VEREINBARUNG ÜBER DIE AUFTRAGSVERARBEITUNG

Version April 2026

Diese Vereinbarung über die Auftragsverarbeitung („AVV“) wird geschlossen zwischen der im jeweiligen Bestellformular genannten Revalize-Gesellschaft („Anbieter“) und der diesen Bedinfgungen zustimmenden Rechtseinheit („Kunde“) (gemeinsam die „Parteien“ und jeweils eine „Partei“) und gilt für die Verarbeitung personenbezogener Daten im Zusammenhang mit der zwischen den Parteien bestehenden Vereinbarung über die Bereitstellung von Software und/oder Dienstleistungen durch den Anbieter an den Kunden („Vertrag“). Diese AVV ist Bestandteil des Vertrags und regelt die jeweiligen Rechte und Pflichten der Parteien in Bezug auf eine solche Verarbeitung. In Anbetracht der hierin enthaltenen Zusicherungen und Verpflichtungen sowie einer weiteren angemessenen Gegenleistung, deren Erhalt und Angemessenheit hiermit bestätigt wird, vereinbaren die Parteien Folgendes:

1. VERARBEITUNG PERSONENBEZOGENER DATEN

1.1. Der Kunde weist den Anbieter im eigenen Namen sowie im Namen jedes mit dem Kunden verbundenen Unternehmens (Customer Affiliate) an, während der Laufzeit des Vertrags personenbezogene Daten zu verarbeiten und zwar ausschließlich zum Zweck der Erbringung der Leistungen gemäß dem Vertrag und dieser AVV. Die Datenverarbeitungsanweisungen (Data Processing Instructions) legen den Gegenstand sowie weitere Einzelheiten der im Rahmen der Leistungen vorgesehenen Verarbeitung personenbezogener Daten fest, einschließlich betroffener Personen, Kategorien personenbezogener Daten, besonderer Kategorien personenbezogener Daten, Unterauftragsverarbeiter und Beschreibung der Verarbeitung. Zusätzliche oder spezifischere Beschreibungen von Verarbeitungstätigkeiten können im Vertrag enthalten sein.

1.2. Der Anbieter darf personenbezogene Daten – abhängig von den Leistungen – zu folgenden Zwecken verarbeiten: Hosting und Speicherung; Backup sowie Disaster-Recovery; Service-Change-Management; Incident- und Issue-Behebung; Einspielen neuer Produkt- oder Systemversionen, Patches, Updates und Upgrades; Überwachung und Tests der Systemnutzung und -leistung; IT-Sicherheit (einschließlich Bedrohungserkennung, Incident-Management und Zugriffskontrolle); Wartung und Betrieb technischer Support-Systeme und der IT-Infrastruktur; sowie Migration, Implementierung, Konfiguration und Performance-Tests der Leistungen.

1.3. Im Rahmen der Erbringung der Leistungen und abhängig von den jeweils beauftragten Leistungen darf der Anbieter personenbezogene Daten verarbeiten, die sich auf die natürlichen Personen des Kunden beziehen, einschließlich Endnutzer, Beschäftigte, Bewerber, Auftragnehmer, Mitarbeitende, Partner, Lieferanten, Kunden und Klienten des Kunden.

1.4. Die Parteien erkennen an, dass die Übermittlung oder Offenlegung personenbezogener Daten durch den Kunden an den Anbieter keinen „Verkauf“ personenbezogener Daten im Sinne anwendbarer Datenschutzgesetze (einschließlich des CCPA) darstellt und dass der Anbieter dem Kunden hierfür keine geldwerte oder sonstige Gegenleistung gewährt.

1.5. Sofern im Vertrag nicht ausdrücklich etwas anderes bestimmt ist, darf der Kunde dem Anbieter keine sensiblen Daten oder sonstigen Daten zur Verfügung stellen, die dem Anbieter besondere Datensicherheits-, Datenschutz- oder regulatorische Pflichten auferlegen, die über die in dieser AVV vorgesehenen Pflichten hinausgehen oder von diesen abweichen.

1.6. Der Anbieter wird personenbezogene Daten nicht (i) für andere Zwecke (einschließlich eigener kommerzieller Zwecke) als auf dokumentierte Weisungen des Kunden (wie in dieser AVV und im Vertrag festgelegt) verarbeiten, aufbewahren, nutzen, offenlegen oder anderweitig verarbeiten, es sei denn, die Verarbeitung ist nach anwendbarem Recht und nach Maßgabe der Standardvertragsklauseln (soweit anwendbar) erforderlich; oder (ii) personenbezogene Daten, die er vom Kunden erhält oder im Zusammenhang mit der Erbringung der Leistungen für den Kunden erlangt, verkaufen.

