände, so gilt dies als Zustimmung zum Einsatz des betreffenden Unterauftragsverarbeiters.

5.4 Falls der Kunde einem neuen Unterauftragsverarbeiter widerspricht, wird der Anbieter alle zumutbaren Anstrengungen unternehmen, um dem Kunden eine Änderung der Leistungen zur Verfügung zu stellen oder eine wirtschaftlich angemessene Abänderung der Leistungen empfehlen, um die Verarbeitung der personenbezogenen Daten des Kunden durch den betreffenden neuen Unterauftragsverarbeiter zu vermeiden. Sofern keine Alternative möglich ist, haben die Parteien das Recht, den Vertrag zu kündigen.

5.5 Die Mitteilung des Anbieters an den Kunden über einen neuen Unterauftragsverarbeiter umfasst auch die Bereitstellung eines aktualisierten **Anhang C**. Der Anbieter ist verpflichtet, **Anhang C** auf dem neuesten Stand zu halten.

5.6 Der Anbieter bleibt gegenüber dem Kunden für die Erfüllung der Verpflichtungen der Unterauftragsverarbeiter verantwortlich.

6. Datenübertragung

6.1 Gemäß Artikel 28 Abs. 3 (a) DSGVO darf der Anbieter keine personenbezogenen Daten des Kunden in Länder außerhalb des EWR oder des Vereinigten Königreichs (je nach Anwendbarkeit) übertragen und darf dies auch keinem Unterauftragsverarbeiter erlauben, es sei denn, es ist in dieser Vereinbarung vorgesehen. Um Zweifel auszuschließen, erklärt sich der Kunde hiermit mit der Übertragung und Verarbeitung der personenbezogenen Daten gemäß **Anhang A** einverstanden.

6.2 Der Anbieter erkennt an, dass im Einklang mit der DSGVO ein angemessener Schutz für die personenbezogenen Daten nach einer Übermittlung außerhalb des Vereinigten Königreichs oder des EWR (entweder direkt oder über die Weiterübermittlung durch einen Unterauftragsverarbeiter) bestehen muss, und schließt mit dem Kunden und/oder einem Unterauftragsverarbeiter entsprechende Vereinbarungen. Dazu gehören die geltenden Standardvertragsklauseln, es sei denn, es besteht ein anderer Angemessenheitsmechanismus für die Übermittlung (z.B. das EU-US-Data Privacy Framework).

7. Verletzung des Schutzes personenbezogener Daten

7.1 Im Falle einer Verletzung des Schutzes personenbezogener Daten, die personenbezogene Daten des Kunden betrifft, wird der Anbieter:

7.1.1 den Kunden unverzüglich (innerhalb von maximal 48 Stunden) benachrichtigen, damit der Kunde die Meldepflichten nach der DSGVO erfüllen kann, und den Kunden angemessen dabei unterstützen, wenn er einer betroffenen Person die Verletzung des Schutzes personenbezogener Daten mitteilen muss. Der Anbieter darf die relevanten Informationen schrittweise bereitstellen, sobald sie verfügbar sind. Eine entsprechende Benachrichtigung ist nicht als Eingeständnis eines Verschuldens oder einer Haftung seitens des Anbieters auszulegen.

7.1.2 angemessene Anstrengungen unternehmen, um die Ursache einer solchen Verletzung des Schutzes personenbezogener Daten zu ermitteln und alle Schritte unternehmen, die der Anbieter für angemessen und durchführbar hält, um die Ursache einer solchen Verletzung zu beheben.

7.1.3 vorbehaltlich der Bestimmungen dieses AVV, den Kunden dessen auf Verlangen, in angemessener Weise bei der Korrektur oder Behebung einer Verletzung des Schutzes personenbezogener Daten unterstützen.

8. Verzeichnis von Verarbeitungstätigkeiten

8.1 Soweit dies auf die Verarbeitung durch den Anbieter für den Kunden zutrifft, hat der Anbieter ein Verzeichnis über alle nach Artikel 30 Abs. 2 DSGVO erforderlichen Angaben zu führen und es dem Kunden auf Anfrage zur Verfügung zu stellen.

9. Kontrollbefugnisse

9.1 Der Anbieter stellt dem Kunden auf Anfrage angemessene Informationen zur Verfügung, die für den Nachweis der Einhaltung seiner Datenschutzverpflichtungen gemäß der Datenschutzgesetze erforderlich sind, und sorgt dafür, dass auch seine Unterauftragsverarbeiter diese Informationen zur Verfügung stellen, und gestattet dem Kunden oder einem vom Kunden beauftragten Prüfer Kontrollen, einschließlich der Inspektionen seiner Geschäftsräume, in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden, vorausgesetzt, dass ein solcher Prüfer kein Wettbewerber des Anbieters ist.

