ANHANG ZUR DATENVERARBEITUNG

Dieser Anhang zur Datenverarbeitung (einschließlich seiner Anlagen**) ("Anhang**") ist Teil und unterliegt den Bedingungen der Bestellung (einschließlich der für diese Bestellung geltenden Bedingungen) (die "**Vereinbarung**") zwischen dem Anbieter und dem Kunden, der die Vereinbarung abgeschlossen hat ("**Kunde**"), handelnd in seinem eigenen Namen und für jedes verbundene Unternehmen, und gilt hiermit durch Bezugnahme.

Dieser Anhang ersetzt vollumfänglich alle bestehenden Vereinbarungen, Nachträge, Anhänge, Zusatzvereinbarungen oder andere Dokumente, die die Verarbeitung und den Schutz der Personenbezogenen Daten des Kunden in Bezug auf die Dienste regeln.

Definierte Begriffe, die in diesem Anhang verwendet, aber nicht anderweitig definiert sind, haben die in der Vereinbarung angegebenen Bedeutungen . Sofern im weiteren Verlauf dieses Anhangs nicht geändert, bleiben die Bedingungen der Vereinbarung in vollem Umfang in Kraft und wirksam.

Dieser Anhang spiegelt die Verpflichtung der Parteien zur Einhaltung der Datenschutzgesetze in Bezug auf die Verarbeitung Personenbezogener Kundendaten im Zusammenhang mit den Dienstleistungen in der Vereinbarung wider. Wenn und soweit Regelungen in diesem Anhang im Widerspruch zur Vereinbarung stehen, hat dieser Anhang Vorrang.

Dieser Anhang wird mit dem Datum des Inkrafttretens der Vereinbarung oder an dem Tag, an dem die Parteien diesen Anhang unterzeichnen, rechtsverbindlich, wenn der Anhang nach dem Datum des Inkrafttretens der Vereinbarung abgeschlossen wurde.

1. Definitionen.

Für die Zwecke dieses Anhanges gelten die folgenden Begriffe und die im Hauptteil dieses Anhanges definierten Begriffe.

a) "**Personenbezogene Daten des Kunden**" bezeichnet personenbezogene Daten, die sich im Besitz oder unter der Kontrolle des Kunden befinden und die vom oder im Namen des Kunden dem Anbieter in Verbindung mit den Diensten zur Verfügung gestellt werden.

b) "**Vertraglicher Auftragsverarbeiter**" bezeichnet den Anbieter oder einen Unterauftragsverarbeiter.

c) "**Verantwortlicher**" bezeichnet die Stelle, die über die Zwecke und Mittel der Verarbeitung Personenbezogener Kundendaten entscheidet.

d) "**Datenschutzgesetze"** bezeichnet alle Gesetze und Vorschriften, die für die Verarbeitung Personenbezogener Kundendaten im Zusammenhang mit der Erbringung der Dienstleistungen im Rahmen der Vereinbarung gelten. "Datenschutzgesetze" können unter anderem den California Consumer Privacy Act von 2018 ("**CCPA")** umfassen; die EU-Datenschutz-Grundverordnung 2016/679 ("**DSGVO")** und ihre jeweiligen nationalen Umsetzungsgesetze; das Schweizer Bundesgesetz über den Datenschutz; die UK Datenschutz-Grundverordnung ("**UK GDPR**"); und das britische Datenschutzgesetz 2018 (jeweils in der jeweils geänderten, angenommenen oder ersetzten Fassung);

e) "**Betroffene Person**" hat die in den Datenschutzgesetzen angegebene Bedeutung;

f) "**Personenbezogene Daten**" bezeichnet alle Informationen, die vom oder im Namen des Kunden zur Verwendung in den Diensten zur Verfügung gestellt wurden und sich auf eine identifizierte oder identifizierbare Person beziehen.

g) "**Verarbeiten**" oder "**Verarbeitung**" bezeichnet jeden Vorgang oder jede Reihe von Verarbeitungsvorgängen, die mit Personenbezogenen Daten des Kunden oder Datensätzen personenbezogener Kundendaten durchgeführt werden, unabhängig davon, ob sie automatisiert sind oder nicht, wie das Erheben, das Aufzeichnen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Abrufen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder anderweitige Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

h) "**Auftragsverarbeiter**" bezeichnet das Unternehmen, das Personenbezogene Kundendaten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

i) "**Sicherheitsvorfall(e)"** bezeichnet die versehentliche oder unrechtmäßige Zerstörung, den Verlust, die Veränderung, die unbefugte Offenlegung oder den unbefugten Zugriff auf Personenbezogene Kundendaten. Ein Sicherheitsvorfall umfasst keine erfolglosen Versuche oder Aktivitäten, die die Sicherheit personenbezogener Kundendaten nicht gefährden, einschließlich erfolgloser Anmeldeversuche, Pings, Port-Scans, Denial-of-Service-Angriffe und andere Netzwerkangriffe auf Firewalls oder Netzwerksysteme.

j) "**Dienste**" bezeichnet die Dienstleistungen, die der Anbieter im Rahmen der Vereinbarung erbringt.

k) "**Standardvertragsklauseln**" (hierin durch Bezugnahme aufgenommen) bezieht sich auf:

die "Standardvertragsklauseln für 2021", definiert als die Klauseln, die gemäß dem Durchführungsbeschluss (EU) 2021/914 der EU-Kommission vom Juni 2021 über

Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates erlassen wurden und unter http://data.europa.eu/eli/dec_impl/2021/914/oj (in der jeweils gültigen und jeweils aktualisierten Fassung) verfügbar sind.

l) "**Unterauftragsverarbeiter**" bezeichnet die autorisierten Dienstleister des Anbieters und Drittanbieter, die Personenbezogene Kundendaten verarbeiten.

m) "**Aufsichtsbehörde**" bezeichnet eine unabhängige öffentliche Behörde, die gemäß den Datenschutzgesetzen eingerichtet wurde, um die Einhaltung der Datenschutzgesetze zu überwachen.