1.7. Die zusätzlichen Bestimmungen in Anlage VI finden Anwendung, soweit der CCPA auf den Kunden anwendbar ist.

2. PERSONAL DES ANBIETERS

Der Anbieter stellt sicher, dass sämtliches Personal, das zur Verarbeitung personenbezogener Daten befugt ist, (i) zur Vertraulichkeit verpflichtet ist oder einer geeigneten gesetzlichen Vertraulichkeitspflicht in Bezug auf solche personenbezogenen Daten unterliegt und (ii) eine angemessene Schulung zum Schutz personenbezogener Daten erhalten hat.

3. SICHERHEIT

3.1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Anbieter in Bezug auf die personenbezogenen Daten geeignete technische und organisatorische Maßnahmen, um im Rahmen der Erbringung der Leistungen ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Für die Zwecke dieser AVV sind die technischen und organisatorischen Maßnahmen des Anbieters in der Anlage „Information Security Schedule" beschrieben.

3.2. Bei der Beurteilung des angemessenen Schutzniveaus berücksichtigt der Anbieter insbesondere die durch die Verarbeitung personenbezogener Daten entstehenden Risiken.

4. UNTERAUFTRAGSVERARBEITUNG

4.1. Der Anbieter darf ausschließlich Unterauftragsverarbeiter einsetzen, die es dem Anbieter ermöglichen, die anwendbaren Datenschutzgesetze einzuhalten. Der Kunde ermächtigt den Anbieter hiermit, Unterauftragsverarbeiter gemäß diesem Abschnitt 4 zu beauftragen, vorbehaltlich etwaiger in dieser AVV ausdrücklich festgelegter Beschränkungen oder Bedingungen. Entsprechend Anlage III stimmt der Kunde den Unterauftragsverarbeitern in der Liste der Unterauftragsverarbeiter (abrufbar Revalize-Unterauftragsverarbeiter-Liste) zum Wirksamkeitsdatum dieser AVV sowie etwaigen neuen Unterauftragsverarbeitern nach Maßgabe von Abschnitt 4.2 zu. Soweit nach anwendbaren Datenschutzgesetzen erforderlich, schließt der Anbieter mit jedem Unterauftragsverarbeiter einen geeigneten schriftlichen Vertrag. Der Anbieter bleibt dem Kunden gegenüber für die Leistungserbringung seiner Unterauftragsverarbeiter nach dieser AVV verantwortlich.

4.2. Ungeachtet etwaiger Mitteilungspflichten in dieser AVV wird der Anbieter den Kunden, bevor er einen neuen Unterauftragsverarbeiter einsetzt, über eine solche Beauftragung informieren, einschließlich Angaben zu der vom vorgeschlagenen Unterauftragsverarbeiter durchzuführenden Verarbeitung. Jeder neue Unterauftragsverarbeiter wird zur Liste der Unterauftragsverarbeiter (abrufbar unter Revalize-Unterauftragsverarbeiter-Liste) hinzugefügt, und der Kunde wird per E-Mail oder auf anderem angemessenem elektronischem Wege benachrichtigt. Zusätzlich zu sonstigen Benachrichtigungen kann der Anbieter eine solche Mitteilung auch durch Aktualisierung der Liste der Unterauftragsverarbeiter auf der Website bereitstellen. Der Kunde kann innerhalb von 15 Tagen nach der Benachrichtigung über die aktualisierte Liste der Unterauftragsverarbeiter dem Anbieter etwaige Einwände (aus sachlichen Gründen im Zusammenhang mit Datenschutzgesetzen) gegen den vorgeschlagenen Unterauftragsverarbeiter oder gegen Datenverarbeitungsanweisungen („Einwand") mitteilen. Anbieter und Kunde werden dann in gutem Glauben verhandeln, um weitere Maßnahmen – einschließlich vertraglicher oder operativer Anpassungen im Zusammenhang mit der Beauftragung des vorgeschlagenen Unterauftragsverarbeiters oder dem Betrieb der Leistungen – zu vereinbaren, um den Einwand des Kunden auszuräumen. Können sich die Parteien innerhalb von fünfundvierzig (45) Tagen nach Eingang des Einwands beim Anbieter (oder innerhalb eines vom Kunden schriftlich genehmigten längeren Zeitraums) nicht auf solche weiteren Maßnahmen einigen, kann der Kunde durch schriftliche Mitteilung an den Anbieter mit sofortiger Wirkung denjenigen Teil der Leistungen kündigen, der den Einsatz des vorgeschlagenen Unterauftragsverarbeiters erfordert, oder einen anderen Teil der Leistungen kündigen, der hierdurch beendet wird.