9.2 Der Kunde hat jede Kontrolle mindestens sechzig (60) Tage im Voraus anzukündigen, es sei denn es besteht eine kürzere Ankündigungsfrist aufgrund anwendbarer Datenschutzgesetze oder der Entscheidung einer zuständigen Datenschutzbehörde. Die Häufigkeit und der Umfang der Kontrollen werden von den Parteien nach Treu und Glauben einvernehmlich festgelegt.

9.3 Der Kunde trägt die Kosten für jede Kontrolle. Wird bei einer Prüfung festgestellt, dass der Anbieter gegen seine Verpflichtungen aus diesem AVV verstoßen hat, wird der Anbieter den Verstoß unverzüglich auf eigene Kosten beheben.

10. Laufzeit

10.1 Dieser AVV bleibt in vollem Umfang in Kraft und wirksam, solange:

10.1.1 Der Vertrag in Kraft bleibt; oder

10.1.2 Der Anbieter personenbezogene Daten des Kunden in seinem Besitz oder unter seiner Kontrolle hat.

10.2 Alle Bestimmungen dieses AVV, die ausdrücklich oder stillschweigend, bei oder nach Beendigung des Vertrages in Kraft treten oder fortbestehen sollen, um die personenbezogenen Daten des Kunden zu schützen, bleiben in vollem Umfang in Kraft und wirksam.

11. Rückgabe und Vernichtung der Daten

11.1 Der Anbieter wird auf schriftliche Aufforderung des Kunden nach Beendigung der Erbringung von Leistungen alle personenbezogenen Daten des Kunden löschen oder an den Kunden zurückgeben und vorhandene Kopien löschen, es sei denn, dass die Aufbewahrung der personenbezogenen Daten des Kunden gesetzliche zwingend ist. Geht keine schriftliche Aufforderung des Kunden ein, so löscht der Anbieter die personenbezogenen Daten des Kunden neunzig (90) Tage nach Beendigung des Vertrags.

11.2 Auf Verlangen des Kunden teilt der Anbieter schriftlich mit, welche Maßnahmen hinsichtlich der personenbezogenen Daten des Kunden getroffen wurden.

12. Haftung

12.1 Der Anbieter wird den Kunden von allen Kosten, Ansprüchen, Schäden oder Ausgaben freistellen, die dem Kunden aufgrund eines Verstoßes gegen datenschutzrechtliche Pflichten dieses AVV oder der Datenschutzgesetze gemäß Artikel 82 DSGVO durch den Anbieter oder seine Mitarbeiter, Unterauftragsverarbeiter, Subunternehmer oder Vertreter entstehen.

12.2 Ungeachtet anderslautender Bestimmungen in diesem AVV oder im Vertrag (insbesondere die Entschädigungsverpflichtungen einer Partei) ist keine Partei für Geldbußen verantwortlich, die gemäß Artikel 83 DSGVO von einer Aufsichtsbehörde oder staatlichen Stelle gegen die jeweils

andere Partei für Verstöße gegen Datenschutzgesetze dieser anderen Partei verhängt oder erhoben werden.

12.3 Vorbehaltlich der in Ziffer 12.1 dargelegten gesetzlichen Pflichten und der in Ziffer 12.2 dargelegten Beschränkungen unterliegt die Haftung jeder Partei im Rahmen dieses AVV den im Vertrag dargelegten Haftungsausschlüssen und -beschränkungen. Jede Bezugnahme auf eine "Haftungsbeschränkung" einer Partei im Vertrag ist so auszulegen, dass sie die gesamte Haftung einer Partei und aller ihrer Tochtergesellschaften und verbundenen Unternehmen im Rahmen des Vertrags und dieses AVV umfasst.

13. Dokumentation

13.1 Jede Partei ist für die Einhaltung ihrer Dokumentationspflichten verantwortlich, insbesondere für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten, soweit dies nach den Datenschutzgesetzen erforderlich ist.

