ZUSATZVEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

Diese Datenverarbeitungsvereinbarung ("AVV") regelt die Verarbeitung personenbezogener Daten durch die Revalize GmbH und ihre verbundenen Unternehmen ("Anbieter") für die Organisation, die den Bedingungen dieser DPA zustimmt ("Kunde"). Anbieter und Kunde werden hier jeweils einzeln als "Partei" oder gemeinsam als "Parteien" bezeichnet.

Während die Parteien eine Vereinbarung über die Bereitstellung von Software und/oder anderen Dienstleistungen durch den Anbieter für den Kunden ("Vereinbarung" oder "MSA") abgeschlossen haben, regelt diese DPA die Rechte und Pflichten der Parteien in Bezug auf die Verarbeitung personenbezogener Daten, die im Zusammenhang mit der Bereitstellung und dem Erhalt dieser Software und/oder anderer Dienstleistungen erfolgt.

Für und unter Berücksichtigung der hierin dargelegten Zusicherungen und Versprechen der Parteien und anderer guter und wertvoller Gegenleistungen, deren Erhalt und Hinlänglichkeit hiermit anerkannt werden, vereinbaren die Parteien Folgendes:

1. DEFINITIONEN.

Zusätzlich zu den in Anhang A definierten Begriffe haben alle definierten Begriffe die ihnen in dieser Zusatzvereinbarung zugewiesene Bedeutung und sind für die Zwecke dieser Zusatzvereinbarung im Falle von Konflikten maßgebend, einschließlich der folgenden Begriffe:

1.1 In dieser AVV haben die folgenden Begriffe die nachstehend angegebene Bedeutung und verwandte Begriffe sind entsprechend auszulegen:

1.1.1 Angemessenheitsbeschluss bedeutet für eine Rechtsordnung mit Datenschutzgesetzen, die Beschränkungen für die Datenübermittlung vorsehen, ein Land, das von der Aufsichtsbehörde oder einer anderen Stelle in dieser Rechtsordnung als ein Land anerkannt wird, das ein angemessenes Datenschutzniveau, wie es in den Datenschutzgesetzen des betreffenden Landes vorgeschrieben ist, so dass die Übermittlung in dieses Land ohne zusätzliche Anforderungen zulässig ist;

1.1.2 Verbundenes Unternehmen: jede Organisation, die den Unterzeichner dieser AVV jetzt oder in Zukunft kontrolliert, von ihm kontrolliert wird oder unter gemeinsamer Kontrolle steht, wobei "Kontrolle" definiert ist als der direkte oder indirekte Besitz der Befugnis, einer solchen Person oder Organisation, sei es durch den Besitz von stimmberechtigten Wertpapieren, durch einen Vertrag oder auf andere Weise, das Management und die Politik zu lenken oder zu bestimmen.

1.1.3 CCPA bezeichnet den California Consumer Privacy Act von 2018 (California Privacy Act Cal Civ Code § 1798.100 et seq) und seine Durchführungsbestimmungen;

1.1.4 Verantwortlicher für die Datenverarbeitung ist 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 des Begriffs "Unternehmen" gemäß der Definition des CCPA); im Zusammenhang mit dieser DSGVO ist damit der Kunde gemeint;

1.1.5 Datenverarbeitungsanweisungen sind die in Anhang 1 dieser AVV aufgeführten Weisungen;

1.1.6 Datenverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die Personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen Verarbeitet (einschließlich "Dienstleister" gemäß der Definition dieses Begriffs in der CCPA) und bedeutet im Zusammenhang mit dieser AVV Anbieter;

1.1.7 Betroffene Person ist die identifizierte oder identifizierbare Person, auf die sich die Personenbezogenen Daten beziehen (einschließlich "Verbraucher" gemäß der Definition im CCPA);

1.1.8 EU-DSGVO bezeichnet alle EU-Verordnungen, die (ganz oder teilweise) auf die Verarbeitung Personenbezogener Daten anwendbar sind, wie die Verordnung (EU) 2016/679;

1.1.9 EU-Standardvertragsklauseln sind die Vertragsklauseln im Anhang des Durchführungsbeschlusses 2021/914 der Europäischen Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, wie in Anhang 2 dieser AVV beigefügt;

1.1.10 Informationssicherheitsplan bezeichnet die technischen und organisatorischen Maßnahmen zur Informationssicherheit, die im Informationssicherheitsplan, der diesem Vertrag als Anhang 1 beigefügt ist, in seiner jeweils aktualisierten Fassung aufgeführt sind;

1.1.11 Verletzung des Schutzes Personenbezogener Daten; bedeutet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise Verarbeitet wurden;

1.1.12 Datenschutzgesetze bezeichnet alle Datenschutzgesetze und -vorschriften, die auf die betreffenden Personenbezogenen Daten anwendbar sind, einschließlich (ohne Einschränkung und soweit zutreffend) der EU-DSGVO, der UK-DSGVO und des CCPA, in der jeweils geltenden Fassung**.**

1.1.13 Verarbeiten oder Verarbeitung bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten wie das Erheben, den Zugang, 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, das Löschen oder die Vernichtung; wie in den Datenverarbeitungsanweisungen beschrieben.

1.1.14 Eingeschränkte Übermittlung bedeutet:

1.1.14.1 eine Übermittlung Personenbezogener Daten vom Kunden oder einem Verbundenen Unternehmen des Kunden an den Anbieter; oder

1.1.14.2 eine Weiterübermittlung Personenbezogener Daten vom Anbieter an einen Unterauftragsverarbeiter, wenn eine solche Übermittlung ohne eine genehmigte Übermittlungsmethode (wie z. B. (a) einem Angemessenheitsbeschluss, (b) Standardvertragsklauseln, (c) genehmigten Formen von Datenübermittlungsvereinbarungen oder -verfahren gemäß den geltenden Datenschutzgesetzen oder (d) einer zulässigen Ausnahmeregelung) durch die Datenschutzgesetze verboten wäre oder gegen die Bedingungen einer solchen anerkannten Übermittlungsmethode oder zulässigen Ausnahmeregelung verstoßen würde;

1.1.15 Dienste sind die Dienste und sonstigen Tätigkeiten, die vom Anbieter oder in seinem Namen für den Kunden gemäß dem Vertrag zu erbringen oder durchzuführen sind;

1.1.16 Standardvertragsklauseln sind die von einer Aufsichtsbehörde gemäß den Datenschutzgesetzen genehmigten Vertragsklauseln, die von Zeit zu Zeit aktualisiert werden können und die die Übermittlung Personenbezogener Daten in Fällen erlauben, in denen eine solche Übermittlung andernfalls eine Eingeschränkte Übermittlung wäre;

1.1.17 Unterauftragsverarbeiter ist jeder Dritte (einschließlich Dritter und Verbundener Unternehmen des Anbieters), der vom Anbieter oder in dessen Namen mit der Verarbeitung in Verbindung mit den Diensten beauftragt wird und in Anhang 1 dieser AVV aufgeführt ist;

1.1.18 Aufsichtsbehörde ist eine öffentliche Behörde oder eine staatliche oder quasi-staatliche Stelle, die in einem Land mit Datenschutzgesetzen eingerichtet wurde und für Datenschutzfragen zuständig ist;

1.1.19 UK-Zusatz bezeichnet das „UK Addendum to he EU Standard Contractual Clauses", das vom Information Commissioner's Office gemäß s.119A(1) des UK Data Protection Act 2018 herausgegeben wurde und dieser AVV als Anhang 3 beigefügt ist; und

1.1.20 UK-DGSVO bezeichnet die EU-DGSVO, wie sie aufgrund von Abschnitt 3 des European Union (Withdrawal) Act 2018 Teil des britischen Rechts ist;

1.1.21 Das Wort „einschließlich " ist so zu verstehen, dass es ohne Einschränkung einschließt, und verwandte Begriffe sind entsprechend auszulegen.

1.1.22 Die in dieser AVV verwendeten Begriffe haben die in dieser AVV festgelegte Bedeutung, wobei definierte Begriffe, die hier nicht anderweitig definiert sind, die Bedeutung haben, die ihnen in dem Vertrag gegeben wird. Mit Ausnahme der nachstehenden Änderungen bleiben die Bestimmungen des Vertrages unverändert und in vollem Umfang in Kraft und wirksam.

2. VERARBEITUNG VON PERSONENBEZOGENEN DATEN

2.1 Der Anbieter wird Personenbezogene Daten nicht: Aufbewahren, verwenden, offenlegen oder anderweitig Verarbeiten (auch nicht für seine eigenen kommerziellen Zwecke), außer auf dokumentierte Weisung des Kunden (wie in dieser AVV und im Vertrag dargelegt), es sei denn, die Verarbeitung ist nach geltendem Recht und gemäß den Bestimmungen der Standardvertragsklauseln (sofern anwendbar) erforderlich; oder

2.1.1 Personenbezogene Daten verkaufen, die sie vom Kunden erhalten oder im Zusammenhang mit der Erbringung der Dienste für den Kunden erhalten haben.

2.2 Kunde im eigenen Namen und im Namen jedes verbundenen Unternehmens des Kunden:

2.2.1 weist den Anbieter an:

2.2.1.1 Personenbezogene Daten zu Verarbeiten; und

2.2.1.2 insbesondere Personenbezogene Daten in ein beliebiges Land oder Gebiet zu übermitteln, soweit dies für die Erbringung der Dienste und im Einklang mit dieser AVV erforderlich ist.

2.3 In den Datenverarbeitungsanweisungen werden der Gegenstand und andere Einzelheiten der Verarbeitung der Personenbezogenen Daten, die im Rahmen der Dienste vorgesehen ist, dargelegt, einschließlich der Betroffenen Personen, der Kategorien Personenbezogener Daten, der besonderen Kategorien Personenbezogener Daten, der Unterauftragsverarbeiter und der Beschreibung der Verarbeitung.

2.4 Die Parteien erkennen an, dass die Übermittlung Personenbezogener Daten durch den Kunden an den Anbieter keinen „Verkauf" Personenbezogener Daten im Sinne der geltenden Datenschutzgesetze (einschließlich des CCPA) darstellt und dass der Anbieter dem Kunden im Austausch für die Personenbezogenen Daten kein Geld oder eine andere Gegenleistung von Wert bietet.