5. RECHTE BETROFFENER PERSONEN

Der Anbieter wird:

5.1. Sobald er Kenntnis davon erlangt, den Kunden unverzüglich benachrichtigen, wenn der Anbieter einen Antrag einer betroffenen Person in Bezug auf ein durchsetzbares Recht der betroffenen Person nach anwendbaren Datenschutzgesetzen hinsichtlich personenbezogener Daten erhält;

5.2. Auf einen solchen Antrag nicht reagieren, außer auf dokumentierte Weisung des Kunden oder soweit dies von einer Aufsichtsbehörde oder nach anwendbarem Recht verlangt wird; und

5.3. Auf Verlangen des Kunden, soweit nach Datenschutzgesetzen erforderlich und im Zusammenhang mit den Leistungen, den Kunden in angemessenem Umfang bei der Bearbeitung eines durchsetzbaren Antrags auf Ausübung von Rechten betroffener Personen unterstützen, soweit der Kunde den Antrag ohne Unterstützung des Anbieters nicht erfüllen kann. Der Anbieter kann dieser Verpflichtung nachkommen, indem er (auf Kosten des Kunden) Funktionalitäten bereitstellt, die es dem Kunden ermöglichen, einen solchen Antrag ohne zusätzliche Verarbeitung durch den Anbieter zu erfüllen. Soweit eine solche Funktionalität nicht verfügbar ist, muss der Kunde, damit der Anbieter eine solche angemessene Unterstützung leisten kann, dem Anbieter den Antrag schriftlich übermitteln und

ausreichende Informationen bereitstellen, damit der Anbieter (auf Kosten des Kunden) den/die betreffenden Datensatz/-sätze lokalisieren und anschließend berichtigen, exportieren oder löschen kann.

6. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN.

6.1. Der Anbieter benachrichtigt den Kunden unverzüglich nach Bestätigung einer Verletzung des Schutzes personenbezogener Daten (Personal Data Breach) durch den Anbieter oder einen Unterauftragsverarbeiter und stellt dem Kunden ausreichende Informationen zur Verfügung, damit der Kunde etwaige Pflichten nach anwendbaren Datenschutzgesetzen zur Meldung oder Benachrichtigung betroffener Personen erfüllen kann. Vorbehaltlich Abschnitt 6.3 unten muss diese Benachrichtigung mindestens Folgendes enthalten:

a) Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, der Kategorien und Anzahl der betroffenen Personen sowie der Kategorien und Anzahl der betroffenen Datensätze mit personenbezogenen Daten;
b) Mitteilung des Namens und der Kontaktdaten des Datenschutzbeauftragten des Anbieters oder einer sonstigen zuständigen Kontaktstelle, von der weitere Informationen eingeholt werden können;
c) Beschreibung der voraussichtlichen Folgen der Verletzung des Schutzes personenbezogener Daten, soweit der Anbieter dies unter Berücksichtigung der Art der Leistungen und der Verletzung des Schutzes personenbezogener Daten feststellen kann; und
d) Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten.

6.2. Der Anbieter arbeitet mit dem Kunden zusammen und ergreift die wirtschaftlich angemessenen Maßnahmen, die erforderlich sind, um bei der Untersuchung, Eindämmung und Behebung jeder solchen Verletzung des Schutzes personenbezogener Daten zu unterstützen.

6.3. Soweit und solange es nicht möglich ist, die in Abschnitt 6.1 genannten Informationen gleichzeitig bereitzustellen, oder der Anbieter durch Gesetz oder Strafverfolgungsbehörden an der Bereitstellung dieser Informationen gehindert ist, können die Informationen stufenweise und ohne unangemessene weitere Verzögerung übermittelt werden.

7. DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE KONSULTATION

Soweit erforderlich leistet der Anbieter dem Kunden angemessene Unterstützung bei etwaigen Datenschutz-Folgenabschätzungen sowie bei vorherigen Konsultationen mit Aufsichtsbehörden oder sonstigen zuständigen Datenschutzbehörden, die der Kunde nach billigem Ermessen als nach Datenschutzgesetzen erforderlich ansieht, jeweils ausschließlich in Bezug auf die Verarbeitung personenbezogener Daten durch den Anbieter und unter Berücksichtigung der Art der Verarbeitung und der dem Anbieter verfügbaren Informationen. Soweit eine solche Folgenabschätzung und/oder vorherige Konsultation eine Unterstützung erfordert, die über die Bereitstellung der einschlägigen Verarbeitungsverzeichnisse des Anbieters und der Dokumentation hinausgeht, behält sich der Anbieter das Recht vor, dem Kunden diesen Aufwand zu den jeweils geltenden Tagessätzen des Anbieters in Rechnung zu stellen.