Anhang A

Zwecke und Einzelheiten der Verarbeitung personenbezogener Daten

Gegenstand der Verarbeitung	Details	Gilt für:
Zweck Geben Sie alle Zwecke an, für die personenbezogenen Daten vom Anbieter verarbeitet werden	Systemzugang Systemverwaltung Lieferung von Systeminhalten entsprechend der abonnierten Module. Siehe unten:	Alle Kunden
	Richtlinien, Wissensüberprüfung	Kunden, die die Policy-Module (PolicyLite, MetaEngage und MetaPolicy) abonniert haben
	eLearning, sonstige Medien	Kunden, die die eLearning-Module (MetaLearning Fusion) abonniert haben
	Datenschutz-Umfragen	Kunden, die das MetaPrivacy-Modul abonniert haben
	Zwischenfallberichte	Kunden, die das MetaIncident-Modul abonniert haben
	Simulierte Phishing-Kampagnen	Kunden, die MetaPhish abonniert haben
	SCORM-Übertragung auf das Kunden-LMS	Kunden, die SCORM Übertragung abonniert haben
Arten von personenbezogenen Daten Geben Sie die personenbezogenen Daten an, die vom Anbieter verarbeitet werden	Vorname, Nachname, E-Mail-Adresse, Abteilung, Ausbildungsnachweis	Alle Kunden
	Active Directory Organisation Unit (OU)	Kunden, die Azure AD oder AD vor Ort verwenden
	LMS-Kennung	Kunden, die SCORM Übertragung abonniert haben
Kategorien von betroffenen Personen Geben Sie die Kategorien der betroffenen Personen an, deren personenbezogene Daten vom Anbieter verarbeitet werden	Mitarbeiter des Kunden, Auftragnehmer, Lieferanten, Partner und/oder verbundene Unternehmen.	Alle Kunden in Übereinstimmung mit den dem Anbieter zur Verfügung gestellten Daten der betroffenen Personen. Der Kunde kann dies je nach beabsichtigter Nutzung der Leistungen einschränken.

Gegenstand der Verarbeitung	Details	Gilt für:
Verarbeitende Tätigkeiten Spezifizieren Sie alle vom Anbieter durchzuführenden Verarbeitungstätigkeiten	Verarbeitung und Speicherung personenbezogener Daten von Kunden, um Konten Autorisierter Nutzer auf der MyCompliance-Plattform einzurichten und zu pflegen. Verteilung verschiedener Benachrichtigungs-E-Mails, die durch das MetaCompliance MyCompliance-System ausgelöst werden.	Alle Kunden
	Verteilung von simulierten Phishing-E-Mails, die vom Kunden über die MetaCompliance MyCompliance-Plattform initiiert wurden.	Kunden, die MetaPhish abonniert haben
	Speicherung von personenbezogenen Daten, wenn diese vom Kunden über das MetaCompliance MetaPrivacy-Modul eingegeben werden.	Kunden, die das MetaPrivacy-Modul abonniert haben
	Kommunikation mit dem Kunden-LMS und Auswertung der Lizenzanzahl	Kunden, die SCORM Übertragung abonniert haben
Ort der Verarbeitungsvorgänge Geben Sie alle Orte an, an denen die personenbezogenen Daten vom Anbieter verarbeitet werden	Vereinigtes Königreich (MetaCompliance Group ALSO von Microsoft Azure und Amazon Web Services, wie in Anhang C angegeben) Deutschland (MetaCompliance-Gruppe) Dänemark (MetaCompliance-Gruppe) Portugal (MetaCompliance-Gruppe) Irland (MetaCompliance Group ALSO von Microsoft Azure und Amazon Web Services wie in Anhang C angegeben). Holland (Microsoft Azure wie in Anhang C angegeben) Kanada (Microsoft Azure und Amazon Web Services wie in Anhang C angegeben)	Alle Kunden, soweit zutreffend. Weitere Einzelheiten finden Sie in Anhang C.
Anforderungen an die Aufbewahrung Geben Sie gegebenenfalls die Aufbewahrungsfrist für die vom Anbieter gespeicherten personenbezogenen Daten des Kunden an.	Wenn ein Kundenabonnement abgelaufen ist oder gekündigt wird, werden alle damit verbundenen personenbezogenen Daten des Kunden 90 Tage lang aufbewahrt, bevor sie tatsächlich gelöscht werden, um einen Datenverlust bei versehentlicher Kündigung zu verhindern.	Alle Kunden

Anhang B

Sicherheitsmaßnahmen

Der Anbieter ist verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten des Kunden zu ergreifen, um den Kunden bei der Erfüllung seiner rechtlichen Verpflichtungen zu unterstützen, einschließlich, aber nicht beschränkt auf, Sicherheitsmaßnahmen und Datenschutzrisikobewertungen. Die Maßnahmen müssen zu einem angemessenen Sicherheitsniveau führen, wobei das Folgende zu beachten ist:

(a) bestehende technische Möglichkeiten;

(b) die Kosten der Durchführung dieser Maßnahme;

(c) die besonderen Risiken, die mit der Verarbeitung der personenbezogenen Daten des Kunden verbunden sind; und

(d) die Sensibilität der personenbezogenen Daten der Kunden, die verarbeitet werden.