3. ANBIETERPERSONAL

Der Anbieter gewährleistet, dass die zur Verarbeitung der Personenbezogenen Daten befugten Personen:

3.1 sich zur Vertraulichkeit verpflichtet haben oder einer oder einer angemessenen gesetzlichen Verschwiegenheitspflicht in Bezug auf die Personenbezogenen Daten unterliegen; und

3.2 eine angemessene Schulung in Bezug auf den Schutz Personenbezogener Daten absolviert haben.

4. SICHERHEIT

4.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichen und der Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen setzt der Anbieter in Bezug auf die Personenbezogenen Daten geeignete technische und organisatorische Maßnahmen ein, die so konzipiert sind, dass sie bei der Erbringung der Dienste ein diesem Risiko angemessenes Schutzniveau gewährleisten; für die Zwecke dieser AVV sind die technischen und organisatorischen Maßnahmen des Anbieters im Informationssicherheitsplan festgelegt.

4.2 Bei der Bewertung des angemessenen Schutzniveaus berücksichtigt der Anbieter insbesondere die Risiken, die mit der Verarbeitung verbunden sind.

5. UNTERAUFTRAGSVERARBEITUNG.

5.1 Der Anbieter darf nur Unterauftragsverarbeiter ernennen, die es ihm ermöglichen, die Datenschutzgesetze einzuhalten. Der Kunde ermächtigt den Anbieter zur Ernennung von Unterauftragsverarbeitern gemäß diesem Abschnitt 5 vorbehaltlich etwaiger Einschränkungen oder Bedingungen, die ausdrücklich in dem Vertrag festgelegt sind. Die zum Zeitpunkt des Inkrafttretens dieser AVV ernannten Unterauftragsverarbeiter sind in den Datenverarbeitungsanweisungen aufgeführt. Der Anbieter bleibt gegenüber dem Kunden für die Erfüllung der Verpflichtungen der Unterauftragsverarbeiter im Rahmen des Vertrages haftbar.

5.2 Bevor der Anbieter einen neuen Unterauftragsverarbeiter einstellt, muss er den Kunden ungeachtet der in der Vereinbarung enthaltenen Mitteilungspflichten von der Ernennung in Kenntnis setzen und ihm Einzelheiten über die von dem vorgeschlagenen Unterauftragsverarbeiter vorzunehmende Verarbeitung mitteilen. Jeder neue Unterauftragsverarbeiter wird zu dem folgenden Link www.revalizesoftware.com\legal hinzugefügt und/oder dem Kunden per E-Mail mitgeteilt. Zusätzlich zu allen anderen Mitteilungen kann der Anbieter eine solche Mitteilung durch Aktualisierung der Liste der Unterauftragsverarbeiter in den Datenverarbeitungsanweisungen machen. Der Kunde kann dem Anbieter innerhalb von 15 Tagen nach der Benachrichtigung durch den Anbieter über die aktualisierte Liste der Unterauftragsverarbeiter etwaige Einwände (aus angemessenen Gründen im Zusammenhang mit Datenschutzgesetzen) gegen den vorgeschlagenen Unterauftragsverarbeiter oder die Datenverarbeitungsanweisungen mitteilen ("Einwände"), woraufhin der Anbieter und der Kunde nach Treu und Glauben verhandeln, um weitere Maßnahmen zu vereinbaren, einschließlich vertraglicher oder betrieblicher Anpassungen, die für die Ernennung des vorgeschlagenen Unterauftragsverarbeiters oder den Betrieb der Dienste relevant sind, um den Einwänden des Kunden Rechnung zu tragen. Können sich die Parteien nicht innerhalb von fünfundvierzig (45) Tagen nach Eingang des Widerspruchs beim Anbieter (oder einer vom Kunden schriftlich vereinbarten längeren Frist) auf weitere Maßnahmen einigen, kann der Kunde den Teil der Dienste, der die Nutzung des vorgeschlagenen Unterauftragsverarbeiters erfordert, oder einen anderen Teil der Dienste, der auf diese Weise beendet wird, durch schriftliche Mitteilung an den Anbieter mit sofortiger Wirkung kündigen.

6. RECHTE DER BETROFFENEN PERSON.

6.1 Der Anbieter muss:

6.1.1 sobald er davon Kenntnis erlangt, den Kunden unverzüglich benachrichtigen, wenn der Anbieter eine Anfrage einer Betroffenen Person zur Ausübung ihrer Betroffenenrechte erhält, die sich auf ein Betroffenenrecht der Betroffenen Person gemäß einem Datenschutzgesetz in Bezug auf Personenbezogene Daten bezieht;

6.1.2 nicht auf diese Anfrage reagieren, es sei denn, auf dokumentierte Weisung des Kunden oder es wird von einer Aufsichtsbehörde oder nach geltendem Recht verlangt; und

6.1.3 auf Anfrage des Kunden, sofern dies aufgrund von Datenschutzgesetzen und im Zusammenhang mit den Diensten erforderlich ist, den Kunden in angemessener Weise bei der Bearbeitung einer Anfrage zur Ausübung von Betroffenenrechten unterstützen, soweit der Kunde diese Anfrage nicht ohne die Unterstützung des Anbieters erfüllen kann. Der Anbieter kann diese Anforderung erfüllen, indem er (auf Kosten des Kunden) eine Funktionalität zur Verfügung stellt, die es dem Kunden ermöglicht, eine solche Anfrage zur Ausübung der Betroffenenrechte ohne zusätzliche Verarbeitung durch den Anbieter zu bearbeiten. Soweit eine solche Funktionalität nicht zur Verfügung steht, muss der Kunde, damit der Anbieter eine solche angemessene Unterstützung leisten kann, dem Anbieter eine solche Anfrage schriftlich übermitteln und dabei ausreichende Informationen zur Verfügung stellen, damit der Anbieter (auf Kosten des Kunden) den betreffenden Datensatz lokalisieren und anschließend ändern, exportieren oder löschen kann.

7. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN.

7.1 Der Anbieter muss den Kunden unverzüglich benachrichtigen, wenn der Anbieter oder ein Unterauftragsverarbeiter eine Verletzung des Schutzes Personenbezogener Daten bestätigt, und dem Kunden ausreichende Informationen zur Verfügung stellen, damit der Kunde seinen Verpflichtungen zur Meldung oder zur Information der Betroffenen Personen über die Verletzung des Schutzes Personenbezogener Daten gemäß den Datenschutzgesetzen nachkommen kann. Vorbehaltlich des nachstehenden Abschnitts 7.3 muss eine solche Benachrichtigung mindestens:

7.1.1 die Art der Verletzung des Schutzes Personenbezogener Daten, die Kategorien und die Zahl der Betroffenen Personen, die betroffenen Kategorien und die Zahl der betroffenen personenbezogenen Datensätze beschreiben;

7.1.2 den Namen und die Kontaktdaten des Datenschutzbeauftragten des Anbieters oder eines anderen Ansprechpartners, bei dem weitere Informationen erhältlich sind, enthalten;

7.1.3 die wahrscheinlichen Folgen der Verletzung des Schutzes Personenbezogener Daten beschreiben, soweit der Anbieter in der Lage ist, diese in Anbetracht der Art der Dienste und der Verletzung des Schutzes Personenbezogener Daten festzustellen; und

7.1.4 die Maßnahmen beschreiben, die zur Behebung der Verletzung des Schutzes Personenbezogener Daten ergriffen wurden oder ergriffen werden sollen.

7.2 Der Anbieter arbeitet mit dem Kunden zusammen und unternimmt die angemessenen kommerziellen Schritte, die erforderlich sind, um bei der Untersuchung, Abmilderung und Behebung einer solchen Verletzung des Schutzes Personenbezogener Daten zu helfen.

7.3 Wenn und soweit es nicht möglich ist, die Informationen zu übermitteln, oder wenn es dem Anbieter aufgrund von Gesetzen oder von Vollstreckungsbehörden untersagt ist, die in Abschnitt 7.1 genannten Informationen gleichzeitig zu übermitteln, können die Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung gestellt werden.

8. DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE KONSULTATION.

8.1 Soweit erforderlich, unterstützt der Anbieter den Kunden in angemessenem Umfang bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen mit Aufsichtsbehörden oder anderen zuständigen Datenschutzbehörden, die der Kunde nach vernünftigem Ermessen aufgrund von Datenschutzgesetzen für erforderlich hält, und zwar jeweils ausschließlich in Bezug auf die Verarbeitung Personenbezogener Daten durch den Anbieter und unter Berücksichtigung der Art der Verarbeitung und der dem Anbieter vorliegenden Informationen. Soweit eine solche Folgenabschätzung und/oder vorherige Konsultation Unterstützung erfordert, die über die Bereitstellung der entsprechenden Verarbeitungsprotokolle und Dokumentationen des Anbieters hinausgeht, behält sich der Anbieter das Recht vor, dem Kunden eine solche Beauftragung zu den dann geltenden Tagessätzen des Anbieters in Rechnung zu stellen.

9. LÖSCHUNG ODER RÜCKGABE VON PERSONENBEZOGENEN DATEN.

9.1 Innerhalb von dreißig (30) Tagen nach Kündigung oder Ablauf des Vertrages (die "Rückgabefrist") und vorbehaltlich des Abschnitts 9.2 unten, wird der Anbieter auf Wunsch des Kunden verfügbare Personenbezogene Daten entweder löschen oder zurückgeben. Hat sich der Kunde nicht für eine der beiden Möglichkeiten entschieden, kann der Anbieter nach Ablauf der Rückgabefrist alle Personenbezogenen Daten ohne Benachrichtigung oder Haftung gegenüber dem Kunden löschen und vernichten. Wenn der Kunde den Anbieter auffordert, verfügbare Personenbezogene Daten zurückzugeben, kann der Anbieter dieser Aufforderung nachkommen, indem er eine Funktion zur Verfügung stellt, die es dem Kunden ermöglicht, die Personenbezogenen Daten ohne zusätzliche Verarbeitung durch den Anbieter abzurufen. Lehnt der Kunde die Nutzung dieser Funktion ab, kann er innerhalb der Rückgabefrist vom Anbieter die Rückgabe der verfügbaren Personenbezogenen Daten im Rahmen einer Bestellung für die entsprechenden Professional Services verlangen. Wird der Vertrag wegen eines Verstoßes des Kunden gekündigt, hat der Anbieter das Recht, vom Kunden eine Vorauszahlung für diese Professional Services zu verlangen. Der Anbieter muss dem Kunden innerhalb von dreißig (30) Tagen nach dem Ersuchen des Kunden um eine solche Bestätigung schriftlich bestätigen, dass er die Bestimmungen dieses Abschnitts 9 vollständig eingehalten hat.

