Zusätzliche Bedingungen zur Einhaltung der Datenschutz-Grundverordnung (DS-GVO), UK-GDPR, DSG (Schweiz), CCPA/CPRA und zur Vertraulichkeit von Geschäftsgeheimnissen

Diese Allgemeinen Geschäftsbedingungen werden automatisch zum wesentlichen Bestandteil jeder vertraglichen Vereinbarung oder der getroffenen Abreden (im Folgenden „Hauptvertrag"), die zwischen unserem Unternehmen (im Folgenden „Anbieter", „Exporter", „Business", „uns" oder „unser"), wie im Impressum dieser oder einer unserer Webseite(n) und/oder im Hauptvertrag angegeben, und Ihrem Unternehmen (im Folgenden „Geschäftspartner", „Vertragspartner", „Lieferant", „Kunde", „Importer" „Contractor" oder „Ihnen") wie im Hauptvertrag angegeben, beziehungsweise bei einem mündlich, konkludent oder auf sonstige Weise abgeschlossenen Hauptvertrag, die juristische Person, Behörde, Einrichtung oder andere Stelle, die unser Vertragspartner ist, jedoch nur dann, wenn die Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrags erforderlich ist und die von der Verarbeitung betroffenen Personen in der EU, im EWR, in der Schweiz, im Vereinigten Königreich oder in Kalifornien ansässig sind, oder anderweitig durch die DS-GVO oder die UK-GDPR, das Schweizer Datenschutzgesetz (DSG) oder den CCPA/CPRA geschützt werden, und falls Betriebs- und Geschäftsgeheimnisse zwischen Ihnen und uns verarbeitet oder ausgetauscht werden.

Basierend auf der individuellen Geschäftsbeziehung zwischen Ihnen und uns gelten automatisch (1) einer oder mehrere der folgenden „EU-Standardvertragsklauseln", und/oder (2) das „International Data Transfer Agreement", und/oder (3) das „International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers" und/oder das (4) „Data Processing Agreement for the United Kingdom", und/oder (5) das „CCPA-CPRA CONTRACTOR AGREEMENT", und/oder (6) die Verschwiegenheitsvereinbarung und Wahrung des Datengeheimnisses für Lieferanten, falls Sie unser Lieferant aber kein Auftragsverarbeiter von uns sind, und/oder (7) basierend auf separat abgegebenen Willenserklärungen beider Parteien, die Verschwiegenheitsvereinbarung und Wahrung des Datengeheimnisses für Kunden, wenn Sie ein Kunde von uns sind, und auf unsere Geschäftsbeziehung keiner der nachfolgend aufgelisteten EU-Standardverträge oder andere hier enthaltene Verträge anwendbar sind:

Version: 1.05
Classification: Public
Document Owner: Heiko Maniero.
Information Contained: Business Data
Approved by: Heiko Maniero, Ulrich Baumann.
Date: 2022-10-27

Anlage 1 – SCCs 2021/915 - Verantwortlicher zu Auftragsverarbeiter

Anlage 2 – SCCs 2021/914 - MODUL EINS: Übermittlung Verantwortlicher zu Verantwortlicher

Anlage 3 - SCCs 2021/914 - MODUL ZWEI: Übermittlung Verantwortlicher zu Auftragsverarbeiter

Anlage 4 - SCCs 2021/914 - MODUL DREI: Übermittlung Auftragsverarbeiter zu Auftragsverarbeiter

Anlage 5 - SCCs 2021/914 - MODUL VIER: Übermittlung Auftragsverarbeiter zu Verantwortlicher

Anlage 6 – UNTERAUFTRGSVERARBEITER

Anlage 7 – LISTE DER PARTEIEN

Anlage 8 – BESCHREIBUNG DER DATENÜBERMITTLUNG ODER VERARBEITUNG

Anlage 9 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Anlage 10 – ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Anlage 11 – Verschwiegenheitsvereinbarung und Wahrung des Datengeheimnisses für Lieferanten

Anlage 12 – Verschwiegenheitsvereinbarung und Wahrung des Datengeheimnisses für Kunden

Anlage 13 – International Data Transfer Agreement (United Kingdom) (Vertragssprache: Englisch)

Anlage 14 – International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers (United Kingdom) (Vertragssprache: Englisch)

Anlage 15 – Data Processing Agreement for the United Kingdom (Vertragssprache: Englisch)

Anlage 16 – CCPA-CPRA CONTRACTOR AGREEMENT (Vertragssprache: Englisch)

Die geltenden Standardvertragsklauseln oder andere hier enthaltene Verträge regeln ausschließlich die Beziehung zwischen Ihnen und uns in Bezug auf die Verarbeitung personenbezogener Daten von betroffenen Personen mit Sitz oder Wohnsitz in Ländern oder Regionen, in denen die DS-GVO, die UK-GDPR, das DSG oder der CCPA/CPRA anwendbar sind („Personen-Daten-Verarbeitung") und haben Vorrang vor allen widersprüchlichen oder anders interpretierbaren Bestimmungen mit Bezug auf die Personen-Daten-Verarbeitung in allen Zusagen, Verpflichtungen, Vereinbarungen, Verträgen oder Übereinkommen zwischen Ihnen und uns, soweit und solange die EU-Standardvertragsklauseln oder UK-Verträge oder die anderen enthaltenen Verträge nicht durch neue Gesetze oder Verordnungen ersetzt wurden, die vom europäischen, britischen, schweizerischen oder kalifornischen Gesetzgeber (zusammenfassend, die „neuen DS-Gesetze") erlassen wurden, wobei diese neuen DS-Gesetze ab dem Datum ihrer Anwendbarkeit automatisch anstelle der jeweiligen Vertragsklauseln für die Personen-Daten-Verarbeitung zwischen Ihnen und uns gelten, es sei denn, eine Partei widerspricht gegenüber der anderen Partei schriftlich innerhalb von 30 Tagen nach dem offiziellen Veröffentlichungsdatum der neuen DS-Gesetze.