2. Datennutzung und -verarbeitung.

a) Rollen der Parteien. Die Parteien erkennen an und stimmen zu, dass (i) wenn der Kunde ein Verantwortlicher ist, der Anbieter der Verarbeiter ist und (ii) wenn der Kunde ein Auftragsverarbeiter ist, der Anbieter ein Unterauftragsverarbeiter des Kunden ist. Wenn der CCPA für die Verarbeitung personenbezogener Kundendaten durch den Anbieter gilt, erkennen die Parteien außerdem an und stimmen zu, dass der Kunde ein Unternehmen ist, wie dieser Begriff im CCPA und seinen Durchführungsbestimmungen definiert ist, und dass der Anbieter der Dienstleister des Kunden ist, wie dieser Begriff im CCPA und seinen Durchführungsbestimmungen definiert ist.

b) Dokumentierte Anweisungen. Der Kunde weist den Anbieter an, Personenbezogene Daten des Kunden zu verarbeiten, damit er die Dienste erbringen und der Kunde die Dienste in Übereinstimmung mit der Vereinbarung, diesem Anhang, einer anwendbaren Leistungsbeschreibung und allen von den Parteien schriftlich vereinbarten Anweisungen erhalten kann. Gegenstand der Verarbeitung ist die Nutzung der Dienste durch den Kunden und seiner Endnutzer. Die Kategorien der betroffenen Person sind Nutzer der Dienste und Personen in Räumlichkeiten, in denen die Dienste genutzt werden, und können daher Mitarbeiter und Besucher des Kunden umfassen. Der Anbieter stellt sicher, dass jede Übermittlung Personenbezogener Kundendaten aus dem EWR und/oder dem Vereinigten Königreich in Übereinstimmung mit den Datenschutzgesetzen unter Verwendung eines rechtmäßigen Übertragungsmechanismus erfolgt. Der Kunde stellt sicher, dass die Verarbeitung Personenbezogener Kundendaten durch den Anbieter in Übereinstimmung mit den Anweisungen des Kunden nicht dazu führt, dass der Anbieter gegen geltende Gesetze oder Vorschriften, einschließlich der geltenden Datenschutzgesetze, verstößt. Der Kunde trägt die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der Personenbezogenen Daten des Kunden, für alle erforderlichen Einwilligungen, Prozesse und Mitteilungen, die erforderlich sind, um die rechtmäßige Übermittlung Personenbezogener Kundendaten an den Anbieter im Rahmen der Vereinbarung und dieses Anhanges zu ermöglichen, sowie für die Mittel, mit denen der Kunde die Personenbezogenen Daten erhalten hat. Die Dauer, für die der Anbieter personenbezogene Kundendaten verarbeitet, ist die Dauer der Vereinbarung zuzüglich etwaiger anwendbarer Aufbewahrungsfristen in diesem Anhang. Der Anbieter wird, sofern dies nicht gesetzlich verboten ist, den Kunden schriftlich informieren, wenn er Grund zu der Annahme hat, dass ein Konflikt zwischen den Anweisungen des Kunden und den geltenden Datenschutzgesetzen besteht.

c) Berechtigung zur Verwendung von Unterauftragsverarbeitern. Soweit dies zur Erfüllung der vertraglichen Verpflichtungen des Anbieters im Rahmen der Vereinbarung erforderlich ist, ermächtigt der Kunde den Anbieter hiermit, Unterauftragsverarbeiter zu beauftragen. Die aktuelle Liste der Unterauftragsverarbeiter des Anbieters für die anwendbaren Dienste finden Sie unter www.eptura.com/subprocessors (die "**Unterauftragsverarbeiterliste**"). Der Kunde stimmt der Ernennung der in der Unterauftragsverarbeiterliste aufgeführten Unterauftragsverarbeiter zu. Der Anbieter stimmt zu, dass er keine Personenbezogenen Daten an Unternehmen übermittelt, die nicht in der Liste der Unterauftragsverarbeiter aufgeführt sind.

d) Lieferanten- und Unterauftragsverarbeiter-Compliance. Der Anbieter verpflichtet sich, (i) eine schriftliche Vereinbarung mit Unterauftragsverarbeitern über die Verarbeitung Personenbezogener Kundendaten durch diese Unterauftragsverarbeiter zu treffen, die diesen Unterauftragsverarbeitern Datenschutzanforderungen für Personenbezogene Kundendaten auferlegt, die mit diesem Anhang übereinstimmen; und (ii) bleiben für die Handlungen und Unterlassungen seiner Unterauftragsverarbeiter in demselben Umfang verantwortlich, in dem der Anbieter haften würde, wenn er Dienstleistungen jedes Unterauftragsverarbeiters direkt unter den Bedingungen dieses Anhanges erbringen würde.