9.2 Der Anbieter darf Personenbezogene Daten nur in dem Umfang und für den Zeitraum aufbewahren, wie es die Datenschutzgesetze oder andere gesetzliche Vorschriften, denen der Anbieter unterliegt, vorschreiben, und immer unter der Voraussetzung, dass (a) während dieses Aufbewahrungszeitraums die Bestimmungen dieser AVV weiterhin Anwendung finden, (b) der Anbieter die Vertraulichkeit all dieser Personenbezogenen Daten sicherstellt und (c) der Anbieter sicherstellt, dass diese Personenbezogenen Daten nur für die Zwecke verarbeitet werden, die in den Datenschutzgesetzen, die ihre Speicherung vorschreiben, oder in anderen gesetzlichen Bestimmungen, denen der Anbieter unterliegt, festgelegt sind, und für keinen anderen Zweck.

10. ÜBERPRÜFUNGS-, AUDIT- UND INSPEKTIONSRECHTE.

10.1 Auf angemessene Anfrage des Kunden stellt der Anbieter alle relevanten und notwendigen Materialien, Unterlagen und Informationen in Bezug auf die technischen und organisatorischen Sicherheitsmaßnahmen des Anbieters zum Schutz der Personenbezogenen Daten im Zusammenhang mit den erbrachten Diensten zur Verfügung, um die Einhaltung der Datenschutzgesetze nachzuweisen. Diese Informationen können in zusammengefasster Form bereitgestellt werden, um das Risiko zu minimieren, dass diese Maßnahmen umgangen werden.

10.2 Der Anbieter stellt sicher, dass mindestens einmal jährlich eine Sicherheitsüberprüfung seiner technischen und organisatorischen Sicherheitsmaßnahmen in Übereinstimmung mit den Datenschutzgesetzen durchgeführt wird. Die Ergebnisse einer solchen

Sicherheitsüberprüfung werden in einem zusammenfassenden Bericht dokumentiert. Der Anbieter stellt dem Kunden auf Anfrage unverzüglich (i) eine vertrauliche Zusammenfassung des Berichts und (ii) einen Nachweis über die angemessene Behebung kritischer Probleme innerhalb von vier (4) Wochen nach dem Datum der Ausstellung des Auditberichts zur Verfügung.

10.3 Wenn der Kunde nach Abschluss, der in den Abschnitten 10.1 und 10.2 beschriebenen Schritte vernünftigerweise der Meinung ist, dass der Anbieter die Datenschutzgesetze nicht einhält, kann der Kunde vom Anbieter verlangen, dass dieser entweder per Webinar oder bei einer persönlichen Überprüfung Auszüge aller relevanten Informationen zur Verfügung stellt, die für den weiteren Nachweis der Einhaltung der Datenschutzgesetze erforderlich sind. Der Kunde, der eine solche Überprüfung vornimmt, muss den Anbieter in angemessener Weise benachrichtigen, indem er sich an den Direktor für Informationssicherheit des Anbieters unter privacy@revalizesoftware.com wendet, und jede Überprüfung wird gemäß diesem Abschnitt 10.3 durchgeführt.

10.4 Falls der Kunde vernünftigerweise der Meinung ist, dass seine Feststellungen nach Durchführung der in Abschnitt 10.3 dargelegten Schritten den Kunden nicht in die Lage versetzen, seinen Verpflichtungen gemäß den Datenschutzgesetzen in Bezug auf die Beauftragung des Anbieters im Wesentlichen nachzukommen, kann der Kunde den Anbieter mindestens dreißig (30) Tage im Voraus schriftlich von seiner Absicht in Kenntnis setzen, ein Audit durchzuführen, das Inspektionen des Anbieters durch den Kunden oder einen vom Kunden beauftragten Prüfer (der kein Konkurrent des Anbieters ist) beinhalten kann. Eine solche Prüfung und/oder Inspektion (i) unterliegt den zwischen dem Kunden (oder dem von ihm beauftragten Prüfer) und dem Anbieter vereinbarten Vertraulichkeitsverpflichtungen, (ii) wird nur in dem Umfang durchgeführt, der durch die geltenden Datenschutzgesetze vorgeschrieben ist, und darf unter den geltenden Datenschutzgesetzen nicht weiter eingeschränkt werden, (iii) darf den Anbieter nicht dazu verpflichten, die Vertraulichkeit von Sicherheitsaspekten seiner Systeme und/oder Datenverarbeitungseinrichtungen (einschließlich derjenigen seiner Unterauftragsverarbeiter) zu gefährden, und (iv) darf nicht in Fällen durchgeführt werden, in denen der Anbieter dadurch gegen seine Vertraulichkeitsverpflichtungen gegenüber anderen Kunden, Verkäufern und/oder Partnern des Anbieters verstoßen oder der Anbieter anderweitig gegen für den Anbieter geltende Gesetze verstoßen würde. Der Kunde (oder ein von ihm beauftragter Prüfer), der eine solche Prüfung oder Inspektion durchführt, muss es vermeiden, im Verlauf einer solchen Prüfung Schäden, Verletzungen oder Störungen an den Räumlichkeiten, der Ausrüstung, dem Personal und dem Geschäft des Anbieters zu verursachen. Soweit eine solche gemäß diesem Abschnitt 10.4 durchgeführte Prüfung einen (1) Arbeitstag überschreitet, behält sich der Anbieter das Recht vor, dem Kunden jeden weiteren Tag zu seinen dann gültigen Tagessätzen in Rechnung zu stellen.

10.5 Stellt der Kunde nach einer solchen Prüfung oder Inspektion gemäß Abschnitt 10.4 nach vernünftigem Ermessen fest, dass der Anbieter die Datenschutzgesetze nicht einhält, so übermittelt der Kunde dem Anbieter Einzelheiten dazu, woraufhin der Anbieter seine Antwort und, soweit erforderlich, den Entwurf eines Plans zur Behebung des Problems zur gegenseitigen Zustimmung der Parteien vorlegt (diese Zustimmung darf nicht unangemessen verweigert oder verzögert werden; der einvernehmlich vereinbarte Plan ist der "Behebungsplan"). Können die Parteien keine Einigung über den Behebungsplan erzielen, oder im Falle einer Vereinbarung eines Behebungsplans der Anbieter den Behebungsplan nicht zu den vereinbarten Terminen umsetzt und dies nicht innerhalb von fünfundvierzig (45) Tagen nach der Benachrichtigung des Kunden oder einer anderen zwischen den Parteien vereinbarten Frist behebt, kann der Kunde die Dienste, die von der nicht konformen Verarbeitung betroffen sind, ganz oder teilweise kündigen, wobei die übrigen Dienste von einer solchen Kündigung unberührt bleiben.

10.6 Die Rechte des Kunden gemäß diesem Abschnitt 10 können nur einmal pro Kalenderjahr ausgeübt werden, es sei denn, der Kunde ist der begründeten Ansicht, dass der Anbieter seine Verpflichtungen gemäß dieser AVV oder den Datenschutzgesetzen wesentlich verletzt.

11. EINGESCHRÄNKTE ÜBERMITTLUNGEN.

11.1 Der Kunde (als "Datenexporteur") und der Anbieter (als "Datenimporteur") vereinbaren hiermit, dass die anwendbaren Standardvertragsklauseln in Bezug auf jede Eingeschränkte Übermittlung vom Kunden oder eines Verbundenen Unternehmens des Kunden an den Anbieter in dem von den Datenschutzgesetzen vorgeschriebenen Umfang. Die Parteien vereinbaren, dass die Bestimmungen der Standardvertragsklauseln für die Eingeschränkte Übermittlung gelten sollen. Wenn Personenbezogene Daten der EU-DSGVO unterliegen, sind die anwendbaren Standardvertragsklauseln die EU--Standardvertragsklauseln, und wenn Personenbezogene Daten der UK-DSGVO unterliegen, sind die anwendbaren Standardvertragsklauseln der UK-Zusatz, der in jedem Fall wie hier beschrieben und wie in Anhang 2 und Anhang 3 dargelegt ausgefüllt wird.

11.2 Für die Zwecke von Anhang I oder eines anderen relevanten Teils der anwendbaren Standardvertragsklauseln werden in den Datenverarbeitungsanweisungen die betroffenen Personen, die Kategorien Personenbezogener Daten, die besonderen Kategorien Personenbezogener Daten, die Unterauftragsverarbeiter und die Beschreibung der Verarbeitung (Verarbeitungsvorgänge) angegeben. Wenn die EU-Standardvertragsklauseln für Übermittlungen vom Kunden oder einem Verbundenen Unternehmen des Kunden an den Anbieter gelten, werden sie wie in Anhang 2 dieser AVV beschrieben ausgefüllt. Optionale Klauseln in den anwendbaren Standardvertragsklauseln finden keine Anwendung, sofern in Anhang 2 dieser AVV nichts anderes festgelegt ist.

11.3 Für die Zwecke des Anhangs II oder eines anderen relevanten Teils der anwendbaren Standardvertragsklauseln enthält der Informationssicherheitsplan eine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die vom Anbieter (dem Datenimporteur) durchgeführt werden.

11.4 Wo immer die anwendbaren Standardvertragsklauseln eine Rechtswahl oder Gerichtsbarkeit ermöglichen, gelten die Gesetze und Gerichte Irlands, sofern nicht das anwendbare Datenschutzrecht etwas anderes vorschreibt.

11.5 Der Anbieter darf keine Eingeschränkte Übermittlung Personenbezogener Daten vornehmen, die er im Rahmen dieser AVV erhalten hat, es sei denn, er hat nach den geltenden Datenschutzgesetzen rechtmäßige Gründe dafür. Solche rechtmäßigen Gründe können sein: (a) ein Angemessenheitsbeschluss, (b) Standardvertragsklauseln, (c) die Bedingungen anderer anerkannter Formen von Datenübermittlungsvereinbarungen oder -verfahren oder (d) eine nach dem Datenschutzrecht zulässige Ausnahmeregelung.

