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 vom Anbieter 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 betreffen die Tätigkeit des Anbieters als Auftragsverarbeiter personenbezogener Kundendaten im Rahmen der Bereitstellung der Software und Dienstleistungen („**Gegenstand der Vereinbarung**"). Die AVV-Bedingungen haben Vorrang vor etwaigen entgegenstehenden Bestimmungen der Datenschutzrichtlinie der MetaCompliance Group, soweit diese den Gegenstand der Vereinbarung betreffen. 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 7. Juli 2025

1. Parteien

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

1.2 Der Anbieter ist wie in den AGB definiert ("**Anbieter**").

2. Allgemeines

2.1 Der Kunde und der Anbieter haben einen Vertrag geschlossen, der den Anbieter verpflichtet, personenbezogene Daten im Auftrag des Kunden zu verarbeiten.

2.2 Dieser Auftragsverarbeitungsvertrag ("AVV") legt die zusätzlichen Bedingungen und Regelungen fest, unter denen der Anbieter personenbezogene Daten bei der Erbringung seiner Leistungen im Rahmen des Vertrages verarbeitet sowie die Pflichten des Kunden im Hinblick auf diese personenbezogenen Daten und bestimmte andere personenbezogene Daten, die er gegebenenfalls vom Anbieter im Rahmen des Vertrages erhält. 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 und 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 den Gegenstand der Vereinbarung 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. Hierzu gehören insbesondere, soweit anwendbar: (1) die Datenschutz-Grundverordnung EU 2016/679 ("**DSGVO**"); (2) die Datenschutzgesetze von 1988 bis 2018 in ihrer jeweils gültigen Fassung (3) das britische Datenschutzgesetz von 2018 ("**DPA2018**") (4) die britische Datenschutz-Grundverordnung im Sinne des DPA2018 ("**UK GDPR**"); (5) die britische Verordnung über Datenschutz und elektronische Kommunikation von 2003 ("**EG-Richtlinie**"); und/oder (6) die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG ("**ePrivacy-Richtlinie**"), 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 und zwar entweder ausdrücklich durch den Abschluss des Vertrags und/oder durch die Konfiguration und Nutzung der im Rahmen der Leistungen bereitgestellten Software.
“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.
„Angemessenheitsbeschluss“	bezeichnet den Angemessenheitsbeschluss der Europäischen Kommission in Bezug auf die Übermittlung personenbezogener Daten in das Vereinte Königreich, der am 28. Juni 2021 angenommen wurde.
“Unterauftragsverarbeiter”	ist ein vom Anbieter beauftragter Auftragnehmer, der im Rahmen der Leistungserbringung personenbezogene Daten verarbeitet.
"Verantwortlicher", "betroffene Person", "Auftragsverarbeiter", "Verarbeitung", "personenbezogene Daten", "Verletzung des Schutzes personenbezogener Daten"	haben die Bedeutung, die ihnen in der DSGVO gegeben wird.

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 zur Erbringung der Leistungen 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 und dem Anbieter auf Anforderung nachgewiesen werden können), soweit dies nach den Datenschutzgesetzen in Verbindung mit allen Verarbeitungsaktivitäten erforderlich ist, die vom Anbieter und seinen Unterauftragsverarbeitern in Übereinstimmung mit diesem AVV und dem Vertrag durchgeführt werden;

4.3 Bei der Erbringung der Leistungen verarbeitet der Anbieter personenbezogene Daten des Kunden: (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.

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 Hinsichtlich der personenbezogenen Daten des Kunden gelten 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 vereinbaren, dass vorbehaltlich der Ziffer 5 und ergänzend zu den in diesem AVV und in **Anhang A** aufgeführten Verarbeitungsanweisungen, der Kunde auch durch die direkte

Nutzung und Konfiguration der Leistungen weitere Anweisungen zur Verarbeitung personenbezogener Daten erteilen kann.

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 Hinsichtlich des Gegenstands der Vereinbarung darf der Anbieter 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 Zuständigkeiten. 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.

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 Betroffenenrechten, der Durchführung von Datenschutz-Folgenabschätzungen (im Zusammenhang mit der Nutzung der MetaCompliance-Leistungen durch den Kunden) sowie der Kommunikation mit Aufsichtsbehörden (jeweils in Verbindung mit einer Datenschutz-Folgenabschätzung im Zusammenhang mit den MetaCompliance-Leistungen).