e) Widerspruchsrecht gegenüber Unterauftragsverarbeitern. Der Anbieter wird den Kunden mindestens 15 Tage vor der Ernennung eines neuen Unterauftragsverarbeiters über seine Absicht informieren, neue Unterauftragsverarbeiter zu beauftragen, indem

er die Liste der Unterauftragsverarbeiter aktualisiert, und der Anbieter bietet dem Kunden die Möglichkeit, sich für Benachrichtigungen über solche Änderungen anzumelden. Der Kunde kann dem Einsatz des neuen Unterauftragsverarbeiters durch den Anbieter widersprechen, indem er den Anbieter umgehend schriftlich 15 Tage nach Erhalt der Mitteilung des Anbieters benachrichtigt. Die Benachrichtigung des Kunden erfolgt an die E-Mail-Adresse(n), die in der Bestellung für die Dienste angegeben sind, oder anderweitig an den Anbieter beim Kauf von Dienstleistungen. Wenn der Kunde dem Einsatz des neuen Unterauftragsverarbeiters gemäß diesem Abschnitt nicht widerspricht, gilt der neue Unterauftragsverarbeiter für die Zwecke dieses Anhanges als genehmigt. Wenn der Kunde dem Einsatz oder Ersetzung eines Unterauftragsverarbeiters durch den Anbieter aus berechtigten datenschutzrechtlichen Gründen widerspricht, wird er den Anbieter vor der Ernennung oder Ersetzung des Unterauftragsverarbeiters schriftlich darüber informieren. In diesem Fall wird der Anbieter angemessene Maßnahmen treffen, um die Dienste dem Kunden in Übereinstimmung mit der Vereinbarung zur Verfügung zu stellen, ohne den Unterauftragsverarbeiter zu verwenden. Wenn der Anbieter den Einsatz des Unterauftragsverarbeiters vernünftigerweise verlangt und nicht in der Lage ist, den Kunden innerhalb von dreißig (30) Tagen nach dem Widerspruch des Kunden von der Eignung des Unterauftragsverarbeiters zu überzeugen, kann der Kunde sich dafür entscheiden, den Teil der Dienstleistungen oder Bestellungen zu kündigen, der vom Anbieter nicht ohne den Einsatz des beanstandeten Unterauftragsverarbeiters bereitgestellt werden kann.

f) Vertraulichkeit. Der Anbieter stellt sicher, dass sein Personal und das seiner verbundenen Unternehmen, die an der Verarbeitung Personenbezogener Kundendaten beteiligt sind, über die Vertraulichkeit der Personenbezogenen Daten des Kunden informiert werden und schriftliche Vertraulichkeitsvereinbarungen getroffen haben.

g) Datenschutz-Folgenabschätzung und vorherige Konsultation. Der Anbieter leistet dem Kunden angemessene Unterstützung bei allen Datenschutz-Folgenabschätzungen (wenn eine solche angemessene Zusammenarbeit des Anbieters erfordert, erhebliche Ressourcen für diese Bemühungen bereitzustellen, auf Kostern des Kunden) und vorherigen Konsultationen mit einer Aufsichtsbehörde oder anderen zuständigen Datenschutzbehörden, soweit dies nach den geltenden Datenschutzgesetzen erforderlich ist, jeweils ausschließlich in Bezug auf die Verarbeitung Personenbezogener Kundendaten und unter Berücksichtigung der Art der Verarbeitung und der dem Anbieter zur Verfügung stehenden Informationen.

3. Betroffene Personen.

Der Anbieter benachrichtigt, soweit dies nach den Datenschutzgesetzen zulässig ist, den Kunden, wenn der Anbieter eine Anfrage von einer betroffenen Person erhält, die Personenbezogene Daten des Kunden identifiziert oder den Kunden anderweitig identifiziert, einschließlich der Fälle, in denen die betroffene Person versucht, eines ihrer Rechte gemäß den geltenden Datenschutzgesetzen auszuüben (zusammen "**Anfrage der betroffenen Person**"). Wenn der Anbieter eine Anfrage einer betroffenen Person in Bezug auf Personenbezogene Daten des Kunden erhält, wird der Anbieter der betroffenen Person empfehlen, ihre Anfrage an den Kunden zu senden, und der Kunde ist dafür verantwortlich, auf diese Anfrage zu antworten, einschließlich, falls erforderlich, durch Nutzung der Funktionalität der Dienste. In dem Umfang, in dem der Kunde nicht in der Lage ist, auf die relevanten Personenbezogenen Daten des Kunden innerhalb der Dienste unter Verwendung solcher Steuerung oder auf andere Weise zuzugreifen, wird der Anbieter (auf schriftliche Anfrage des Kunden und unter Berücksichtigung der Art der Verarbeitung) auf wirtschaftlich angemessene Art kooperieren, um den Kunden bei der Beantwortung von Anfragen betroffener Personen zu unterstützen.

4. Datenübertragungen.

Wenn personenbezogene Daten des Kunden, die aus dem Europäischen Wirtschaftsraum (EEA), der Schweiz und/oder dem Vereinigten Königreich stamen, vom Kunden an den Anbieter in ein Land übermittelt werden, das nach den geltenden Datenschutzgesetzen kein angemessenes Schutzniveau bietet, vereinbaren die Parteien, dass die Übermittlung den Standardvertragsklauseln unterliegt, oder SCCs. Wenn die SCCs anwendbar sind und der Kunde Verantwortlicher für Personenbezogene Kundendaten und der Anbieter Verarbeiter Personenbezogener Kundendaten ist, muss jede Partei ihren Verpflichtungen gemäß Modul Zwei der SCCs nachkommen. Wenn die SCCs anwendbar sind und der Kunde Verarbeiter Personenbezogener Kundendaten ist und der Anbieter ebenfalls Verarbeiter personenbezogener Kundendaten ist, muss jede Partei ihren Verpflichtungen gemäß Modul Drei der SCCs nachkommen. Die Parteien sind sich einig, dass: (i) die optionale Andockklausel in Klausel 7 keine Anwendung findet; (ii) die in Klausel 8.5 und Klausel 16(d) der SCCs erforderliche Löschungsbescheinigung wird auf schriftliche Anfrage des Kunden zur Verfügung gestellt; (iii) die Maßnahmen, die der Anbieter gemäß Klausel 8.6(c) der SCCs ergreifen muss, gelten nur für die betroffenen Systeme des Anbieters; iv) das in Klausel