12. ANDERE DATENSCHUTZGESETZE.

12.1 Soweit sich die Verarbeitung auf Personenbezogene Daten bezieht, die aus einer Rechtsordnung oder in einer Rechtsordnung stammen, die zwingende Anforderungen stellt oder in Zukunft solche Anforderungen einführt, können beide Parteien zusätzliche Maßnahmen vereinbaren, die erforderlich sind, um die Einhaltung der geltenden Datenschutzgesetze zu gewährleisten; solche zusätzlichen Maßnahmen, auf die sich die Parteien geeinigt haben, werden als Anhang zu dieser AVV oder in einem Auftrag zum Vertrag dokumentiert.

12.2 Der Kunde erklärt sich ferner damit einverstanden, dass der Anbieter in dem Maße, in dem er nach den geltenden Datenschutzgesetzen verpflichtet ist, einen angemessenen Übermittlungsmechanismus oder zusätzliche Sicherheitsvorkehrungen für die Übermittlung Personenbezogener Daten zu treffen, eine Vereinbarung zur Durchführung einer solchen Übermittlung in seinem eigenen Namen und, falls erforderlich, im Namen des Kunden auf benannter oder unbenannter Basis treffen kann.

12.3 Aufgrund der Tatsache, dass der Anbieter keine Kontrolle über die Art, den Charakter, die Eigenschaften, den Inhalt und/oder die Herkunft der im Rahmen dieser Vereinbarung

Verarbeiteten Personenbezogenen Daten hat, verstößt der Anbieter ungeachtet gegenteiliger Bestimmungen in dieser Vereinbarung nicht gegen diese AVV oder den Vertrag und haftet dem Kunden gegenüber nicht, wenn Personenbezogene Daten, die rechtlichen Anforderungen unterliegen, die Sicherheits-, Verarbeitungs- oder andere Maßnahmen vorschreiben, die nicht in dieser AVV festgelegt sind oder den Bedingungen dieser AVV widersprechen, vom Kunden zur Verfügung gestellt werden, ohne dass diese AVV geändert wird oder ein entsprechender Auftrag erteilt wird.

12.4 Wenn aufgrund einer Änderung der Datenschutzgesetze eine Änderung dieser AVV erforderlich ist, einschließlich einer Änderung der Standardvertragsklauseln, kann jede Partei die andere Partei schriftlich über diese Gesetzesänderung informieren. Die Parteien werden nach Treu und Glauben alle notwendigen Änderungen dieser AVV, einschließlich der Standardvertragsklauseln, erörtern und aushandeln, um solchen Änderungen Rechnung zu tragen.

13. ALLGEMEINE BEDINGUNGEN.

13.1 Die Parteien dieser AVV unterwerfen sich hiermit der Wahl des anwendbaren Rechts und der Gerichtsbarkeit, die in dem Vertrag festgelegt sind.

13.2 Diese AVV und alle außervertraglichen oder sonstigen Verpflichtungen, die sich aus oder in Verbindung mit ihr ergeben, unterliegen dem Recht des Landes oder Gebiets, das zu diesem Zweck in dem Vertrag festgelegt wurde. Das UN-Übereinkommen über Verträge über den internationalen Warenkauf findet in keiner Weise auf diesen Vertrag oder die Parteien Anwendung, ungeachtet des anwendbaren Rechts und der Gerichtsbarkeit.

13.3 Die Bestimmungen über das anwendbare Recht in dieser AVV gelten vorbehaltlich der Klauseln 7 (Schlichtung und Gerichtsstand) und 10 (Anwendbares Recht) der Standardvertragsklauseln, soweit diese auf die Eingeschränkte Übermittlung Personenbezogener Daten aus der Europäischen Union (einschließlich des Vereinigten Königreichs) in ein Drittland anwendbar sind.

14. RANGFOLGE.

14.1 Keine Bestimmung dieser AVV schränkt die Verpflichtungen des Anbieters oder eines Verbundenen Unternehmens des Anbieters unter dem Vertrag in Bezug auf den Schutz Personenbezogener Daten ein oder erlaubt es dem Anbieter oder einem Verbundenen Unternehmen des Anbieters, Personenbezogene Daten in einer Weise zu Verarbeiten (oder deren Verarbeitung zuzulassen), die durch den Vertrag untersagt ist. Im Falle von Widersprüchen zwischen den Bestimmungen dieser AVV und (i) dem Informationssicherheitsplan oder (ii) anderen Vereinbarungen zwischen den Parteien, einschließlich dem Vertrag und einschließlich (sofern nicht ausdrücklich schriftlich und im Namen der Parteien unterzeichnet etwas anderes vereinbart wurde) Vereinbarungen, die nach dem Datum dieser AVV abgeschlossen wurden oder angeblich abgeschlossen wurden, sind die Bestimmungen dieser AVV maßgebend. Zur Vermeidung von Zweifeln gelten die in dem Vertrag festgelegten Haftungsbeschränkungen und -ausschlüsse auch für diese AVV, soweit dies nach geltendem Recht zulässig ist.

15. SALVATORISCHE KLAUSEL.

Sollte eine Bestimmung dieser AVV ungültig oder nicht durchsetzbar sein, so bleibt der Rest dieser AVV gültig und in Kraft. Die unwirksame oder undurchführbare Bestimmung ist entweder (i) so zu ändern, dass ihre Wirksamkeit gewährleistet ist oder, wenn dies nicht möglich ist (ii) so auszulegen, als ob der unwirksame oder undurchführbare Teil nie bestanden hätte.

VEREINBART UND ANERKANNT:

[NAME]	**[NAME]**
(“KUNDE”)	**(“ANBIETER”)**
Durch _____	Durch _____
Titel _____	Titel: _____
Datum: _____	Datum: _____

ANHANG 1 ZUM AVV

WEISUNGEN ZUR DATENVERARBEITUNG

A. LISTE DER PARTEIEN

Wenn die Standardvertragsklauseln gelten, sind der/die Datenexporteur(e) und der/die Datenimporteur(e):

Organisation des Datenexporteurs	
Name:	Kunde wie in dem Vertrag angegeben.
Unterschrift und Datum:	Durch den Abschluss des Vertrages gelten die hierin einbezogenen Standardvertragsklauseln, zum Zeitpunkt des Inkrafttretens des Vertrages als vom Datenexporteur unterzeichnet.
Rolle (Verantwortlicher/Verarbeiter):	Verantwortlicher
Organisation des Datenimporteurs	
Name:	Revalize, Inc. oder deren verbundenes Unternehmen, wie in dem Vertrag angegeben.
Adresse:	Revalize, Inc. 8800 Baymeadows W #500, FL 32256 oder die eingetragene Adresse des verbundenen Unternehmens, das in dem Vertrag genannt ist.
Unterschrift und Datum:	Durch den Abschluss des Vertrages gelten die hierin einbezogenen Standardvertragsklauseln, zum Zeitpunkt des Inkrafttretens des Vertrages als vom Datenimporteur unterzeichnet.
Rolle (Verantwortlicher/Verarbeiter):	Verarbeiter
Zentraler Kontakt:	Kristen Shaheen, Chief Privacy Officer (dpo@revalizesoftware.com)

B. BESCHREIBUNG DER ÜBERMITTLUNG

Verarbeitungs-tätigkeit: Support	Der Anbieter kann in Übereinstimmung mit dem Supportplan des Anbieters Supportleistungen erbringen. Bei der Bereitstellung von Support kann der Anbieter vom Kunden aufgefordert werden, Personenbezogene Daten zu Verarbeiten. Der Anbieter kann bei der Bereitstellung von Support auf Personenbezogene Daten zugreifen und/oder diese erhalten. Nicht in jedem Supportfall wird auf Personenbezogene Daten zugegriffen und/oder werden diese erhalten, da einige Fehler ohne einen solchen Zugriff analysiert und behoben werden können, wenn der Hintergrund des Fehlers bekannt ist. Je nach Problemstellung kann der Anbieter oder ein Drittanbieter Support leisten, wodurch es zu einer internationalen Übermittlung von Personenbezogenen Daten kommen kann.

Verarbeitungs-tätigkeit: Professional	Wenn der Kunde im Rahmen einer Bestellung vom Anbieter verlangt, Professional Services zu erbringen, um die Bereitstellung des Produkts während der Laufzeit zu unterstützen, kann der Anbieter vom Kunden aufgefordert werden, Personenbezogene Daten als Teil dieses Auftrags zu Verarbeiten.
Verarbeitungs-tätigkeit: Gehostete Abonnement-dienste	Der Kunde lädt Daten auf die gehosteten Abonnementdienste hoch, um die Funktionalität des Produkts zu maximieren. Einige der Daten, die in die gehosteten Abonnementdienste hochgeladen werden können, können Personenbezogene Daten enthalten. Der Anbieter speichert (entweder direkt oder mit Hilfe eines dritten Unterverarbeiters, wie unten angegeben) alle Daten, die im Namen des Kunden in die gehosteten Abonnementdienste hochgeladen werden, in Übereinstimmung mit den von den Parteien einvernehmlich unter dem Vertrag festgelegten Bedingungen für den Dienst. Der Kunde bestimmt, wie und warum das Produkt zu seinem Vorteil genutzt werden soll, was die häufige oder seltene Nutzung Personenbezogener Daten einschließen kann. Der Kunde erkennt an, dass der Anbieter in Bezug auf diese Verarbeitungsvorgänge keine Kontrolle über die Übermittlung der Personenbezogenen Daten der Betroffenen Person hat und dass die Gestaltung der Daten, die an die gehosteten Abonnementdienste des Anbieters übermittelt werden sollen, jederzeit unter der Kontrolle des Kunden steht. Abgesehen von der Speicherung der Daten innerhalb der gehosteten Abonnementdienste (und der Bereitstellung von Support, falls zutreffend, wie oben beschrieben) ist der Anbieter nicht an den Verarbeitungsaktivitäten beteiligt, die mit dieser Nutzung des Produkts verbunden sind. Wenn der Kunde im Rahmen einer Bestellung vom Anbieter die Erbringung von Professional Services zur Unterstützung bei der Bereitstellung des Produkts oder der Application Managed Services während der Laufzeit verlangt, kann der Anbieter vom Kunden aufgefordert werden, Folgendes zu verarbeiten
Kategorien von Personenbezogenen Daten	▪ Mitarbeiterkategorien des Kunden: Name, Titel, Abteilung, ID-Nummer, Systemnutzung, E-Mail-Adresse, Berufsbezeichnung, Anmeldedaten und/oder Kontakttelefonnummer. ▪ Endnutzer- oder Verbraucherkategorien des Kunden: Name, E-Mail-Adresse, Kontakttelefonnummer, Kontonummer. Weitere Kategorien Personenbezogener Daten können vom Kunden entweder als Teil einer Support-Anfrage oder durch die Nutzung von Hosted Subscription Services durch den Kunden bereitgestellt werden.
Besondere Kategorien von Personenbezogenen Daten	Nicht anwendbar.
Betroffene Personen	Mitarbeiter, Klienten, Kunden und Lieferanten des Kunden. Mitarbeiter oder Auftragnehmer des Kunden, die sich an die technischen Support-Einrichtungen des Anbieters wenden.
Dauer der Verarbeitung	Unterstützung und Professional Services: Personenbezogene Daten werden nur so lange verarbeitet, wie es für die Erbringung der jeweiligen Support- und/oder Professional Services erforderlich ist. SaaS: Personenbezogene Daten werden für die Dauer der Dienste gespeichert und werden gelöscht oder an den Kunden zurückgegeben, wie in der Auftragsverarbeitungsvereinbarung festgelegt oder wie sie anderweitig vom Kunden während des Zugangszeitraums geändert oder gelöscht werden.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