4.11 Hinsichtlich des Gegenstands der Vereinbarung gilt, dass wenn betroffene Personen, zuständige Behörden oder sonstige Dritte vom Anbieter Informationen über die Verarbeitung personenbezogener Daten des Kunden verlangen, der Anbieter diese Anfragen an den Kunden weiterleitet, es sei denn Datenschutzgesetze verbieten eine solche Information; in diesem Fall wird der Anbieter den Kunden vorab über entgegenstehende gesetzliche Verpflichtung informieren, sofern dies dem Anbieter zumutbar und gestattet ist.

4.12 Der Kunde nimmt zur Kenntnis, dass er im Rahmen und in Verbindung mit dem Vertrag personenbezogene Daten vom Anbieter erhält (einschließlich, aber nicht beschränkt auf Informationen zu beim Anbieter, dessen Subunternehmern und Lieferanten eingesetzten Personen sowie über betroffene Personen, die durch Bild- oder Tonaufnahmen identifizierbar sind, welche über bestimmte Dienste des Anbieters bereitgestellt werden). Der Kunde bestätigt, dass er diese personenbezogenen Daten als eigenständig Verantwortlicher verarbeitet und dabei die sämtlichen geltenden Datenschutzgesetze einhält.

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 B** und **Anhang C** näher beschriebenen Unterauftragsverarbeiter einsetzen darf, bei denen es sich um verbundene Unternehmen des Anbieters und/oder Dritte handeln kann. Die Beauftragung solcher Parteien durch den Anbieter erfolgt auf Grundlage eines schriftlichen (einschließlich in elektronischer Form geschlossenen) Vertrags, der im Hinblick auf die erforderliche Verarbeitung personenbezogener Daten den Bestimmungen dieses AVV entspricht.

5.2 Der Kunde nimmt zur Kenntnis, dass der Anbieter die allgemeine Erlaubnis zur Beauftragung der in **Anhang C** aufgeführten Unterauftragsverarbeiter hat und berechtigt ist, neue Unterauftragsverarbeiter hinzuzufügen (oder zu entfernen), ohne eine weitere schriftliche, spezifische Erlaubnis des Kunden einholen zu müssen. 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 (die „**Benachrichtigungsfrist**“).

5.3 Möchte der Kunde dem Einsatz des betreffenden Unterauftragsverarbeiter widersprechen, so hat er dies innerhalb der Benachrichtigungsfrist schriftlich mitzuteilen. Die Mitteilung muss Angaben zu den geltend gemachten Sicherheitsrisiken oder sonstigen Risiken im Zusammenhang mit dem neuen Unterauftragsverarbeiter enthalten. Erhebt der Kunde innerhalb der Benachrichtigungsfrist 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 die Bedenken auszuräumen, dem Kunden eine Leistungsänderung anbieten 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 mit sofortiger Wirkung zu kündigen, ohne dass eine Haftung entsteht oder Rückzahlungen durch den Anbieter zu leisten sind.

5.5 Die Mitteilung des Anbieters an den Kunden über einen neuen Unterauftragsverarbeiter umfasst die Bereitstellung eines aktualisierten **Anhangs C**. Der Anbieter ist verpflichtet, **Anhang C** über die folgende Webseite MetaCompliance Sub-Processors | MetaCompliance 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** und **Anhang C** einverstanden, sofern diese Anwendung finden.

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 gültiger 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.

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 auf dessen Verlangen, in angemessener Weise bei der Korrektur oder Behebung einer Verletzung des Schutzes personenbezogener Daten zu 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 aus diesem AVV erforderlich sind, und sorgt dafür, dass auch seine Unterauftragsverarbeiter diese Informationen zur Verfügung stellen. Der Anbieter 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.

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 Sofern die personenbezogenen Daten des Kunden nicht bereits gemäß den Bestimmungen des Vertrages gelöscht wurden, löscht oder gibt der Anbieter nach Wahl des Kunden und auf dessen schriftliches Verlangen sämtliche personenbezogene Daten des Kunden nach Beendigung der Leistungserbringung im Zusammenhang mit der Verarbeitung zurück und löscht alle vorhandenen Kopien, 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 Soweit gesetzlich nach Artikel 82 DSGVO erforderlich und vorbehaltlich der Regelung in Ziffer 12.2 dieses AVV, leistet der Anbieter dem Kunden Entschädigung für nachgewiesene Kosten, Ansprüche, Schäden oder Ausgaben, die dem Kunden aufgrund eines Verstoßes gegen die Bestimmungen dieses AVV oder die Datenschutzgesetze durch den Anbieter oder seine Mitarbeiter, Unterauftragsverarbeiter, Subunternehmer oder Vertreter entstehen. Eine darüber hinausgehende Freistellungsverpflichtung des Anbieters besteht nicht.