8.9 der SCCs beschriebene Audit wird gemäß Abschnitt 7 (Audits) dieses Anhangs durchgeführt; (v) In Klausel 9 ist die Mindestfrist für die vorherige Benachrichtigung über Änderungen des Unterauftragsverarbeiters wie in Abschnitt 2 (e) dieses Anhanges festgelegt (vi) sofern dies nach den Datenschutzgesetzen zulässig ist, kann der Anbieter bestehende Unterauftragsverarbeiter unter Verwendung des Beschlusses C(2010) 593 der Europäischen Kommission beauftragen, und ein solcher Einsatz von Unterauftragsverarbeitern gilt als mit Klausel 9 der SCCs übereinstimmend; vii) in Klausel 11 gilt die optionale Regelung nicht; (viii) das in Klausel 14(f) und Klausel 16(c) der SCCs vorgesehene Kündigungsrecht ist auf die Kündigung der SCCs beschränkt, in welchem Fall die entsprechende Verarbeitung der von einer solchen Kündigung betroffenen Personenbezogenen Kundendaten eingestellt wird, sofern die Parteien nichts anderes vereinbart haben; (ix) die gemäß Klausel 15.1(c) erforderlichen Informationen werden auf schriftliche Anfrage des Kunden zur Verfügung gestellt; (x) In Klausel 17 unterliegen die Vertragsparteien den Gesetzen der Republik Irland; (xi) In Klausel 18 (b) werden Streitigkeiten vor den Gerichten der Republik Irland beigelegt; xii) Anlage A zu diesem Anhang enthält die in Anhang I der SCC geforderten Angaben; xiii) Anlage B zu diesem Anhang enthält die in Anhang II der SCC geforderten Angaben; (xiv) soweit Personenbezogene Daten den britischen Datenschutzgesetzen unterliegen, werden die SCCs durch Anlage C ergänzt; und (xv) ungeachtet gegenteiliger Bestimmungen erstattet der Kunde dem Anbieter alle Kosten und Aufwendungen, die dem Anbieter im Zusammenhang mit der Erfüllung der Verpflichtungen des Anbieters gemäß Klausel 15.1(b) und Klausel 15.2 der SCCs entstehen. Die Unterzeichnung dieses Anhangs durch jede Vertragspartei gilt als Unterschrift unter die SCC, soweit die SCCs im Rahmen dieser Vereinbarung Anwendung finden.

5. Informationssicherheitsprogramm.

Der Anbieter hat angemessene administrative, technische und organisatorische Maßnahmen implementiert und wird diese aufrechterhalten, um die Personenbezogenen Daten des Kunden vor einem Sicherheitsvorfall zu schützen, unter Berücksichtigung des Stands der technologischen Entwicklung und der Kosten für die Umsetzung solcher Maßnahmen sowie der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung und der Wahrscheinlichkeit und Schwere einer Schädigung der Interessen der betroffenen Personen, von der erwartet werden kann, dass sie sich aus einem solchen Sicherheitsvorfall ergibt (einschließlich, gegebenenfalls die in Art. 32 Abs. 1 DSGVO genannten Maßnahmen). Alle Fragen zu den Sicherheitsmaßnahmen des Anbieters können an das Sicherheits- und Datenschutzteam des Anbieters unter privacy@eptura.com.

6. Sicherheitsvorfälle.

a) Der Anbieter wird den Kunden unverzüglich schriftlich benachrichtigen, wenn er von einem Sicherheitsvorfall Kenntnis erlangt. Eine solche Benachrichtigung stellt keine Anerkennung von Verschulden oder Verantwortung dar. Die Benachrichtigung soll den Kunden so weit wie möglich in die Lage versetzen, die betroffenen Personen über den Sicherheitsvorfall gemäß den Datenschutzgesetzen zu informieren und, soweit dem Anbieter bekannt, (i) die Art des Sicherheitsvorfalls zu beschreiben, einschließlich, soweit möglich, der Kategorien und der ungefähren Anzahl der betroffenen Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen personenbezogenen Datensätze; und (ii) die Maßnahmen zu beschreiben, die der Anbieter ergriffen hat oder vorschlagen hat zu ergreifen, um auf den Sicherheitsvorfall zu reagieren, einschließlich, falls zutreffend, Maßnahmen zur Schadensbegrenzung.

b) Im Falle eines Sicherheitsvorfalls und vor der Abgabe einer erforderlichen öffentlichen Erklärung oder erforderlichen Benachrichtigung verpflichtet sich der Anbieter, die Zustimmung des Kunden einzuholen, bevor eine Benachrichtigung der betroffenen Personen oder der zuständigen Aufsichtsbehörden über den Sicherheitsvorfall erfolgt. Ungeachtet des vorstehenden Satzes ist der Kunde nicht verpflichtet, seine Verpflichtungen aus den Datenschutzgesetzen zu beeinträchtigen.

c) Die in Abschnitt 7(a) und 7(b) beschriebenen Verpflichtungen gelten nicht für den Fall, dass eine Verletzung des Schutzes personenbezogener Daten auf Handlungen oder Unterlassungen des Kunden zurückzuführen ist.