8. LÖSCHUNG ODER RÜCKGABE PERSONENBEZOGENER DATEN.

8.1. Innerhalb von dreißig (30) Tagen nach Beendigung oder Ablauf des Vertrags („Rückgabezeitraum“) wird der Anbieter – vorbehaltlich Abschnitt 8.2 unten – auf Verlangen des Kunden die verfügbaren personenbezogenen Daten entweder löschen oder zurückgeben. Nach Ablauf des Rückgabezeitraums kann der Anbieter, sofern der Kunde keine der vorgenannten Optionen gewählt hat, alle personenbezogenen Daten ohne Mitteilung und ohne Haftung gegenüber dem Kunden löschen und vernichten. Verlangt der Kunde die Rückgabe verfügbarer personenbezogener Daten, kann der Anbieter diesem Verlangen dadurch nachkommen, dass er Funktionalitäten bereitstellt, die es dem Kunden ermöglichen, die personenbezogenen Daten ohne zusätzliche Verarbeitung durch den Anbieter abzurufen. Lehnt der Kunde die Nutzung dieser Funktionalität ab, kann der Kunde innerhalb des Rückgabezeitraums verlangen, dass der Anbieter die verfügbaren personenbezogenen Daten im Rahmen eines Auftrags für die entsprechenden Professional Services zurückgibt. Wird der Vertrag wegen eines Vertragsverstoßes des Kunden beendet, ist der Anbieter berechtigt, vom Kunden eine Vorauszahlung für solche Professional Services zu verlangen. Der Anbieter bestätigt dem Kunden innerhalb von dreißig (30) Tagen nach dem Verlangen des Kunden schriftlich, dass er diesen Abschnitt 8 vollständig erfüllt hat.

8.2. Der Anbieter darf personenbezogene Daten in dem Umfang aufbewahren, in dem dies nach Datenschutzgesetzen oder aufgrund sonstiger gesetzlicher Anforderungen, denen der Anbieter unterliegt, erforderlich ist, und nur in dem Umfang und für den Zeitraum, der nach Datenschutzgesetzen oder einer solchen sonstigen gesetzlichen Anforderung erforderlich ist, stets unter der Voraussetzung, dass (i) während eines solchen Aufbewahrungszeitraums die Bestimmungen dieser AVV weiterhin gelten, (ii) der Anbieter die Vertraulichkeit sämtlicher solcher

personenbezogenen Daten gewährleistet und (iii) der Anbieter sicherstellt, dass solche personenbezogenen Daten ausschließlich soweit verarbeitet werden, wie dies für die in den Datenschutzgesetzen, die deren Speicherung verlangen, oder in sonstigen gesetzlichen Anforderungen, denen der Anbieter unterliegt, genannten Zwecke erforderlich ist und zu keinem anderen Zweck.

9. RECHTE AUF ÜBERPRÜFUNG, AUDIT UND INSPEKTION.

9.1. Auf angemessenes Verlangen des Kunden stellt der Anbieter alle relevanten und erforderlichen Informationen zur Verfügung, um seine Einhaltung anwendbarer Datenschutzgesetze nachzuweisen, einschließlich der relevanten und erforderlichen Informationen über die technischen und organisatorischen Sicherheitsmaßnahmen des Anbieters zum Schutz der personenbezogenen Daten im Zusammenhang mit den erbrachten Leistungen. Solche Informationen können in zusammengefasster Form bereitgestellt werden, um das Risiko zu minimieren, dass diese Maßnahmen umgangen werden.

9.2. Der Anbieter stellt sicher, dass mindestens jährlich ein Sicherheitsaudit seiner technischen und organisatorischen Sicherheitsmaßnahmen in Übereinstimmung mit anwendbaren Datenschutzgesetzen durchgeführt wird. Die Ergebnisse eines solchen Sicherheitsaudits werden in einem zusammenfassenden Bericht dokumentiert. Der Anbieter stellt dem Kunden auf Verlangen unverzüglich Folgendes zur Verfügung: (i) eine vertrauliche Zusammenfassung dieses Berichts; und (ii) Nachweise über eine angemessene Behebung etwaiger kritischer Feststellungen innerhalb von vier (4) Wochen ab Ausstellungsdatum des Auditberichts.

9.3. Wenn der Kunde nach Abschluss der in den Abschnitten 9.1 und 9.2 genannten Schritte nach billigem Ermessen davon ausgeht, dass der Anbieter die anwendbaren Datenschutzgesetze nicht einhält, kann der Kunde verlangen, dass der Anbieter – entweder per Webinar oder im Rahmen einer Vor-Ort-Überprüfung – Auszüge sämtlicher relevanter Informationen zur Verfügung stellt, die erforderlich sind, um die Einhaltung der anwendbaren Datenschutzgesetze weiter nachzuweisen. Der Kunde, der eine solche Überprüfung durchführt, wird dem Anbieter eine angemessene Vorankündigung geben, indem er das Data Privacy Team des Anbieters unter dpo@revalizesoftware.com kontaktiert; jede Überprüfung erfolgt nach Maßgabe dieses Abschnitts 9.3.