ZUSTÄNDIGE AUFSICHTS-BEHÖRDE	Europäischer Wirtschaftsraum: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Baden-Württemberg (https://www.baden-wuerttemberg.datenschutz.de)
	Vereinigtes Königreich: Das Büro des Informationsbeauftragten (ICO) (https://ico.org.uk/)

D. UNTERAUFTRAGSVERARBEITER VON DRITTUNTERNEHMEN

Bitte beachten Sie die Liste(n), die Sie unter folgender Adresse finden:

https://revalizesoftware.com/legal

ANHANG 2 ZUM AVV

STANDARDVERTRAGSKLAUSELN (VERARBEITER) MODUL 2

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

(a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung von personenbezogenen Daten in ein Drittland eingehalten werden.

(b) Die Parteien:

(i) die in Anhang I.A 1 aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und

(ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Anbieter“,

haben sich mit diesen Standardvertragsklauseln (im Folgenden: "Klauseln") einverstanden erklärt.

(c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten, wie in Anhang I.B beschrieben.

(d) Die Anlage zu diesen Klauseln, mit den darin enthaltenen Anhängen, ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

(a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe, gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie - in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die die in diesen Klauseln festgelegten Standardvertragsklauseln, in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

(b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

[1] An*hang 1 dieser AVV dient als Anhang I.A.*

Klausel 3

Drittbegünstigte

(a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Anbieter geltend machen und durchsetzen, mit den folgenden Ausnahmen:

(i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7;

(ii) Klausel 8.1 Buchstabe (b), Klausel 8.9 Buchstaben (a), (c), (d) und (e);

(iii) Klausel 9 Buchstaben a), c), d) und e);

(iv) Klausel 12 Buchstaben a), d) und f);

(v) Klausel 13;

(vi) Klausel 15.1 Buchstaben c), d) und e);

(vii) Klausel 16 Buchstabe (e);

(viii) Klausel 18 Buchstaben a) und b).

(b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt.

Klausel 4

Auslegung

(a) Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.

(b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

(c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

Klausel 6

Beschreibung der Datenübermittlung(en)

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogener Daten, und der /die Zwecke, zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

Klausel 7

Kopplungsklausel

Nicht anwendbar.

ABSCHNITT II - PFLICHTEN DER PARTEIEN

Klausel 8

Datenschutzgarantien

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Anbieter— durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen — in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

8.1 Weisungen

(a) Der Anbieter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs. Der Datenexporteur kann solche Weisungen während der gesamten Vertragslaufzeit erteilen.

(b) Der Anbieter unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann.

8.2 Zweckbindung

Der Anbieter verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

8.3 Transparenz

Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anhang II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen. Diese Klausel gilt unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.4 Richtigkeit

Stellt der Anbieter fest, dass die erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet er unverzüglich den Datenexporteur. In diesem Fall arbeitet der Anbieter mit dem Datenexporteur zusammen, um die Daten zu löschen oder zu berichtigen.

8.5 Dauer der Verarbeitung und Löschung oder Rückgabe der Daten

Die Daten werden vom Datenimporteur nur für die in Anhang I.B angegebene Dauer verarbeitet. Nach Wahl des Datenexporteurs löscht der Anbieter nach Beendigung der Erbringung der Datenverarbeitungsdienste alle im Auftrag des Datenexporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenexporteur, dass dies erfolgt ist, oder gibt dem Datenexporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien. Bis zur Löschung oder Rückgabe der Daten stellt der Anbieter weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Anbieter lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Anbieter zu, dass er die Einhaltung dieser Klauseln

auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist. Dies gilt unbeschadet von Klausel 14, insbesondere der Pflicht des Anbieter gemäß Klausel 14 Buchstabe e, den Datenexporteur während der Vertragslaufzeit zu benachrichtigen, wenn er Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten oder gelten werden, die nicht mit den Anforderungen in Klausel 14 Buchstabe a im Einklang stehen.

8.6 Sicherheit der Verarbeitung

(a) Der Anbieter und, während der Datenübermittlung, auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu diesen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann. Im Falle einer Pseudonymisierung verbleiben die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, soweit möglich, unter der ausschließlichen Kontrolle des Datenexporteurs. Zur Erfüllung seinen Pflichten gemäß diesem Absatz setzt der Anbieter mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Anbieter führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

(b) Der Anbieter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Er gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(c) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Anbieter gemäß diesen Klauseln ergreift der Anbieter geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Anbieter dem Datenexporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde. Diese Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen. Wenn und soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

(d) Unter Berücksichtigung der Art der Verarbeitung und der dem Anbieter zur Verfügung stehenden Informationen arbeitet der Anbieter mit dem Datenexporteur zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen, insbesondere die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen.

8.7 Sensible Daten

Soweit die Übermittlung personenbezogene Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche

Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Anbieter die in Anhang I.B beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8 Weiterübermittlungen

Der Anbieter gibt die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs an Dritte weiter. Die Daten dürfen zudem nur an Dritte weitergegeben werden, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union ansässig sind (im Folgenden „Weiterübermittlung“), sofern der Dritte im Rahmen des betreffenden Moduls an diese Klauseln gebunden ist oder sich mit der Bindung daran einverstanden erklärt oder falls

(i) die Weiterübermittlung an ein Land erfolgt, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt,

(ii) der Dritte auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 im Hinblick auf die betreffende Verarbeitung gewährleistet,

(iii) die Weiterübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder

(iv) die Weiterübermittlung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Jede Weiterübermittlung erfolgt unter der Bedingung, dass der Anbieter alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

8.9 Dokumentation und Einhaltung der Klauseln

(a) Der Anbieter bearbeitet Anfragen des Datenexporteurs, die sich auf die Verarbeitung gemäß diesen Klauseln beziehen, umgehend und in angemessener Weise.

(b) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können. Insbesondere führt der Anbieter geeignete Aufzeichnungen über die im Auftrag des Datenexporteurs durchgeführten Verarbeitungstätigkeiten.

(c) Der Anbieter stellt dem Datenexporteur alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesen Klauseln festgelegten Pflichten nachzuweisen; auf Verlangen des Datenexporteurs ermöglicht er diesem, die unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung zu prüfen, und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Datenexporteur einschlägige Zertifizierungen des Datenimporteurs berücksichtigen.

(d) Der Datenexporteur kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Datenimporteurs umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

(e) Die Parteien stellen der zuständigen Aufsichtsbehörde die unter den Buchstaben b und c genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

Klausel 9

Einsatz von Unterauftragsverarbeitern

(a) Der Datenimporteur besitzt die allgemeine Genehmigung des Datenexporteurs für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Datenexporteur mindestens dreißig (30) Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch

Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Datenexporteur damit ausreichend Zeit ein, um vor der Beauftragung des/der Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Datenimporteur stellt dem Datenexporteur die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(b) Beauftragt der Anbieter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Datenexporteurs), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die den Datenimporteur gemäß diesen Klauseln binden, einschließlich im Hinblick auf Rechte als Drittbegünstigte für betroffene Personen. Die Parteien erklären sich damit einverstanden, dass der Anbieter durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 8.8 nachkommt. Der Anbieter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Anbieter gemäß diesen Klauseln unterliegt.

(c) Der Anbieter stellt dem Datenexporteur auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Anbieter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

(d) Der Anbieter haftet gegenüber dem Datenexporteur in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Anbieter geschlossenen Vertrag nachkommt. Der Anbieter benachrichtigt den Datenexporteur, wenn der Unterauftragsverarbeiter seinen Pflichten gemäß diesem Vertrag nicht nachkommt.

(e) Der Anbieter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Anbieter faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein — das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Klausel 10

Rechte der betroffenen Person

(a) Der Datenimporteur Anbieter unterrichtet den Datenexporteur unverzüglich über jeden Antrag, den er von einer betroffenen Person erhalten hat. Er beantwortet diesen Antrag nicht selbst, es sei denn, er wurde vom Datenexporteur dazu ermächtigt.

(b) Der Anbieter unterstützt den Datenexporteur bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 zu beantworten. Zu diesem Zweck legen die Parteien in Anhang II unter Berücksichtigung der Art der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen, durch die Unterstützung geleistet wird, sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

(c) Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Anbieter die Weisungen des Datenexporteurs.

Klausel 11

Rechtsbehelf

(a) Der Anbieter informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

(b) Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.

(c) Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Anbieter die Entscheidung der betroffenen Person an,

(i) eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 13 einzureichen,

(ii) den Streitfall an die zuständigen Gerichte im Sinne der Klausel 18 zu verweisen.

(d) Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80 Absatz 1 der Verordnung (EU) 2016/679 vertreten werden kann.

(e) Der Anbieter unterwirft sich einem nach geltendem Unionsrecht oder dem geltenden Recht eines Mitgliedstaats verbindlichen Beschluss.

(f) Der Anbieter erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

Klausel 12

Haftung

(a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

(b) Der Anbieter haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenimporteur oder sein Unterauftragsverarbeiter der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt.