7. Audits.

a) Der Anbieter verwendet unabhängige, externe Gutachter, um die Angemessenheit seiner Verarbeitung Personenbezogener Kundendaten zu überprüfen. Diese Prüfung wird: i) mindestens einmal jährlich durchgeführt werden; (ii) von einem qualifizierten Fachmann nach Auswahl und auf Kosten des Anbieters durchgeführt werden; und (iii) die Einhaltung der geltenden Datensicherheitsstandards für die Verarbeitung Personenbezogener Daten durch den Anbieter nachzuweisen ("**Bericht**"). Auf schriftliche Anfrage des Kunden stellt der Anbieter dem Kunden eine Zusammenfassung seines Berichts zur Verfügung, damit der Kunde die Einhaltung der Sicherheitsverpflichtungen in diesem Anhang durch den Anbieter angemessen überprüfen kann. Jede Bereitstellung eines solchen Berichts unterliegt angemessenen Vertraulichkeitsbestimmungen.

b) Wenn der Anbieter nicht in der Lage ist, aktuelle Berichte rechtzeitig zur Verfügung zu stellen, kann der Kunde auf schriftliche Anfrage (auf eigene Kosten) ein Audit zur Gewährleistung der Informationssicherheit durchführen. Ein solches Audit unterliegt den folgenden Bedingungen: (i) Der Kunde muss seine Absicht zur Prüfung mindestens dreißig (30) Tage im Voraus ankündigen; ii) spätestens zwei (2) Wochen vor der Prüfungstätigkeit wird ein einvernehmlich vereinbarter Umfang und Zeitplan festgelegt; (iii) jeder unabhängige Gutachter ist verpflichtet, eine Geheimhaltungsvereinbarung zu unterzeichnen, wie es der Anbieter vor der Prüfung vernünftigerweise verlangt; (iv) das Audit muss während der normalen Geschäftszeiten des Anbieters durchgeführt werden; (v) das Audit muss an einem (1) Werktag abgeschlossen sein; (vi) das Recht zur Prüfung umfasst das Recht, Aufzeichnungen zu überprüfen, aber nicht zu kopieren oder anderweitig zu entfernen, mit Ausnahme derjenigen, die sich speziell und ausschließlich auf den Kunden beziehen; und (vii) das Audit darf keine Penetrationstests, Schwachstellenuntersuchungen oder andere Sicherheitstests umfassen. Der Kunde kann ein solches Audit nur einmal pro zwölf (12) Monaten durchführen; vorausgesetzt jedoch, dass der Kunde im Falle (i) eines Sicherheitsvorfalls mit Personenbezogenen Daten des Kunden zusätzliche Audits durchführen kann; oder (ii) eine Anfrage einer Aufsichtsbehörde oder einer ähnlichen Aufsichtsbehörde, die für die Durchsetzung der Datenschutzgesetze in einem Land oder Gebiet verantwortlich ist. Anbieter und Kunde werden sich treffen und alle Auditergebnisse mit allen vom Anbieter nach eigenem Ermessen festzulegenden Abhilfemaßnahmen und Zeitplänen besprechen.

8. Löschung von Daten.

Der Anbieter stellt dem Kunden Personenbezogene Daten auf schriftliche Anfrage innerhalb von dreißig (30) Tagen nach dem Datum der Kündigung / des Ablaufs des Vertrags für den Export zur Verfügung. Danach löscht der Anbieter innerhalb von sechzig (60) Tagen alle Personenbezogenen Daten des Kunden (mit Ausnahme von Sicherungs- oder Archivkopien, die gemäß dem Datenaufbewahrungsplan des Anbieters gelöscht werden), es sei denn, der Anbieter ist gemäß den Datenschutzgesetzen verpflichtet, Kopien aufzubewahren, in welchem Fall der Anbieter diese Personenbezogenen Daten des Kunden vor einer weiteren Verarbeitung schützt. Wenn der Kunde eine Kopie der personenbezogenen Daten des Kunden anfordert, wird der Anbieter dieser Anfrage innerhalb von 45 Tagen nach dem Datum der Anfrage nachkommen.

9. Haftung.

Dieser Anhang beschränkt nicht die Rechte und Pflichten der Parteien im Rahmen der Vereinbarung, die weiterhin Gültigkeit und Wirkung haben, einschließlich der darin enthaltenen Haftungsbeschränkungen und -ausschlüsse, die für diesen Anhang gelten, als ob sie hierin geregelt wären. Im Falle eines Widerspruchs zwischen den Bedingungen dieses Anhanges und den Bedingungen der Vereinbarung haben die Bedingungen dieses Anhanges Vorrang, soweit deren Gegenstand die Verarbeitung Personenbezogener Kundendaten betrifft.

10. Sonstiges.

a) Dieser Anhang unterliegt dem Recht und der Gerichtsbarkeit des Landes oder Gebiets, dem die Vereinbarung unterliegt, und ist in Übereinstimmung mit diesem auszulegen, sofern in diesem Anhang nichts anderes angegeben oder durch Datenschutzgesetze vorgeschrieben ist.

b) Der Anbieter kann die Bedingungen dieses Anhanges aktualisieren, wenn die Änderungen (a) erforderlich sind, um den Datenschutzgesetzen, den geltenden Vorschriften, einem Gerichtsbeschluss oder einer von einer Aufsichtsbehörde oder Behörde herausgegebenen Leitlinien zu entsprechen; oder (b) keine wesentlichen nachteiligen Auswirkungen auf die Rechte des Kunden aus dem Anhang haben. Der Anbieter wird dreißig (30) Tage im Voraus Bescheid geben, bevor er wesentliche Änderungen an den Bestimmungen dieses Anhanges vornimmt. Wenn sich die Aktualisierungen wesentlich auf die Nutzung der Dienste durch den Kunden auswirken, hat der Kunde das Recht, die betroffenen Dienste innerhalb von dreißig (30) Tagen nach Erhalt einer schriftlichen Mitteilung über die Änderungen zu kündigen.