9.4. Wenn der Kunde nach billigem Ermessen der Auffassung ist, dass seine Feststellungen nach den in Abschnitt 9.3 genannten Schritten es dem Kunden nicht ermöglichen, seine nach anwendbaren Datenschutzgesetzen vorgeschriebenen Pflichten in Bezug auf die Beauftragung des Anbieters wesentlich zu erfüllen, kann der Kunde dem Anbieter mindestens dreißig (30) Tage vorher schriftlich ankündigen, dass er ein Audit durchführen wird, das Inspektionen beim Anbieter umfassen kann, die durch den Kunden oder durch einen vom Kunden beauftragten Prüfer (der kein Wettbewerber des Anbieters sein darf) durchgeführt werden. Ein solches Audit und/oder eine solche Inspektion: (i) unterliegt zwischen dem Kunden (bzw. dem vom Kunden beauftragten Prüfer) und dem Anbieter vereinbarten Vertraulichkeitspflichten, (ii) erfolgt ausschließlich in dem durch anwendbare Datenschutzgesetze vorgeschriebenen Umfang und darf insoweit nicht weiter eingeschränkt werden, (iii) darf nicht verlangen, dass der Anbieter die Vertraulichkeit sicherheitsrelevanter Aspekte seiner Systeme und/oder Datenverarbeitungseinrichtungen (einschließlich derjenigen seiner Unterauftragsverarbeiter) beeinträchtigt, und (iv) darf nicht durchgeführt werden, wenn dies den Anbieter dazu veranlassen würde, gegen seine Vertraulichkeitspflichten gegenüber anderen Kunden, Lieferanten und/oder Partnern des Anbieters zu verstoßen oder anderweitig gegen für den Anbieter geltende Gesetze zu verstoßen. Der Kunde (oder der vom Kunden beauftragte Prüfer) hat bei der Durchführung eines solchen Audits oder einer solchen Inspektion zu vermeiden, dass Räumlichkeiten, Ausrüstung, Personal und Geschäftsbetrieb des Anbieters beschädigt, verletzt oder beeinträchtigt werden. Soweit ein nach diesem Abschnitt 9.4 durchgeführtes Audit einen (1) Geschäftstag überschreitet, behält sich der Anbieter das Recht vor, dem Kunden jeden zusätzlichen Tag zu den jeweils geltenden Tagessätzen in Rechnung zu stellen.

9.5. Kommt der Kunde nach einem Audit oder einer Inspektion gemäß Abschnitt 9.4 nach billigem Ermessen zu dem Ergebnis, dass der Anbieter die anwendbaren Datenschutzgesetze nicht einhält, wird der Kunde dem Anbieter die entsprechenden Einzelheiten mitteilen. Nach Erhalt wird der Anbieter seine Stellungnahme abgeben und – soweit erforderlich – einen Entwurf eines Maßnahmenplans zur Behebung („Maßnahmenplan“) zur gegenseitigen Vereinbarung durch die Parteien vorlegen (eine solche Vereinbarung darf nicht unbillig verweigert oder verzögert werden; der gemeinsam vereinbarte Plan ist der „Maßnahmenplan“). Können sich die Parteien nicht über den Maßnahmenplan einigen oder – im Falle einer Einigung – setzt der Anbieter den Maßnahmenplan nicht wesentlich zu den vereinbarten Terminen um, und wird dies in beiden Fällen nicht innerhalb von fünfundvierzig (45) Tagen nach Mitteilung des Kunden oder innerhalb eines anderweitig zwischen den Parteien vereinbarten Zeitraums behoben, kann der Kunde die Leistungen ganz oder teilweise kündigen, soweit sie sich auf die nicht konforme Verarbeitung beziehen; die übrigen Leistungen bleiben von einer solchen Kündigung unberührt und werden fortgeführt.

9.6. Die Rechte des Kunden nach diesem Abschnitt 9 dürfen nur einmal pro Kalenderjahr ausgeübt werden, es sei denn, der Kunde geht nach billigem Ermessen davon aus, dass der Anbieter seine Pflichten aus dieser AVV oder aus anwendbaren Datenschutzgesetzen wesentlich verletzt.

10. EINGESCHRÄNKTE ÜBERMITTLUNGEN.

10.1. Der Kunde (als „Datenexporteur“) und der Anbieter – soweit jeweils anwendbar – (als „Datenimporteur“) vereinbaren hiermit, dass die jeweils anwendbaren Standardvertragsklauseln (Standard Contractual Clauses) für jede eingeschränkte Übermittlung (Restricted Transfer) vom Kunden oder einem mit dem Kunden verbundenen Unternehmen (Customer Affiliate) an den Anbieter gelten, soweit dies nach Datenschutzgesetzen erforderlich ist. Die Parteien vereinbaren, dass die Bestimmungen der Standardvertragsklauseln auf die eingeschränkte Übermittlung Anwendung finden. Soweit personenbezogene Daten der EU-DSGVO unterliegen, sind die anwendbaren Standardvertragsklauseln die EU SCCs; soweit personenbezogene Daten der UK GDPR unterliegen, ist das anwendbare Transferinstrument das UK Addendum, jeweils ausgefüllt wie hierin beschrieben und wie in den Anlagen festgelegt. Soweit personenbezogene Daten dem Schweizer Bundesgesetz über den Datenschutz unterliegen, finden die Bestimmungen des Swiss Addendum Anwendung.