12.2 Ungeachtet anderslautender Bestimmungen in diesem AVV oder im Vertrag (insbesondere die Entschädigungsverpflichtungen einer Partei) haftet keine der Parteien für Bußgelder, die gemäß den Datenschutzgesetzen von einer Aufsichtsbehörde oder staatlichen Stelle gegen die jeweils andere Partei wegen eines Verstoßes gegen Datenschutzgesetze verhängt oder erhoben werden.

12.3 Der Kunde verpflichtet sich, den Anbieter von sämtlichen direkten Kosten, Ansprüchen, Schäden oder Aufwendungen freizustellen, die dem Anbieter infolge eines Verstoßes des Kunden gegen seine Pflichten aus diesem AVV oder den Datenschutzgesetzen entstehen (einschließlich, aber nicht beschränkt auf einen Verstoß gegen Ziffer 4.2 dieses AVV).

12.4 Soweit gesetzlich zulässig und vorbehaltlich der in Ziffer 12.12 dargelegten Beschränkungen, unterliegt die Gesamthaftung jeder Partei im Rahmen dieses AVV den im Vertrag dargelegten Haftungsausschlüssen und -beschränkungen.

13. Rechtswahl und Gerichtsstand

13.1 Dieser AVV unterliegt dem Recht der Bundesrepublik Deutschland. Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist, soweit gesetzlich zulässig Leipzig, Deutschland.

Anhang A

Zwecke und Einzelheiten der Verarbeitung personenbezogener Daten

Gegenstand der Verarbeitung	Details	Gilt für:
Zweck	Systemzugang Systemverwaltung	Alle Kunden

Gegenstand der Verarbeitung	Details	Gilt für:
	Lieferung von Systeminhalten entsprechend der abonnierten Module. Siehe unten:	
	Richtlinien, Wissensüberprüfung	Kunden, die Policy-Module (PolicyLite, MetaEngage und MetaPolicy) abonniert haben
	eLearning, sonstige Medien	Kunden, 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-Transfer auf das Kunden-LMS	Kunden, die SCORM-Transfer abonniert haben
	Statische PDF-Dokumente in ein effektives Schulungserlebnis umwandeln	Kunden, die Content to Course abonniert haben
	Kundenskripte in ein kurzes, KI-generiertes Video umwandeln	Kunden, die Virtual Presenter Video abonniert haben
Arten von personenbezogenen Daten	Vorname, Nachname, E-Mail-Adresse, IP-Adresse, Abteilung, Ausbildungsnachweis	Alle Kunden
	Active Directory Organisation Unit (OU)	Kunden, die Azure AD oder AD vor Ort verwenden
	LMS-Kennung	Kunden, die SCORM-Transfer abonniert haben
	Personenbezogene Daten, die der Kunde in den Kundendaten angegeben hat.	Alle Kunden
Benutzung von KI	KI-generierte Erstellung von Phishing-E-Mails	Kunden mit Premium Plus Security Awareness-Paketen (einschließlich Mehrsprachenangebot), die Phish Co-Pilot verwenden.
	KI-Kursersteller	Kunden, die das Add-on Content to Course abonniert haben.
	KI-generierte personalisierte Videos	Kunden, die das Add-on Virtual Presenter abonniert haben.
Kategorien von betroffenen Personen	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

Gegenstand der Verarbeitung	Details	Gilt für:
		beabsichtigter Nutzung der Leistungen einschränken.
Verarbeitende Tätigkeiten	Verarbeitung und Speicherung personenbezogener Daten von Kunden, um Konten Autorisierter Nutzer auf der MyCompliance-Plattform einzurichten und zu pflegen. Versand verschiedener Benachrichtigungs-E-Mails, die durch das MetaCompliance MyCompliance-System ausgelöst werden.	Alle Kunden
	Versand von simulierten Phishing-E-Mails, die vom Kunden über die MetaCompliance MyCompliance-Plattform initiiert wurden.	Kunden, die das MetaPhish-Modul 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-Transfer abonniert haben
	KI-Fähigkeiten nutzen	Kunden, die Phish Co-Pilot, Content to Course und Virtual Presenter abonniert haben.
Ort der Verarbeitungsvorgänge	Ort der Verarbeitungsvorgänge der MetaCompliance Group: Vereinigtes Königreich Dänemark Portugal Deutschland Irland	Alle Kunden
	Standorte der Standard-Rechenzentren von Microsoft Azure: Kunden aus Großbritannien: Rechenzentrum in Großbritannien Kunden aus Kanada: Rechenzentrum in Kanada Kunden aus Deutschland: Rechenzentrum in Deutschland Kunden aus Europa außerhalb Deutschlands: Rechenzentrum in den Niederlanden und Irland	Alle Kunden. Hier sind Standardstandorte angegeben, jedoch kann der Kunde vor der Ersteinrichtung des Tenants in der Onboarding-Phase Änderungen festlegen. Wenn der Kunde während der Vertragslaufzeit die Standorte der Tenants ändern möchte, sollte er sich an den Support wenden, um Unterstützung zu erhalten.
	Standard-Rechenzentrumsstandorte von Amazon Web Services (AWS):	Alle Kunden. Hier sind Standardstandorte angegeben,