Anlage A

ANHANG I

Ein. **LISTE DER PARTEIEN**

MODUL ZWEI: Übertragung Verantwortlicher an Auftragsverarbeiter

MODUL DREI: Übertragung Auftragsverarbeiter an Auftragsverarbeiter

Datenexporteur(e):

Name:	Der Kunde, der in der Vereinbarung und/oder im Bestellformular(en) oder im Statement of Work angegeben ist und die verbundenen Unternehmen des Kunden
Adresse:	Adresse des Kunden, wie in der Vereinbarung und/oder im Bestellformular(en) oder im Statement of Work angegeben
Kontaktperson:	E-Mail-Adresse des Kunden, wie in der Vereinbarung und/oder im Bestellformular(en) oder im Statement of Work angegeben
Aktivitäten, die für übertragene Daten relevant sind:	Kauf von Dienstleistungen vom Anbieter
Rolle:	Verantwortlicher (Modul Zwei); Auftragsverarbeiter (Modul Drei)

Datenimporteur(e):

Name:	Der in der Vereinbarung und/oder Bestellung(en) oder im Statement of Work genannte Anbieter und alle verbundenen Unternehmen des Anbieters
Adresse:	Adresse des Anbieters, wie in der Vereinbarung und/oder Bestellung(en) oder im Statement of Work angegeben
Kontaktperson:	privacy@eptura.com
Aktivitäten, die für übertragene Daten relevant sind:	Der Anbieter ist ein Anbieter von Enterprise-Cloud-Workspace- und Asset-Management-Lösungen, der personenbezogene Daten auf Anweisung des Datenexporteurs gemäß den Bedingungen der Vereinbarung und des Anhangs verarbeitet.
Rolle:	Auftragsverarbeiter

B. BESCHREIBUNG DER ÜBERTRAGUNG

MODUL ZWEI: Übertragung Verantwortlicher an Auftragsverarbeiter

MODUL DREI: Übertragung Auftragsverarbeiter an Auftragsverarbeiter

Gegenstand der Verarbeitung:	Gegenstand der Verarbeitung personenbezogener Daten durch den Anbieter ist die Erbringung von Dienstleistungen für den Datenexporteur gemäß dem Vertrag.
Art und Zweck der Verarbeitung:	Die Verarbeitung steht im Zusammenhang mit der Bereitstellung von SaaS-Lösungen für den Kunden, wie in der Vereinbarung näher beschrieben, und der Anbieter und seine Unterauftragsverarbeiter führen die Verarbeitung personenbezogener Daten durch, die erforderlich sind, um diese Dienste gemäß den Anweisungen des Datenexporteurs bereitzustellen, einschließlich, aber nicht beschränkt auf die Übertragung, Speicherung und andere Verarbeitung personenbezogener Daten, die an die Dienste übermittelt werden.
Dauer der Verarbeitung:	Der Anbieter verarbeitet personenbezogene Daten im Auftrag des Datenexporteurs, bis der Datenexporteur die Nutzung der Dienste einstellt.

Kategorien von betroffenen Personen:	Betroffene Personen, deren personenbezogene Kundendaten gemäß der Vereinbarung verarbeitet werden.
Kategorien personenbezogener Daten:	Personenbezogene Kundendaten, die gemäß der Vereinbarung verarbeitet werden.
Besondere Kategorien personenbezogener Daten:	Besondere Kategorien personenbezogener Daten sind in den Diensten nicht zulässig.
Gegenstand, Art und Dauer der Verarbeitung durch den Unterauftragsverarbeiter:	Alle Übertragungen an Unterauftragsverarbeiter erfolgen zur Erbringung der Dienstleistungen gemäß der Vereinbarung.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

MODUL ZWEI: Übertragung Verantwortlicher an Auftragsverarbeiter

MODUL DREI: Übertragung Auftragsverarbeiter an Auftragsverarbeiter

Die gem Klausel 13 zuständige Aufsichtsbehörde der SCCs. Wenn keine Aufsichtsbehörde gem. Klausel 13 zuständig ist, dann soll die irische Datenschutzbehörde (Irish Data Protection Commission (DPC)) zuständig sein, und wenn dies nicht möglich ist, dann, wie von den Parteien vereinbart, im Einklang mit den in Klausel 13 festgelegten Bedingungen.

Anlage B

ANHANG II

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN EINSCHLIESSLICH TECHNISCHER UND ORGANISATORISCHER MAßNAHMEN ZUR GEWÄHRLEISTUNG DER DATENSICHERHEIT

MODUL ZWEI: Übertragung Verantwortlicher an Auftragsverarbeiter

MODUL DREI: Übertragung Auftragsverarbeiter an Auftragsverarbeiter

Beschreibung der technischen und organisatorischen Maßnahmen, die von dem/den Datenimporteur(en) (einschließlich aller einschlägigen Zertifizierungen) ergriffen wurden, um ein angemessenes Sicherheitsniveau zu gewährleisten, wobei Art, Umfang, Kontext und Zweck der Verarbeitung sowie die Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen sind.

Bei der Festlegung der im Rahmen des Vertrags erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen ("Sicherheitsstandards") berücksichtigt der Anbieter den Stand der Technik, die Implementierungskosten und die Art, den Umfang, den Kontext und die Zwecke der Verarbeitung sowie das unterschiedlich wahrscheinliche und schwere Risiko für die Rechte und Freiheiten natürlicher Personen. Der Anbieter betreibt Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsstandards zur Gewährleistung der Sicherheit der Verarbeitung Personenbezogener Kundendaten.

Der Anbieter stimmt in Bezug auf Personenbezogene Daten des Kunden Folgendem zu:

1. Schutzmaßnahmen – Programm. Der Anbieter wird angemessene Sicherheitsvorkehrungen treffen, die mit den Industriestandards zum Schutz personenbezogener Kundendaten übereinstimmen und deren Vertraulichkeit, Integrität und Verfügbarkeit wahren. Der Anbieter stellt sicher, dass alle diese Sicherheitsvorkehrungen den geltenden Gesetzen und der Vereinbarung entsprechen, einschließlich des Ahangs zur Datenverarbeitung (DPA), falls zutreffend.