10.2. Für die Zwecke der Anlage I oder eines sonstigen einschlägigen Teils der jeweils anwendbaren Standardvertragsklauseln legen die Datenverarbeitungsanweisungen (Data Processing Instructions) die betroffenen Personen, Kategorien personenbezogener Daten, besonderen Kategorien personenbezogener Daten, Unterauftragsverarbeiter und die Beschreibung der Verarbeitung (Verarbeitungsvorgänge) fest. Soweit die EU SCCs für Übermittlungen vom Kunden oder einem Customer Affiliate an den Anbieter gelten, werden sie wie in Anlage I festgelegt ausgefüllt. Optionale Klauseln in den jeweils anwendbaren Standardvertragsklauseln finden keine Anwendung, sofern nicht in Anlage I etwas anderes vorgesehen ist.

10.3. Für die Zwecke der Anlage II oder eines sonstigen einschlägigen Teils der jeweils anwendbaren Standardvertragsklauseln enthält die Anlage „Information Security Schedule“ die Beschreibung der vom Anbieter (als Datenimporteur) implementierten technischen und organisatorischen Sicherheitsmaßnahmen.

10.4. Der Anbieter wird keine eingeschränkte Übermittlung personenbezogener Daten, die er nach dieser AVV erhalten hat, vornehmen, sofern er hierfür nicht nach anwendbaren Datenschutzgesetzen eine rechtmäßige Grundlage hat. Eine solche rechtmäßige Grundlage kann (i) ein Angemessenheitsbeschluss (Adequacy Decision), (ii) Standardvertragsklauseln, (iii) die Bedingungen anderer anerkannter Formen von Datenübermittlungsvereinbarungen oder -prozessen oder (iv) eine nach Datenschutzgesetzen zulässige Ausnahme (derogation) sein.

11. HAFTUNG

Soweit nach anwendbarem Recht zulässig, finden sämtliche Haftungsbeschränkungen und -ausschlüsse des Vertrags, einschließlich insbesondere etwaiger Haftungsregelungen für Datenschutzansprüche zwischen den Parteien, auch auf diese AVV Anwendung. Diese vertragliche Risikozuweisung und Haftungsbegrenzung gilt ausschließlich für das Innenverhältnis zwischen den Parteien und beschränkt oder schließt keine zwingende Haftung einer Partei gegenüber betroffenen Personen oder Dritten nach der DSGVO oder sonstigen anwendbaren Datenschutzgesetzen aus, einschließlich des Rechts betroffener Personen auf vollständigen und wirksamen Schadensersatz nach Art. 82 DSGVO.

12. SONSTIGE DATENSCHUTZGESETZE.

12.1. Soweit sich die Verarbeitung auf personenbezogene Daten bezieht, die aus einer Jurisdiktion stammen oder in einer Jurisdiktion verarbeitet werden, die zwingende Anforderungen enthält oder künftig solche Anforderungen einführt, die über die in dieser AVV geregelten hinausgehen, können die Parteien zusätzliche Maßnahmen vereinbaren, die erforderlich sind, um die Einhaltung der anwendbaren Datenschutzgesetze sicherzustellen; solche zusätzlichen Maßnahmen werden als Anlage zu dieser AVV oder in einer Bestellung zum Vertrag dokumentiert.

12.2. Der Kunde stimmt ferner zu, dass der Anbieter, soweit der Anbieter nach anwendbaren Datenschutzgesetzen verpflichtet ist, einen geeigneten Übermittlungsmechanismus oder zusätzliche Garantien zur Übermittlung personenbezogener Daten zu vereinbaren, eine entsprechende Vereinbarung zur Durchführung einer solchen Übermittlung im eigenen Namen und – soweit erforderlich – im Namen des Kunden schließen darf, benannt oder unbenannt.

12.3. Da der Anbieter keine Kontrolle über Art, Beschaffenheit, Eigenschaften, Inhalt und/oder Herkunft der hierunter verarbeiteten personenbezogenen Daten hat, gilt ungeachtet anderslautender Bestimmungen, dass der Anbieter diese AVV oder den Vertrag nicht verletzt und dem Kunden nicht haftet, soweit personenbezogene Daten, die Jurisdiktionsanforderungen unterliegen, welche Sicherheits-, Verarbeitungs- oder sonstige Maßnahmen

vorschreiben, die nicht in dieser AVV vorgesehen sind oder deren Bestimmungen widersprechen, vom Kunden bereitgestellt werden, ohne dass diese AVV entsprechend geändert oder eine Bestellung hierzu abgeschlossen wurde.

12.4. Sollte aufgrund einer Änderung der Datenschutzgesetze eine Anpassung dieser AVV erforderlich werden, einschließlich einer Anpassung der Standardvertragsklauseln, kann jede Partei der anderen Partei diese Gesetzesänderung schriftlich mitteilen. Die Parteien werden in gutem Glauben über alle erforderlichen Anpassungen dieser AVV, einschließlich der Standardvertragsklauseln, zur Berücksichtigung solcher Änderungen beraten und verhandeln.

13. ALLGEMEINE BESTIMMUNGEN.

Diese AVV unterliegt dem Recht des Landes, in dem der Kunde seinen Sitz hat, und ist entsprechend auszulegen. Die Parteien vereinbaren, dass das Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG) auf diese AVV und die Parteien in keiner Weise Anwendung findet.