Gegenstand der Verarbeitung	Details	Gilt für:
	Kunden im Vereinigten Königreich: Rechenzentrum im Vereinigten Königreich Kanadische Kunden: Rechenzentrum in Kanada Deutsche Kunden: Rechenzentrum in Deutschland Europäische Kunden außerhalb Deutschlands: Rechenzentrum in Irland	jedoch kann der Kunde vor der Ersteinrichtung des Tenants in der Onboarding-Phase Änderungen festlegen. Wenn der Kunde während der Vertragslaufzeit die Standorte der Tenants ändern möchte, sollte er sich an den Support wenden, um Unterstützung zu erhalten.
	Der Verarbeitungsort bei Nutzung von KI-Funktionalitäten ist in Anhang C aufgeführt.	Gilt für Kunden, die Phish Co-Pilot, Content to Course und Virtual Presenter abonniert haben.
Anforderungen an die Aufbewahrung	Spezifische Löschfristen sind im Dokument *„AI at MetaCompliance“* beschrieben, soweit sie für die vom Kunden angeforderten Leistungen relevant sind.	Kunden, die Dienste angefordert haben, die KI enthalten oder verwenden
	Wenn ein Kundenabonnement abgelaufen ist oder gekündigt wird, werden alle damit verbundenen personenbezogenen Daten des Kunden, die nicht bereits zuvor gelöscht wurden, für einen Zeitraum von 90 Tagen 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

1. **Unterauftragsverarbeiter, die für die Erbringung aller Leistungen erforderlich sind:**

Unterauftragsverarbeiter	Zweck	Standort	Unterauftragsverarbeiter
Microsoft Azure (unter Vertrag mit Microsoft Operations Ireland Ltd)	Hosting der Dienste in der Cloud	Standorte der Standard-Rechenzentren von Microsoft Azure: Kunden aus Großbritannien: Rechenzentrum in Großbritannien Kunden aus Kanada: Rechenzentrum in Kanada Kunden aus Deutschland: Rechenzentrum in Deutschland Kunden aus Europa außerhalb Deutschlands: Rechenzentrum in den Niederlanden und Irland	Weitere Unterauftragsverarbeiter hier
Amazon Web Services (unter Vertrag mit „AWS Europe")	Transaktions-E-Mail-Anbieter	Standorte der Rechenzentren von Amazon Web Services: Kunden aus dem Vereinigten Königreich: Rechenzentrum im Vereinigten Königreich Kunden aus Kanada: Rechenzentrum in Kanada Kunden aus Deutschland: Rechenzentrum in Deutschland Kunden aus Europa außerhalb Deutschlands: Rechenzentrum in Irland	Weitere Unterauftragsverarbeiter hier
Unternehmen der MetaCompliance Group (MetaCompliance Limited, MetaCompliance GmbH, Moch A/S, Metacompliance Ireland Ltd, MetaCompliance Ireland Ltd Sucursal Portugal)	Kundenkonten und Support-Services	Vereinigtes Königreich Deutschland Dänemark Irland Portugal (sofern zutreffend und entsprechend dem Sitz der jeweiligen juristischen Person)	

2. Zusätzliche Verarbeitung und Unterauftragsverarbeiter für die Nutzung von Content to Course

A) Open AI

MetaCompliance Rechenzentrum / Region	Startseite / Azure Rechenzentrum Standort	Bereitstellung	Verarbeitete personenbezogene Daten	Aufbewahrung
IRE	Westeuropa (NL)	Datenzone (EU)	Mit Ausnahme der von Kunden eingegebenen personenbezogenen Daten (z. B. als Antwort auf eine Aufforderung oder personenbezogene Daten, die in den zur Erstellung des Kurses bereitgestellten Inhalten enthalten sind) werden keine personenbezogenen Daten von Kunden von diesem Unterauftragsverarbeiter verarbeitet.	Es werden keine Eingabeaufforderungen oder Generierungen im Modell gespeichert. Darüber hinaus werden Eingabeaufforderungen und Generierungen nicht zum Trainieren, Nachschulen oder Verbessern der Basismodelle verwendet.
DACH	Deutschland West-Zentral	Datenzone (EU)	Wie oben.	Wie oben.
NL	Westeuropa (NL)	Datenzone (EU)	Wie oben.	Wie oben.
CAN	Kanada Ost	Standard (Kanada Ost)	Wie oben.	Wie oben.
UK	Großbritannien Süd	Standard (Großbritannien Süd)	Wie oben.	Wie oben.
USA	Nord-Zentral-USA	Standard (Nord-Zentral-USA)	Wie oben.	Wie oben.