Der Anbieter sorgt für einen angemessenen Schutz der personenbezogenen Daten des Kunden. Der Anbieter schützt die personenbezogenen Daten des Kunden vor Zerstörung, Veränderung, unrechtmäßiger Verbreitung oder unrechtmäßigem Zugriff. Die personenbezogenen Daten des Kunden sind auch gegen alle anderen Formen der unrechtmäßigen Verarbeitung zu schützen. Unter Berücksichtigung des Stands der Technik und der Implementierungskosten und unter Berücksichtigung der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des unterschiedlich wahrscheinlichen und schwerwiegenden Risikos für die Rechte und Freiheiten natürlicher Personen müssen die vom Anbieter zu treffenden technischen und organisatorischen Maßnahmen Folgendes umfassen:

(a) die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten des Kunden;

(b) die Fähigkeit, die ständige Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste, die personenbezogene Daten des Kunden verarbeiten, zu gewährleisten;

(c) die Fähigkeit, die Verfügbarkeit und den Zugriff auf personenbezogene Daten des Kunden im Falle eines physischen oder technischen Zwischenfalls zeitnah wiederherzustellen; und

(d) ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Zusätzlich zu den oben genannten technischen und organisatorischen Maßnahmen ergreift der Anbieter die folgenden Maßnahmen:

(a) einen physischen Zugangsschutz, bei dem Computerausrüstung und entfernbare Daten, die personenbezogene Daten des Kunden enthalten, in den Räumlichkeiten des Anbieters unter Verschluss gehalten werden, wenn sie nicht überwacht werden, um sie vor unbefugter Nutzung, Beeinflussung und Diebstahl zu schützen.

(b) ein Verfahren zur Überprüfung der Rücklesung (*read back*) nach der Wiederherstellung personenbezogener Daten der Kunden aus Sicherungskopien.

(c) eine Berechtigungskontrolle, bei der der Zugriff des Anbieters auf die personenbezogenen Daten des Kunden durch ein technisches System der Berechtigungskontrolle verwaltet wird. Die Berechtigung ist auf diejenigen zu beschränken, die bestimmungsgemäß mit personenbezogenen Daten des Kunden arbeiten. Benutzerkennungen und Passwörter sind persönlich und dürfen nicht an andere Personen weitergegeben werden. Es müssen Verfahren für die Zuweisung und den Entzug von Berechtigungen vorhanden sein.

(d) Aufzeichnungen darüber führen, wer Zugang zu den personenbezogenen Daten des Kunden hat.

(e) eine sichere Kommunikation, bei der externe Datenkommunikationsverbindungen durch technische Funktionen geschützt werden, die sicherstellen, dass die Verbindung autorisiert ist, sowie durch eine Inhaltsverschlüsselung für Daten, die auf

Kommunikationskanälen außerhalb der vom Anbieter kontrollierten Systeme übertragen werden.

(f) ein Verfahren zur Gewährleistung einer sicheren Datenvernichtung, wenn ortsfeste oder entfernbare Speichermedien nicht mehr für ihren Zweck verwendet werden sollen.

(g) Routinen für den Abschluss von Vertraulichkeitsvereinbarungen mit Anbietern, die Reparatur- und Wartungsarbeiten an Geräten durchführen, die zur Speicherung personenbezogener Kundendaten verwendet werden.

(h) Routinen für die Überwachung der von Dritten in den Räumlichkeiten des Anbieters erbrachten Dienstleistungen. Die Speichermedien mit den personenbezogenen Daten des Kunden sind zu entfernen, wenn eine Überwachung nicht möglich ist.

Anhang C

Zugelassene Unterauftragsverarbeiter

Unterauftragsverarbeiter	**Standort**
Microsoft Azure (hostet die Dienste in der Cloud)	Holland Irland
Amazon Web Services (unter Vertrag mit "AWS Europe", als vertraglicher E-Mail Provider)	Irland
MetaCompliance Limited (bietet technischen Kundensupport und Kundenkonto-Support)	Vereinigtes Königreich
MOCH A/S, ein Unternehmen der MetaCompliance Group (Bereitstellung von Support-Dienstleistungen für Kunden)	Dänemark
MetaCompliance Ireland Ltd ist eine MetaCompliance-Gruppe (Bereitstellung von Support-Dienstleistungen für Kunden)	Irland
MetaCompliance Ireland Ltd Sucursal Portugal - part of the MetaCompliance Group (providing support services to customers)	Portugal