- Hat der Kunde seinen Sitz in einem Land Europas, ist das auf diese AVV anwendbare Recht das Recht der Bundesrepublik Deutschland, und die Gerichte in Deutschland sind ausschließlich zuständig.
- Hat der Kunde seinen Sitz in den USA, ist das auf diese AVV anwendbare Recht das Recht des Bundesstaats Delaware, und die Gerichte in Delaware sind ausschließlich zuständig.
- Hat der Kunde seinen Sitz im Vereinigten Königreich, ist das auf diese AVV anwendbare Recht das Recht des Vereinigten Königreichs, und die Gerichte im Vereinigten Königreich sind ausschließlich zuständig.
- Hat der Kunde seinen Sitz in einem anderen Land außerhalb Europas oder des Vereinigten Königreichs, ist das auf diese AVV anwendbare Recht das Recht der Bundesrepublik Deutschland, und das Gericht in Karlsruhe ist ausschließlich zuständig.

14. RANGFOLGE

Keine Bestimmung dieser AVV reduziert die Pflichten des Anbieters oder eines verbundenen Unternehmens des Anbieters (Provider Affiliate) aus dem Vertrag in Bezug auf den Schutz personenbezogener Daten oder erlaubt dem Anbieter oder einem Provider Affiliate, personenbezogene Daten in einer Weise zu verarbeiten (oder eine Verarbeitung zu gestatten), die nach dem Vertrag untersagt ist. Im Falle von Widersprüchen zwischen den Bestimmungen dieser AVV und (i) der Anlage „Information Security Schedule“ oder (ii) sonstigen Vereinbarungen zwischen den Parteien, einschließlich des Vertrags sowie einschließlich (sofern nicht ausdrücklich schriftlich etwas anderes vereinbart und im Namen der Parteien unterzeichnet) nach dem Datum dieser AVV abgeschlossener oder vermeintlich abgeschlossener Vereinbarungen, gehen die Bestimmungen dieser AVV vor.

15. SALVATORISCHE KLAUSEL

Sollte eine Bestimmung dieser AVV unwirksam oder nicht durchsetzbar sein, bleibt der übrige Teil dieser AVV wirksam und in Kraft. Die unwirksame oder nicht durchsetzbare Bestimmung wird entweder (i) soweit erforderlich angepasst, um ihre Wirksamkeit und Durchsetzbarkeit sicherzustellen und dabei die Absichten der Parteien so weit wie möglich zu wahren, oder, falls dies nicht möglich ist, (ii) so ausgelegt, als wäre der unwirksame oder nicht durchsetzbare Teil nie enthalten gewesen.

16. BEGRIFFSBESTIMMUNGEN

In dieser AVV haben die folgenden Begriffe die nachstehend festgelegte Bedeutung; entsprechende Begriffe sind entsprechend auszulegen:

- Angemessenheitsbeschluss bezeichnet – für eine Jurisdiktion, deren Datenschutzgesetze Datenübermittlungsbeschränkungen vorsehen – eine Entscheidung, die die Aufsichtsbehörde oder eine sonstige Stelle in dieser Jurisdiktion als Gewähr dafür anerkennt, dass ein angemessenes Datenschutzniveau im Sinne der Datenschutzgesetze dieser Jurisdiktion besteht, sodass eine Übermittlung in dieses Land ohne zusätzliche Anforderungen zulässig ist.
- Aufsichtsbehörde bezeichnet eine Behörde oder eine staatliche oder staatsnahe Stelle, die in einer Jurisdiktion nach Datenschutzgesetzen errichtet ist und für Angelegenheiten des Datenschutzes zuständig ist.
- Auftragsverarbeiter bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (einschließlich „service provider“ im Sinne des CCPA); im Kontext dieser AVV ist damit der Anbieter gemeint.