(c) Ungeachtet von Buchstabe b haftet der Datenimporteur gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenexporteur oder der Datenimporteur (oder dessen Unterauftragsverarbeiter) der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs und, sofern der Datenexporteur ein im Auftrag eines Verantwortlichen handelnder Auftragsverarbeiter ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.

(d) Die Parteien erklären sich damit einverstanden, dass der Datenexporteur, der nach Buchstabe c für durch den Anbieter (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Anbieter den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Anbieters für den Schaden entspricht.

(e) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

(f) Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe e haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.

(g) Der Anbieter kann sich nicht auf das Verhalten eines Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung entziehen.

Klausel 13

Aufsicht

(a) Die Aufsichtsbehörde eines der Mitgliedstaaten, in denen die betroffenen Personen niedergelassen sind, deren personenbezogene Daten gemäß diesen Klauseln im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen übermittelt werden oder deren Verhalten beobachtet wird, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

(b) Der Anbieter erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

ABSCHNITT III - LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 14

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

(a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Anbieter geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

(b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:

(i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

(ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien,

(iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

(c) Der Anbieter versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe b nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.

(d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe b zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

(e) Der Anbieter erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe a im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe a im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht.

(f) Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Anbieter seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Anbieter ergreifen müssen, um Abhilfe zu schaffen. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben d und e Anwendung.

Klausel 15

Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

15.1 Benachrichtigung

(a) Der Anbieter erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen,

(i) wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder

(ii) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.

(b) Ist es dem Anbieter gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Anbieter einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Anbieter verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.

(c) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Anbieter bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).

(d) Der Anbieter erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben a bis c während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

(e) Die Buchstaben a bis c gelten unbeschadet der Pflicht des Anbieters gemäß Klausel 14 Buchstabe e und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

15.2 Überprüfung der Rechtmäßigkeit und Datenminimierung

(a) Der Anbieter erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Anbieter mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Anbieter einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Anbieters gemäß Klausel 14 Buchstabe e.

(b) Der Anbieter erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.

(c) Der Anbieter erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

ABSCHNITT IV - SCHLUSSBESTIMMUNGEN

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrages

(a) Der Anbieter unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

(b) Verstößt der Anbieter gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur Anbieter aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14 Buchstabe f.

(c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

(i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe b ausgesetzt hat und die Einhaltung dieser

Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,

(ii) der Datenimporteur Anbieter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

(iii) der Datenimporteur Anbieter einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

(a) Personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten. Der Datenimporteur Anbieter bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur Anbieter weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur Anbieter lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur Anbieter zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

(b) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn (i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder (ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 17

Anwendbares Recht

Diese Klauseln unterliegen dem Recht des EU-Mitgliedstaats, in dem der Datenexporteur niedergelassen ist. Wenn dieses Recht keine Rechte als Drittbegünstigte zulässt, unterliegen diese Klauseln dem Recht eines anderen EU-Mitgliedstaats, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von Irland ist.

Klausel 18

Gerichtsstand und Zuständigkeit

(a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.

(b) Die Parteien vereinbaren, dass dies die Gerichte von Irland sind.

(c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Anbieter auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.

(d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

ANHANG 3 zum AVV - UK Zusatz

Vom Commissioner gemäß S119A(1) Data Protection Act 2018

herauszugebende Standarddatenschutzklauseln

Zusatz zu den Standardvertragsklauseln der EU-Kommission für den

internationalen Datentransfer

VERSION B1.0, in Kraft am 21. März 2022

Dieser Zusatz wurde vom Information Commissioner für Parteien, die Eingeschränkte Übermittlungen vornehmen, herausgegeben. Der Information Commissioner ist der Ansicht, dass es Angemessene Garantien für Eingeschränkte Übermittlungen bietet, wenn er als rechtsverbindlicher Vertrag abgeschlossen wird.

Teil 1: Tabellen

Tabelle 1: Parteien

Datum des Beginns	Das Datum des Inkrafttretens, wie in dem Vertrag definiert.	
Die Parteien	Exporteur (der die Eingeschränkte Übermittlung sendet)	Importeur (der die Eingeschränkte Übermittlung erhält)
Angaben zu den Parteien	Vollständiger rechtlicher Name: wie in Teil A, Anhang 1 der AVV angegeben . Handelsname (falls abweichend): Wie in Teil A, Anhang 1 der AVV angegeben. Hauptanschrift (falls es sich um eine Firmenanschrift handelt): Wie in Teil A, Anhang 1 der AVV angegeben. Offizielle Registrierungsnummer (falls vorhanden) (Unternehmensnummer oder ähnliche Kennung): Wie in Teil A, Anhang 1 der AVV angegeben.	Vollständiger rechtlicher Name: wie in Teil A, Anhang 1 der AVV angegeben. Handelsname (falls abweichend): Wie die in Teil A, Anhang 1 der AVV angegeben. Hauptanschrift (falls es sich um eine Firmenanschrift handelt): Wie in Teil A, Anhang 1 der AVV angegeben. Offizielle Registrierungsnummer (falls vorhanden) (Unternehmensnummer oder ähnliche Kennung): Wie in Teil A, Anhang 1 der AVV angegeben.
Wichtiger Kontakt	Vollständiger Name (fakultativ): Berufsbezeichnung: Wie in Teil A, Anhang 1 des der AVV angegeben	Vollständiger Name (fakultativ): Berufsbezeichnung: Wie in Teil A, Anhang 1 der AVV angegeben.

	Kontaktinformationen einschließlich E-Mail: Wie in Teil A Anhang 1 des AVV angegeben.	Kontaktinformationen einschließlich E-Mail: Wie in Teil A, Anhang 1 der AVV angegeben.
Unterschrift (falls für die Zwecke von Abschnitt 2 erforderlich)	Wie im Unterschriftsblock der AVV angegeben.	Wie im Unterschriftsblock der AVV angegeben.

Tabelle 2: Ausgewählte Standardvertragsklauseln, Module und ausgewählte Klauseln

Zusatz EU Standardvertragsklauseln		[X] Die Version der Genehmigten Standardvertragsklauseln, denen dieser Zusatz beigefügt ist, einschließlich der Angaben im Anhang: Datum: wie in der AVV in Anhang 1 und Anhang 2 sowie im Informationssicherheitsplan festgelegt. Referenz (falls vorhanden): Andere Kennung (falls vorhanden): Oder [ ] die Genehmigten EU-Standardvertragsklauseln, einschließlich der Informationen im Anhang, wobei nur die folgenden Module, Klauseln oder fakultativen Bestimmungen der Genehmigten EU-Standardvertragsklauseln für die Zwecke dieses Zusatzes wirksam werden:				
Modul	Genutztes Modul	Klausel 7 (Koppelungsklausel)	Klausel 11 (Option)	Klausel 9a (Vorherige Genehmigung oder Allgemeine Autorisierung)	Klausel 9a (Zeitraum)	Werden vom Importeur erhaltende personenbezogene Daten mit vom Exporteur gesammelten personenbezogenen Daten kombiniert?
1						
2						
3						
4						

Tabelle 3: Informationen zum Anhang

"Informationen zum Anhang" sind die Informationen, die für die ausgewählten Module gemäß dem Anhang der Genehmigten EU-Standardvertragsklauseln (mit Ausnahme der Parteien) bereitgestellt werden müssen und die für diesen Zusatz enthalten sind in:

Anhang 1A	Liste der Parteien:	Wie in Teil A des Anhangs I der Anlage zu den EU-Standardvertragsklauseln, die in Anhang 1 dieser AVV beigefügt ist, festgelegt.
Anhang 1B	Beschreibung der Übertragung:	Wie in Teil B des Anhangs I der Anlage zu den EU-Standardvertragsklauseln, die in Anhang 1 dieser AVV beigefügt ist, festgelegt.
Anhang II	Technische und organisatorische Maßnahmen einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Daten:	Wie in Anhang II der Anlage zu den EU-Standardvertragsklauseln, und im Informationssicherheitsplan detailliert beschrieben.
Anhang III	Liste der Unterauftragsverarbeiter (nur Module 2 und 3)	k. A..

Tabelle 4: Beendigung dieses Zusatzes bei Änderungen des Genehmigten Zusatzes

Beendigung dieses Zusatzes bei Änderungen des Genehmigten Zusatzes	Welche Partei(en) diesen Zusatz gemäß Abschnitt 19 beenden kann (können): [X] Importeur [X] Exporteur [ ] Keine der beiden Parteien

Teil 2: Obligatorische Klauseln

Zusatz	Dieser Zusatz zum internationalen Datentransfer besteht aus diesem Zusatz, der das Addendum EU-Standardvertragsklauseln enthält.
Addendum EU-Standardvertragsklauseln	Die Version(en) der Genehmigten EU-Standardvertragsklauseln, denen dieser Zusatz beigefügt ist, wie in Tabelle 2 aufgeführt, einschließlich der Informationen im Anhang.
Informationen im Anhang	Wie in Tabelle 3 dargelegt.
Geeignete Garantien	Die Schutzstandards für die Rechte der betroffenen Personen in Bezug auf Personenbezogene Daten, die nach den Datenschutzgesetzen des Vereinigten Königreichs erforderlich sind, wenn Sie eine Eingeschränkte Übermittlung vornehmen und

	sich dabei auf die Standard-Datenschutzklauseln gemäß Artikel 46 Absatz 2 der britischen Datenschutz-Grundverordnung stützen.
Genehmigter Zusatz	Der vom ICO herausgegebene und dem Parlament gemäß § 119A des Data Protection Act 2018 am 2. Februar 2022 vorgelegte Muster-Zusatz in der gemäß § 18 überarbeiteten Fassung.
Genehmigte EU-Standardvertragsklauseln	Die Standardvertragsklauseln, die im Anhang des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 aufgeführt sind.
ICO	Der Information Commissioner.
Eingeschränkte Übermittlung	Eine Übermittlung, die unter Kapitel V der UK-DGSVO fällt.
UK	Das Vereinigte Königreich von Großbritannien und Nordirland.
UK-Datenschutzgesetze	Alle Gesetze, die sich auf den Datenschutz, die Verarbeitung personenbezogener Daten, den Schutz der Privatsphäre und/oder die elektronische Kommunikation beziehen und die von Zeit zu Zeit im Vereinigten Königreich in Kraft sind, einschließlich der UK-DGSVO und des Data Protection Act 2018**.**
UK DGSVO	Wie in Abschnitt 3 des Data Protection Act 2018 definiert.