B) Microsoft Document Intelligence und Azure Translator Services

MetaCompliance Rechenzentrum / Region	**Startseite / Azure Rechenzentrum Standort**	**Verarbeitung**	**Verarbeitete personenbezogene Daten**	**Lagerung (24 Stunden)**
IRE	Nordeuropa (Irland)	Nordeuropa (Irland)	Mit Ausnahme der personenbezogenen Daten, die in den zur Erstellung des Kurses bereitgestellten Inhalten enthalten sind, werden keine personenbezogenen Daten von Kunden durch diesen Unterauftragsverarbeiter verarbeitet.	Nordeuropa (Irland)
DACH	Deutschland West-Zentral	Deutschland West-Zentral	Wie oben.	Deutschland West-Zentral

NL	Westeuropa (NL)	Westeuropa (NL)	Wie oben.	Westeuropa (NL)
CAN	Kanada Zentral	Kanada Zentral	Wie oben.	Kanada Zentral
UK	Großbritannien Süd	Großbritannien Süd	Wie oben.	Großbritannien Süd
US	Nord-Zentral-USA	Nord-Zentral-USA	Wie oben.	Nord-Zentral-USA

3. Zusätzliche Verarbeitung und Unterauftragsverarbeiter für die Nutzung von Phish Co-Pilot

Unterauftragsverarbeiter	**Verarbeitete personenbezogene Daten**	**Region**	**Speicherung / Aufbewahrung**
Dienst: ChatGPT	Abgesehen von personenbezogenen Daten, die von Kunden eingegeben werden (z. B. im Rahmen eines Prompts oder in bereitgestellten Inhalten zur Kurserstellung), werden durch diesen Unterauftragsverarbeiter keine personenbezogenen Daten von Kunden verarbeitet.	Bereitstellung: Westeuropa Verarbeitung: Globaler Standard (beliebige Region)	Keine Eingabeaufforderungen oder Generierungen werden im Modell gespeichert. Darüber hinaus werden Eingabeaufforderungen und Generierungen nicht zur Schulung, Nachschulung oder Verbesserung der Basismodelle verwendet.
Dienst: Text Embedding	Wie oben.	Wie oben.	Wie oben.

4. Zusätzliche Verarbeitung und Unterauftragsverarbeiter für die Nutzung von Virtual Presenter

Unterauftragsverarbeiter	**Verarbeitete personenbezogene Daten**	**Region**	**Speicherung / Aufbewahrung**
Colossyan Inc.	Freitext, der ggf. personenbezogene Daten enthält und vom Kunden über Skripte oder andere Inhalte bereitgestellt wird. Der Kunde bestätigt, dass keine sensiblen Daten an den Auftragsverarbeiter übermittelt werden.	Verarbeitung in den Vereinigten Staaten, im Vereinigten Königreich und in Ungarn (es handelt sich um Standorte von Colossyan und verbundenen Unternehmen). Siehe Unterauftragsverarbeiter von Colossyan unten.	24 Stunden. Endgültige Löschung innerhalb von 48 Stunden.

NUTZUNG VON KI-FUNKTIONALITÄT

Bei der Nutzung der oben beschriebenen KI-Funktionalität sind alle KI-Umgebungen auf MetaCompliance-Ebene geschlossen. Kundenprompts (Eingaben) und -antworten (Ausgaben), Einbettungen (Embeddings) sowie Trainingsdaten des Kunden:

- sind NICHT für andere Kunden verfügbar;
- sind NICHT für Azure OpenAI verfügbar;
- werden NICHT zur Verbesserung der Azure-OpenAI-Modelle verwendet;
- werden NICHT zur Schulung, Nachschulung oder Verbesserung der zugrundeliegenden Modelle des Azure OpenAI Service genutzt;
- werden NICHT zur Verbesserung von Microsoft-Produkten oder Produkten Dritter verwendet – außer mit ausdrücklicher Zustimmung oder auf Anweisung des Kunden.

Archivierte Versionen der AVV stehen zur Verfügung hier