- Betroffene Person bezeichnet die identifizierte oder identifizierbare Person, auf die sich personenbezogene Daten beziehen (einschließlich „consumer“ im Sinne des CCPA).
- CCPA bezeichnet den California Consumer Privacy Act of 2018, kodifiziert in Cal. Civ. Code § 1798.100 ff., in der durch den California Privacy Rights Act geänderten Fassung, einschließlich seiner Durchführungsverordnungen, jeweils in der ggf. künftig weiter geänderten Fassung.
- Datenschutzgesetze bezeichnet sämtliche Datenschutz- und Privatsphäre-Gesetze und -Verordnungen, die auf die jeweils betroffenen personenbezogenen Daten anwendbar sind. Ohne Einschränkung des Vorstehenden umfassen Datenschutzgesetze – soweit anwendbar – die EU-DSGVO, die UK-DSGVO, Datenschutzgesetze einzelner US-Bundesstaaten sowie sonstige vergleichbare ausländische, nationale oder regionale Datenschutz- oder Privatsphäre-Gesetze, jeweils in ihrer von Zeit zu Zeit geänderten, ersetzten oder aufgehobenen Fassung.
- Datenverarbeitungsanweisungen bezeichnet die in Anlage I(2) (Description of Transfer) festgelegten Verarbeitungsanweisungen.
- Eingeschränkte Übermittlung bezeichnet: **(i)** eine Übermittlung personenbezogener Daten vom Kunden oder einem Customer Affiliate an den Anbieter; oder **(ii)** eine Weiterübermittlung personenbezogener Daten vom Anbieter an einen Unterauftragsverarbeiter, jeweils sofern eine solche Übermittlung ohne eine genehmigte Übermittlungsgrundlage (z. B. (a) einen Angemessenheitsbeschluss, (b) Standardvertragsklauseln, (c) andere anerkannte Formen von Datenübermittlungsvereinbarungen oder -prozessen nach anwendbaren Datenschutzgesetzen oder (d) eine zulässige Ausnahme (derogation)) nach Datenschutzgesetzen untersagt wäre oder gegen die Bedingungen einer solchen genehmigten Übermittlungsgrundlage oder zulässigen Ausnahme verstoßen würde.
- EU-DSGVO bezeichnet sämtliche EU-Verordnungen, die (ganz oder teilweise) auf die Verarbeitung personenbezogener Daten anwendbar sind, wie z. B. die Verordnung (EU) 2016/679.
- EU-Standardvertragsklauseln bezeichnet die Vertragsklauseln im Anhang des Durchführungsbeschlusses (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, wie in Anlage I zu dieser AVV wiedergegeben.
- Informationssicherheitsanhang bezeichnet die in Anlage II genannten Informationssicherheits- sowie technischen und organisatorischen Maßnahmen, jeweils in der von Zeit zu Zeit aktualisierten Fassung.
- Leistungen bezeichnet die Leistungen und sonstigen Tätigkeiten, die vom Anbieter für den Kunden gemäß dem Vertrag zu erbringen oder durchzuführen sind bzw. in dessen Auftrag erbracht oder durchgeführt werden.
- Personenbezogene Daten bzw. Personenbezogene Informationen bezeichnet sämtliche Informationen über eine identifizierte oder identifizierbare natürliche Person im Sinne der anwendbaren Datenschutzgesetze.
- Schweizer Zusatz bezeichnet den Zusatz zu den EU-Standardvertragsklauseln gemäß Anlage III zu dieser AVV.
- Standardvertragsklauseln bezeichnet die nach Datenschutzgesetzen von einer Aufsichtsbehörde genehmigten Vertragsklauseln (jeweils in der von Zeit zu Zeit aktualisierten Fassung), die eine Übermittlung personenbezogener Daten zulassen, die andernfalls eine eingeschränkte Übermittlung wäre.
- UK-DSGVO bezeichnet die EU-DSGVO, soweit sie aufgrund von Section 3 des European Union (Withdrawal) Act 2018 Bestandteil des Rechts des Vereinigten Königreichs ist. Verweise auf Anlagen beziehen sich auf Anlagen der EU-Standardvertragsklauseln.
- UK-Zusatz bezeichnet den International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, herausgegeben durch den UK Information Commissioner gemäß Section 119A(1) des UK Data Protection Act 2018, jeweils in der von Zeit zu Zeit geänderten oder ersetzten Fassung.
- Unterauftragsverarbeiter bezeichnet jeden Dritten (einschließlich jedes Dritten sowie jedes Provider Affiliate), der vom Anbieter oder in dessen Auftrag bestellt wird, um eine Verarbeitung im Zusammenhang mit den Leistungen durchzuführen; die Kategorien sind in Anlage III aufgeführt und in der Liste der Unterauftragsverarbeiter unter Revalize Subprocessors List gelistet.
- Verantwortlicher bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, einschließlich „business“ im Sinne des CCPA; im Kontext dieser AVV ist damit der Kunde gemeint;
- Verarbeiten bzw. Verarbeitung bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit den Leistungen, wie z. B. das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den

Abgleich oder die Verknüpfung, die Einschränkung, die Rückgabe oder die Vernichtung, jeweils wie in den Datenverarbeitungsanweisungen beschrieben.

- Verbundenes Unternehmen bezeichnet jede Einheit, die derzeit oder künftig eine Partei dieser AVV beherrscht, von ihr beherrscht wird oder mit ihr unter gemeinsamer Beherrschung steht; „Beherrschung“ bedeutet hierbei die unmittelbare oder mittelbare Innehabung der Befugnis, die Geschäftsführung und die Grundsätze einer solchen Person oder Einheit zu bestimmen oder bestimmen zu lassen, sei es durch den Besitz stimmberechtigter Wertpapiere, durch Vertrag oder auf sonstige Weise.
- Verletzung des Schutzes personenbezogener Daten bezeichnet eine Sicherheitsverletzung, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder anderweitig verarbeitet wurden.

AVV Anlage

Die Anlagen dieser AVV sind unter folgendem Link verfügbar: https://revalizesoftware.com/Legal/Revalize-DPA-Annexes-2026-April-DE.pdf.