Vereinbarung dieses Zusatzes

1. Jede Partei erklärt sich damit einverstanden, an die in diesem Zusatz festgelegten Bedingungen gebunden zu sein, und zwar im Gegenzug dafür, dass die andere Partei sich ebenfalls einverstanden erklärt, daran gebunden zu sein.

2. Obwohl Anhang 1A und Klausel 7 der Genehmigten EU-Standardvertragsklauseln von den Parteien unterzeichnet werden müssen, können die Parteien zum Zwecke von Beschränkten Übermittlungen diesen Zusatz in einer Weise schließen, die ihn für die Parteien rechtsverbindlich macht und es den betroffenen Personen ermöglicht, ihre in diesem Zusatz festgelegten Rechte durchzusetzen. Die Vereinbarung dieses Zusatzes hat dieselbe Wirkung wie die Unterzeichnung der Genehmigten EU-Standardvertragsklauseln und jedes Teils der Genehmigten EU-Standardvertragsklauseln.

Auslegung dieses Zusatzes

3. Werden in diesem Zusatz Begriffe verwendet, die in den Genehmigten EU-Standardvertragsklauseln definiert sind, so haben diese Begriffe die gleiche Bedeutung wie in den Genehmigten EU-Standardvertragsklauseln. Darüber hinaus haben die folgenden Begriffe die folgende Bedeutung:

4. Dieser Zusatz muss immer so ausgelegt werden, dass er mit den UK- Datenschutzgesetzen übereinstimmt und somit die Verpflichtung der Vertragsparteien erfüllt, die Geeigneten Garantien zur Verfügung zu stellen.

5. Sollten die in dem Addendum EU- Standardvertragsklauseln enthaltenen Bestimmungen die Genehmigten EU-Standardvertragsklauseln in einer Weise ändern, die nach den Genehmigten Standardvertragsklauseln oder dem Genehmigten Zusatz nicht zulässig ist, werden diese Änderung(en) nicht in diesen Zusatz aufgenommen und die entsprechenden Bestimmungen der Genehmigten EU-Standardvertragsklauseln treten an ihre Stelle.

6. Im Falle von Widersprüchen oder Konflikten zwischen den UK-Datenschutzgesetzen und diesem Zusatz gelten die UK-Datenschutzgesetze.

7. Wenn die Bedeutung dieses Zusatzes unklar ist oder es mehr als eine Bedeutung gibt, gilt die Bedeutung, die am ehesten mit den UK- Datenschutzgesetzen übereinstimmt.

8. Jede Bezugnahme auf Rechtsvorschriften (oder bestimmte Bestimmungen von Rechtsvorschriften) bedeutet, dass diese Rechtsvorschriften (oder bestimmte Bestimmungen) im Laufe der Zeit geändert werden können. Dies gilt auch für den Fall, dass diese Rechtsvorschriften (oder spezifischen Bestimmungen) nach Vereinbarung dieses Zusatzes konsolidiert, wieder in Kraft gesetzt und/oder ersetzt worden sind.

Hierarchie

9. Obwohl Klausel 5 der Genehmigten EU-Standardvertragsklauseln festlegt, dass die Genehmigten EU-Standardvertragsklauseln Vorrang vor allen damit zusammenhängenden Vereinbarungen zwischen den Parteien haben, vereinbaren die Parteien, dass bei Beschränkten Übermittlungen die Hierarchie in Abschnitt 10 Vorrang hat.

10. Bei Unstimmigkeiten oder Widersprüchen zwischen dem Genehmigten Zusatz und dem Addendum EU-Standardvertragsklauseln (soweit zutreffend) hat der Genehmigte Zusatz Vorrang vor dem Addendum EU-Standardvertragsklauseln, es sei denn, die widersprüchlichen oder kollidierenden Bestimmungen des Addendums EU Standardvertragsklauseln bieten einen besseren Schutz für die betroffenen Personen; in diesem Fall haben diese Bestimmungen Vorrang vor dem Genehmigten Zusatz.

11. Soweit dieser Zusatz Addendum EU-Standardvertragsklauseln enthält, die zum Schutz von Übermittlungen abgeschlossen wurden, die der Datenschutzgrundverordnung (EU) 2016/679 unterliegen, erkennen die Parteien an, dass dieser Zusatz keine Auswirkungen auf diese Addendum EU--Standardvertragsklauseln hat.

Übernahme und Änderungen der EU-Standardvertragsklauseln

12. Dieser Zusatz enthält das Addendum EU Standardvertragsklauseln, das im erforderlichen Umfang geändert wird, so dass:

    a. Sie gemeinsam für Datenübermittlungen des Datenexporteurs an den Datenimporteur, soweit die UK- Datenschutzgesetze auf die Verarbeitung durch den Datenexporteur bei dieser Datenübermittlung anwendbar sind, gelten und sie Geeignete Garantien für diese Datenübermittlungen bieten;

    b. Die Abschnitte 9 bis 11 Vorrang vor Klausel 5 (Hierarchie) des Addendums EU Standardvertragsklauseln haben; und

    c. Dieser Zusatz (einschließlich der darin enthaltenen EU-Standardvertragsklauseln) (1) dem Recht von England und Wales unterliegt und (2) alle sich daraus ergebenden Streitigkeiten von den Gerichten von England und Wales entschieden werden, es sei denn, die Parteien haben ausdrücklich die Gesetze und/oder Gerichte von Schottland oder Nordirland gewählt. Sofern die Vertragsparteien keine anderen Änderungen vereinbart haben, die den Anforderungen von Abschnitt 12 entsprechen, gelten die Bestimmungen von Abschnitt 15.

13. An den Genehmigten EU-Standardvertragsklauseln dürfen keine anderen Änderungen vorgenommen werden als die, die den Anforderungen von Abschnitt 12 entsprechen.

14. Es werden die folgenden Änderungen am Addendum EU-Standardvertragsklauseln (für die Zwecke von Abschnitt 12) vorgenommen:

    a. Verweise auf die "Klauseln" bezeichnen diesen Zusatz, der das Addendum EU-Standardvertragsklauseln enthält;

    b. In Klausel 2 werden die Worte gestrichen:

    "sowie - in Bezug auf Datenübermittlungen von für die Verarbeitung Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter, Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679";

c. Klausel 6 (Beschreibung der Übermittlung(en)) erhält folgende Fassung:

"Die Einzelheiten der Datenübermittlung(en) und insbesondere die Kategorien der übermittelten personenbezogener Daten, sowie der Zweck/die Zwecke der Übermittlung zu dem/denen sie übermittelt werden) sind die in Anhang I.B genannten, wenn die UK-Datenschutzgesetze auf die Verarbeitung durch den Datenexporteur bei der Übermittlung Anwendung finden";

d. Klausel 8.7(i) von Modul 1 erhält folgende Fassung:

"Sie erfolgt in ein Land, das von den Angemessenheitsbestimmungen gemäß Abschnitt 17A der UK-DGSVO profitiert, die die Weiterübermittlung von Daten an ein anderes Land abdecken."

e. Klausel 8.8(i) der Module 2 und 3 erhält folgende Fassung:

"die Weiterübermittlung in ein Land erfolgt, für das Angemessenheitsvorschriften gemäß Abschnitt 17A der britischen Datenschutz-Grundverordnung gelten, die die Weiterübermittlung abdecken;".

f. Verweise auf "Verordnung (EU) 2016/679", "Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)" und "diese Verordnung" werden alle durch "UK -Datenschutzgesetze " ersetzt. Verweise auf bestimmte Artikel der "Verordnung (EU) 2016/679" werden durch den entsprechenden Artikel oder Abschnitt der UK--Datenschutzgesetze ersetzt;

g. Verweise auf die Verordnung (EU) 2018/1725 werden entfernt;

h. Verweise auf die "Europäische Union", "Union", "EU", "EU-Mitgliedstaat", "Mitgliedstaat" und "EU oder Mitgliedstaat" werden alle durch "UK" ersetzt;

i. Der Verweis auf "Klausel 12(c)(i)" in Klausel 10(b)(i) des ersten Moduls wird durch "Klausel 11(c)(i)" ersetzt;

j. Klausel 13(a) und Teil C von Anhang I werden nicht verwendet;

k. Die Begriffe "zuständige Aufsichtsbehörde" und "Aufsichtsbehörde" werden beide durch den " Information Commissioner " ersetzt;

l. In Klausel 16 Buchstabe e) erhält der Unterabschnitt i) folgende Fassung:

"Der Secretary of State erlässt gemäß Abschnitt 17A des Data Protection Act 2018 Bestimmungen, die die Übermittlung von personenbezogenen Daten, für die diese Klauseln gelten, abdecken;"

m. Klausel 17 wird ersetzt durch: "Diese Klauseln unterliegen den Gesetzen von England und Wales.";

n. Klausel 18 wird ersetzt durch:

"Alle Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten in England und Wales beigelegt. Eine betroffene Person kann Klage gegen auch den Datenexporteur und/oder den Datenimporteur vor den Gerichten eines beliebigen Landes des Vereinigten Königreichs verklagen. Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen"; und

o. Die Fußnoten zu den Genehmigten EU-Standardvertragsklauseln sind mit Ausnahme der Fußnoten 8, 9, 10 und 11 nicht Teil des Addendums.

Änderungen an diesem Zusatz

15. Die Vertragsparteien können vereinbaren, die Klauseln 17 und/oder 18 des Addendums EU - Standardvertragsklauseln so zu ändern, dass auf das Recht und/oder die Gerichte von Schottland oder Nordirland verwiesen wird.

16. Möchten die Vertragsparteien das Format der in Teil 1: Tabellen des Genehmigten Zusatzes enthaltenen Informationen ändern, so können sie dies durch eine schriftliche Vereinbarung tun, sofern die Änderung nicht zu einer Verringerung der angemessenen Sicherheitsvorkehrungen führt.