2. Schutzmaßnahmen – Spezifisch. Zu den Sicherheitsstandards des Anbieters gehören mindestens: (a) sichere Standorte, Rechenzentren, Papierakten, Server, Backup-Systeme und Computerausrüstung, einschließlich, aber nicht beschränkt auf alle mobilen Geräte und andere Gerät, die Informationen speichern können; b) Netzwerk-, Geräteanwendungs-, Datenbank- und Plattformsicherheit; c) sichere Übermittlung, Lagerung und Entsorgung; d) Authentifizierung und Zugangskontrollen innerhalb von Anwendungen, Betriebssystemen und Geräten; e) Protokollierung des Zugriffs auf Material und Aufbewahrung solcher Zugangskontrollprotokolle für einen Zeitraum, der ausreicht, um eine Untersuchung zu ermöglichen; (f) Verschlüsselung personenbezogener Kundendaten im Ruhezustand (Dta at Rest), auch wenn sie auf einem elektronischen Notebook, einer tragbaren Festplatte oder einem austauschbaren elektronischen Datenträger, der Informationen speichern kann, gespeichert sind; (g) Verschlüsselung Personenbezogener Kundendaten bei der Übertragung über öffentliche oder drahtlose Netzwerke; (h) Trennung der Personenbezogenen Daten des Kunden von den Informationen der anderen Kunden des Anbieters; (i) Sicherheit und Integrität des Personals, einschließlich, aber nicht beschränkt auf Hintergrundüberprüfungen im Einklang mit geltendem Recht; (j) jährliche externe und interne Tests und Schwachstellenscans und die unverzügliche Umsetzung eines Korrekturmaßnahmenplans (einschließlich des Zeitplans) auf alleinige Kosten des Anbieters, um wesentliche Probleme zu beheben, die durch Tests identifiziert wurden; und (k) den Zugriff auf Personenbezogene Kundendaten einzuschränken und dem autorisierten Personal des Anbieters Schulungen zu Datenschutz und Informationssicherheit anzubieten. "Autorisiertes Personal" bezeichnet das Personal des Anbieters, das Kundendaten kennen oder anderweitig darauf zugreifen muss, damit der Anbieter seine Verpflichtungen aus der Vereinbarung erfüllen kann, und das schriftlich an Vertraulichkeitsverpflichtungen gebunden ist, die ausreichen, um die Personenbezogenen Daten des Kunden in Übereinstimmung mit den Bedingungen der Vereinbarung, einschließlich des Anhangs zum Datenschutz (DPA), falls zutreffend, zu schützen.

3. Malware. Die gelieferte Software des Anbieters enthält keine Viren, Malware, Ransomware, Keylogger, Logikbomben, Trojaner, Würmer oder andere Softwareroutinen, die darauf abzielen, Software, Hardware oder Daten, die sich im Besitz des Kunden befinden oder vom Kunden kontrolliert werden, zu deaktivieren, zu löschen oder anderweitig zu beschädigen.

4. Verbotene Hardware oder Ausrüstung. Der Anbieter darf keine Hardware oder Ausrüstung verwenden, die nicht Abschnitt 889 (a) (1) (B) des National Defense Authorization Act für das Geschäftsjahr 2019 entspricht. Der Anbieter erklärt auf Anfrage die Einhaltung dieser Bestimmung. Wenn der Anbieter diese Bestimmung nicht mehr einhalten kann, wird der Anbieter den Kunden unverzüglich benachrichtigen, indem er eine E-Mail an den hinterlegten Sicherheitskontakt sendet.

5. Disaster Recovery und Business Continuity. Der Anbieter unterhält und implementiert einen Business Continuity- und Disaster-Recovery-Plan ("BCDR-Plan"), der mindestens Folgendes umfasst: (a) Dokumentation der anwendbaren Geschäftsprozesse, Verfahren und Verantwortlichkeiten; b) Backup-Methodik; (c) Ermittlung von Notfallwiederherstellungsszenarien und Vereinbarungen zum Servicelevel für die Servicewiederherstellung; d) Verantwortlichkeiten der Unterauftragsverarbeiter im Katastrophenfall; e) eine Kommunikationsstrategie; und f) Verfahren für die Wiederherstellung des normalen Dienstes. Der BCDR-Plan wird jährlich überprüft. Der Anbieter stellt sicher, dass er in der Lage ist, den BCDR-Plan jederzeit in Übereinstimmung mit seinen Bedingungen umzusetzen. Der Anbieter testet den BCDR-Plan regelmäßig (und in jedem Fall nicht weniger als jährlich). Auf Anfrage übermittelt der Anbieter einen schriftlichen Bericht, in dem die Ergebnisse des letzten Tests zusammengefasst sind, und führt unverzüglich alle Maßnahmen oder Abhilfemaßnahmen durch, die die Parteien einvernehmlich als Ergebnis dieser Tests für erforderlich halten.