17. Von Zeit zu Zeit kann der ICO ein überarbeitetes Genehmigtes Addendum herausgeben, das:

a. angemessene und verhältnismäßige Änderungen an dem Genehmigten Zusatz vornimmt, einschließlich der Berichtigung von Fehlern in dem Genehmigten Zusatz; und/oder

b. die Änderungen der UK-Datenschutzgesetze widerspiegelt;

In der überarbeiteten Fassung des Genehmigten Zusatzes wird das Datum angegeben, ab dem die Änderungen des Genehmigten Zusatzes wirksam werden, und ob die Parteien diesen Zusatz einschließlich der Informationen im Anhang überprüfen müssen. Dieser Zusatz wird ab dem angegebenen Anfangsdatum automatisch wie in dem überarbeiteten Genehmigten Zusatz festgehalten geändert.

18. Wenn der ICO ein überarbeitetes Genehmigtes Addendum gemäß Abschnitt 18 herausgibt, und eine der in Tabelle 4 "Beendigung des Addendums“, wenn sich das Genehmigte Addendum ändert" ausgewählten Parteien als unmittelbare Folge der Änderungen des Genehmigten Addendums einen erheblichen, unverhältnismäßigen und nachweisbaren Anstieg:

a. in seinen direkten Kosten für die Erfüllung seiner Verpflichtungen aus dem Zusatz hat; und/oder
b. in den Risiken, die sie im Rahmen des Zusatzes zu tragen hat,

erleidet;

und in beiden Fällen zunächst angemessene Schritte unternommen hat, um diese Kosten und Risiken zu verringern, so dass sie nicht erheblich und unverhältnismäßig sind, kann sie diesen Zusatz nach Ablauf einer angemessenen Frist beenden, indem sie die andere Vertragspartei vor dem Inkrafttreten des geänderten Genehmigten Zusatzes schriftlich innerhalb dieser Frist darüber informiert.

19. Die Parteien benötigen nicht die Zustimmung Dritter, um Änderungen an diesem Zusatz vorzunehmen, doch müssen alle Änderungen im Einklang mit den Bestimmungen dieses Zusatzes vorgenommen werden.

INFORMATIONSSICHERHEITSPLAN

TEIL 1 - SICHERHEITSMASSNAHMEN

Technische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	Beschreibung
1. Inventarisierung und Kontrolle von Hardwareanlagen	Aktive Verwaltung aller Hardwaregeräte im Netzwerk, damit nur autorisierte Geräte Zugang erhalten und nicht autorisierte und nicht verwaltete Geräte gefunden und am Zugang gehindert werden.
2. Inventarisierung und Kontrolle von Softwarebeständen	Aktive Verwaltung der gesamten Software im Netz, so dass nur zugelassene Software installiert wird und ausgeführt werden kann und dass nicht zugelassene und nicht verwaltete Software gefunden und an der Installation oder Ausführung gehindert wird.
3. Kontinuierliches Schwachstellenmanagement	Kontinuierliche Sammlung neuer Informationen, Bewertung und Ergreifung von Maßnahmen, um Schwachstellen zu erkennen, zu beheben und die Chancen für Angreifer zu minimieren.
4. Kontrollierte Nutzung von Verwaltungsprivilegien	Pflege von Prozessen und Werkzeugen zur Verfolgung, Kontrolle, Verhinderung und Korrektur der Nutzung, Zuweisung und Konfiguration von administrativen Berechtigungen für Computer, Netzwerke, Anwendungen und Daten.
5. Sichere Konfiguration für Hardware und Software auf mobilen Geräten, Laptops, Workstations und Servern	Implementierung und Verwaltung der Sicherheitskonfiguration von mobilen Geräten, Laptops, Servern und Workstations mithilfe eines Konfigurationsmanagement- und Änderungskontrollprozesses, um Angreifer daran zu hindern, anfällige Dienste und Einstellungen auszunutzen.
6. Pflege, Überwachung und Analyse von Audit-Protokollen	Sammeln, Verwalten und Analysieren von Audit- und Sicherheitsprotokollen von Ereignissen, die zur Erkennung, zum Verständnis oder zur Wiederherstellung nach einem möglichen Angriff beitragen könnten.
7. Schutz von E-Mail und Webbrowser	Einsatz von automatisierten Kontrollen, um die Angriffsfläche und die Möglichkeiten für Angreifer zu minimieren, menschliches Verhalten durch Interaktion mit Webbrowsern und E-Mail-Systemen oder -Inhalten zu manipulieren.

8. Malware-Abwehr	Kontrollieren der Installation, Verbreitung und Ausführung von bösartigen Codes an verschiedenen Stellen im Unternehmen und gleichzeitige Optimierung des Einsatzes von Automatisierung, um eine schnelle Aktualisierung der Abwehr, Datenerfassung und Korrekturmaßnahmen zu ermöglichen.
9. Begrenzung und Kontrolle von Netzanschlüssen, Protokollen und Diensten	Verwalten (verfolgen, kontrollieren, korrigieren) der laufenden betrieblichen Nutzung von Ports, Protokollen, Diensten und Anwendungen auf vernetzten Geräten, um die für Angreifer verfügbaren Schwachstellen und Angriffsmöglichkeiten zu minimieren.
10. Möglichkeiten der Datenwiederherstellung	Pflege von Prozessen und Werkzeugen zur ordnungsgemäßen Sicherung personenbezogener Daten mit einer bewährten Methodik, um die Vertraulichkeit, Integrität, Verfügbarkeit und Wiederherstellbarkeit dieser Daten zu gewährleisten.
11. Sichere Konfiguration von Netzwerkgeräten, wie Firewalls, Router und Switches	Implementierung und Verwaltung der Sicherheitskonfiguration von Netzinfrastrukturgeräten mithilfe eines Konfigurationsmanagement- und Änderungskontrollprozesses, um Angreifer daran zu hindern, anfällige Dienste und Einstellungen auszunutzen.
12. Grenzverteidigung	Erkennen, Verhindern und Korrigieren des Informationsflusses bei der Übertragung von Netzen unterschiedlicher Vertrauensstufen mit Schwerpunkt auf personenbezogenen Daten.
13. Schutz der Daten	Pflege von Prozessen und Werkzeugen zur Verhinderung der Datenexfiltration, zur Abschwächung der Auswirkungen exfiltrierter Daten und zur Gewährleistung der Vertraulichkeit und Integrität personenbezogener Daten.
14. Kontrollierter Zugang auf der Grundlage des Wissensbedarfs	Pflege von Prozessen und Werkzeugen zur Verfolgung, Kontrolle, Verhinderung und Korrektur des sicheren Zugriffs auf kritische oder kontrollierte Güter (z.B. Informationen, Ressourcen, Systeme) entsprechend der formalen Bestimmung, welche Personen, Computer und Anwendungen auf der Grundlage einer genehmigten Klassifizierung einen Bedarf und ein Recht auf Zugriff auf diese kritischen oder kontrollierten Güter haben.
15. Drahtlose Zugangskontrolle	Pflege von Prozessen und Tools zur Überwachung, Kontrolle, Vorbeugung und Korrektur der sicheren Nutzung von drahtlosen lokalen Netzwerken (WLANs), Zugangspunkten und drahtlosen Clientsystemen

16. Überwachung und Kontrolle von Konten	Aktives Management des Lebenszyklus von System- und Anwendungskonten, ihrer Erstellung, Nutzung, Ruhestellung und Löschung, um die Möglichkeiten einer unbefugten, unangemessenen oder schändlichen Nutzung zu minimieren.

TEIL 2 - ZUSÄTZLICHE MASSNAHMEN

1. Umsetzung eines umfassenden Informationssicherheitsprogramms	Durch die Umsetzung eines umfassenden Informationssicherheitsprogramms (Comprehensive Information Security Programme, CISP) verschiedene administrative Schutzmaßnahmen zum Schutz personenbezogener Daten aufrechterhalten. Diese Maßnahmen sollen Folgendes gewährleisten: Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten Schutz vor unbefugtem Zugriff auf (gespeicherte) personenbezogene Daten oder deren Verwendung in einer Weise, die ein erhebliches Risiko für Identitätsdiebstahl oder Betrug darstellt, dass Angestellte, Auftragnehmer, Berater, Zeitarbeiter und andere Arbeitnehmer, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des für die Datenverarbeitung Verantwortlichen verarbeiten.
2. Umsetzung eines Programms zur Sensibilisierung und Schulung für Sicherheitsfragen	Ermittlung für alle funktionalen Rollen (vorrangig für diejenigen, die für das Unternehmen, seine Sicherheit und den Schutz personenbezogener Daten von entscheidender Bedeutung sind) der spezifischen Kenntnisse, Fähigkeiten und Fertigkeiten, die zur Unterstützung des Schutzes und der Verteidigung personenbezogener Daten erforderlich sind; Entwicklung eines integrierten Plans zur Bewertung, Ermittlung von Lücken und Behebung dieser Lücken durch Richtlinien, Organisationsplanung, Schulungen und Sensibilisierungsprogramme und deren Ausführung.
3. Sicherheit der Anwendungssoftware	Verwaltung des Sicherheitslebenszyklus aller intern entwickelten und erworbenen Software, um Sicherheitslücken zu verhindern, zu erkennen und zu beheben.
4. Reaktion auf Vorfälle und Management	Schutz der Informationen der Organisation, einschließlich personenbezogener Daten, sowie ihren Ruf, indem eine Infrastruktur für die Reaktion auf einen Vorfall entwickelt und implementiert wird (z. B. Pläne, definierte Rollen, Schulungen, Kommunikation, Überwachung durch das Management, Rücklagen und Versicherungen), um einen Angriff schnell zu entdecken und dann den Schaden wirksam einzudämmen, die Präsenz des Angreifers zu beseitigen und die Integrität des Netzwerks und der Systeme der Organisation wiederherzustellen.

5. Sicherheits- und Datenschutzbeurteilungen, Penetrationstests und Red-Team-Übungen	Testen der Gesamtstärke der Verteidigung der Organisation (Technologie, Prozesse und Mitarbeiter), indem die Ziele und Handlungen eines Angreifers simuliert, und bewertet und Kontrollen, Richtlinien und Verfahren zum Schutz der Privatsphäre und der personenbezogenen Daten der Organisation validiert werden.
6. Physische Sicherheit und Zugangskontrolle	Forderung, dass alle Einrichtungen das höchste Datenschutzniveau einhalten, das unter den für die Einrichtung und die darin enthaltenen, verarbeiteten oder übermittelten Daten relevanten Umständen möglich und angemessen ist.