6. Sicherheitsvorfälle. Bei Entdeckung eines tatsächlichen oder vernünftigerweise vermuteten Verdachts durch den Anbieter auf (i) unbefugten Zugriff auf oder Offenlegung von Kundendaten; (ii) unbefugten Zugriff auf Anwendungen oder Systeme, die Eigentum des Anbieters sind, vom Anbieter verwaltet oder an Unterauftragnehmer vergeben werden ("Systeme des Anbieters"), auf denen personenbezogene Daten des Kunden verarbeitet werden (jeweils ein "Sicherheitsvorfall"), wird der Anbieter unverzüglich und ohne unangemessene Verzögerung:

(i) Maßnahmen zur Minderung und/oder Behebung des Sicherheitsvorfalls ergreifen, um personenbezogene Kundendaten vor weiteren Risiken oder Schäden zu schützen, und Einleitung einer Untersuchung;

(ii) Geeignete Kontrollen einführen, um alle elektronischen Beweismittel im Zusammenhang mit dem Sicherheitsvorfall in Übereinstimmung mit den Industriestandards aufzubewahren und aufzubewahren;

(iii) Dem Kunden die Art des Sicherheitsvorfalls melden (einschließlich, soweit möglich, der Kategorien der verletzten Daten und der Kategorien von Datenverlustmethoden sowie in dem Umfang, in dem es sich um Personenbezogene Daten des Kunden handelt, der Kategorien und der ungefähren Anzahl der betroffenen Personen und der ungefähren Anzahl der betroffenen personenbezogenen Kundendatensätze);

(iv) Den Namen und die Kontaktdaten der Kontaktstelle des Anbieters angeben, an der unverzüglich weitere Informationen eingeholt werden können, der wahrscheinlichen Folgen des Sicherheitsvorfalls, falls bekannt, und der Maßnahmen, die ergriffen wurden oder vorgeschlagen werden, um den Sicherheitsvorfall zu beheben, einschließlich (gegebenenfalls) Maßnahmen zur Minderung seiner möglichen nachteiligen Auswirkungen;

(v) Maßnahmen ergreifen, um zu verhindern, dass in Zukunft ähnliche Sicherheitsvorfälle auftreten. Der Anbieter ist im Zweifel nicht verpflichtet, Pings auf Firewalls, Port-Scans und Malware zu melden, die höchst unwahrscheinlich zu unbefugtem Zugriff, Verwendung, Offenlegung, Änderung oder Zerstörung von Informationen führen können, oder Interferenzen mit den Systemen des Anbieters werden nicht als meldepflichtiger Sicherheitsvorfall angesehen, den der Anbieter dem Kunden melden soll; und

(vi) Bei allen Untersuchungen, Streitigkeiten, Anfragen, Ansprüche, Rechtsstreitigkeiten oder behördlichen Maßnahmen, die sich aus Sicherheitsvorfällen ergeben, konsultieren und zusammenarbeiten.

7. Zertifizierungen und Sicherheitsbewertungen. Der Anbieter beauftragt unabhängige externe Sicherheitsbewertungsfirmen (Audits) mit der Durchführung von Zertifizierungsprüfungen und Sicherheitstests auf jährlicher Basis. Auf Verlangen des Kunden stellt der Anbieter dem Kunden Nachweise über aktuelle Zertifizierungen und Tests zur Verfügung, einschließlich Zertifikaten, Zusammenfassungen und anderen Aufzeichnungen, die nach dem alleinigem, aber angemessenem Ermessen des Anbieters als relevant erachtet werden (die "Bewertungsunterlagen"), um die Einhaltung der Vereinbarung und der Gesetze nachzuweisen.

8. Sicherheitsfragebögen. Nicht mehr als einmal pro Zeitraum von zwölf (12) Monaten und auf Anfrage beantwortet der Anbieter einen Cybersicherheitsfragebogen oder eine ähnliche Anfrage, der von angemessener Länge ist und nicht die Vorlage von zusätzlichen Belegen zu den aktuellen Bewertungsunterlagen erfordert.

Unterstützung bei Anfragen von betroffenen Personen. Der Kunde ist für die Kommunikation mit den betroffenen Personen gemäß Klausel 15.1(a) der SCCs verantwortlich.

Anlage C

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

TABLE 1: PARTIES

Start date	The date on which the Customer or its Affiliate identified in the Agreement and/or Order Form(s)/Statement(s) of Work enters into the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The Customer identified in the Agreement and/or Order Form(s)/Statement(s) of Work and all Affiliates of Customer Trading name (if different): Main address (if a company registered address): Customer's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work Official registration number (if any) (company number or similar identifier): The registered number of the Customer or Affiliate of the Customer identified in the Agreement and/or Order Form(s)/Statement(s) of Work	Full legal name: The Provider identified in the Agreement and/or Order Form(s)/Statement(s) of Work Trading name (if different): Main address (if a company registered address): Provider's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work Official registration number (if any) (company number or similar identifier): The registered number of the Provider identified in the Agreement and/or Order Form(s)/Statement(s) of Work
Key Contact	Contact details including email: Customer's email address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work	Full Name (optional): James Carder Job Title: Chief Information Security Officer Contact details including email: privacy@eptura.com
Signature (if required for the purposes of Section 2)	Not required	Not required

TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date:

	Reference (if any): Other identifier (if any): Or x the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	x			General Authorisation	14 days	
3	x			General Authorisation	14 days	
4						

TABLE 3: APPENDIX INFORMATION

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As identified in Exhibit A
Annex 1B: Description of Transfer: As identified in Exhibit A
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As identified in Exhibit B
Annex III: List of Sub processors (Modules 2 and 3 only): See www.eptura.com/subprocessors

TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☐ Importer x Exporter ☐ neither Party

PART 2: MANDATORY CLAUSES

ENTERING INTO THIS ADDENDUM

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

INTERPRETATION OF THIS ADDENDUM

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section **Error! Reference source not found.**.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

HIERARCHY

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

INCORPORATION OF AND CHANGES TO THE EU SCCS

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

AMENDMENTS TO THIS ADDENDUM

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which: a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or b. reflects changes to UK Data Protection Laws; The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in: a its direct costs of performing its obligations under the Addendum; and/or b its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

p.