Standardvertragsklauseln 2021/915
Verantwortlicher zu Auftragsverarbeiter

Klausel 1

Zweck und Anwendungsbereich

(a) Mit diesen Standardvertragsklauseln (im Folgenden „**Klauseln**“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

(b) Die in **Anhang I** aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

(c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß **Anhang II**.

(d) Die **Anhänge I bis IV** sind Bestandteil der Klauseln.

(b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

(f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

(a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

(b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

(a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

(b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

(c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

Kopplungsklausel

(a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und **Anhang I** unterzeichnet.

(b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in **Anhang I**.

(c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in **Anhang II** aufgeführt.

Klausel 7

Pflichten der Parteien

7.1. Weisungen

(a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

(b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in **Anhang II** genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in **Anhang II** angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

(a) Der Auftragsverarbeiter ergreift mindestens die in **Anhang III** aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten 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 den 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 den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

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

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, 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 Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

(a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

(b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

(c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

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

(e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

(a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens dreißig Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

(c) Der Auftragsverarbeiter stellt dem Verantwortlichen 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 Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

(d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

(e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

(a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

(b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß **Klausel 7.7** für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

(a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

(b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

(c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß **Klausel 8** Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

(1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

(2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

(3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

(4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

(d) Die Parteien legen in **Anhang III** die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

(a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt

voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

(b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

(1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

(2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

(3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese 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;

(c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679 die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

(a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

(b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

(c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese 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.

Die Parteien legen in **Anhang III** alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

Verstöße gegen die Klauseln und Beendigung des Vertrags

(a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

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

(1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

(2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

(3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

(c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

(d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Liste der Parteien

SIEHE ANLAGE 7

Beschreibung der Verarbeitung

SIEHE ANLAGE 8

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

SIEHE ANLAGE 9

Liste der Unterauftragsverarbeiter

ERLÄUTERUNG:

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 7.7 Buchstabe a, Option 1).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

SIEHE ANLAGE 6

Standardvertragsklauseln 2021/914

MODUL EINS: Übermittlung Verantwortlicher zu Verantwortlicher

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, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

(b) Die Parteien:

i) die in **Anhang I.A** 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 „**Datenimporteur**“), haben sich mit diesen Standardvertragsklauseln (im Folgenden „**Klauseln**“) einverstanden erklärt.

(c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß **Anhang I.B**.

(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 nicht 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 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.

Klausel 3

Drittbegünstigte

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

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

ii) Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b

[iii) entfällt]

iv) Klausel 12 Buchstaben a und d

v) Klausel 13;

vi) Klausel 15.1 Buchstaben c, d und e;

vii) Klausel 16 Buchstabe e;

vii) 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 personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in **Anhang I.B** aufgeführt.

Klausel 7

Kopplungsklause

(a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und **Anhang I.A** unterzeichnet.

(b) Nach Ausfüllen der Anlage und Unterzeichnung von **Anhang I.A** wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in **Anhang I.A**.

(c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln

Klausel 8

Datenschutzgarantien

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

8.1. Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in **Anhang I.B** genannten spezifischen Zweck(e) der Übermittlung. Er darf die personenbezogenen Daten nur dann für einen anderen Zweck verarbeiten,

i) wenn er die vorherige Einwilligung der betroffenen Person eingeholt hat,
ii) wenn dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder,
iii) wenn dies zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist.

8.2. Transparenz

(a) Damit betroffene Personen ihre Rechte gemäß **Klausel 10** wirksam ausüben können, teilt der Datenimporteur ihnen entweder direkt oder über den Datenexporteur Folgendes mit:

i) seinen Namen und seine Kontaktdaten,
ii) die Kategorien der verarbeiteten personenbezogenen Daten,
iii) das Recht auf Erhalt einer Kopie dieser Klauseln,
iv) wenn er eine Weiterübermittlung der personenbezogenen Daten an Dritte beabsichtigt, den Empfänger oder die Kategorien von Empfängern (je nach Bedarf zur Bereitstellung aussagekräftiger Informationen), den Zweck und den Grund einer solchen Weiterübermittlung gemäß **Klausel 8.7**.

(b) Buchstabe a findet keine Anwendung, wenn die betroffene Person bereits über die Informationen verfügt, einschließlich in dem Fall, wenn diese Informationen bereits vom Datenexporteur bereitgestellt wurden, oder wenn sich die Bereitstellung der Informationen als nicht möglich erweist oder einen unverhältnismäßigen Aufwand für den Datenimporteur mit sich bringen würde. Im letzteren Fall macht der Datenimporteur die Informationen, soweit möglich, öffentlich zugänglich.

(c) Die Parteien stellen der betroffenen Person auf Anfrage eine Kopie dieser Klauseln, einschließlich der von ihnen ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, können die Parteien Teile des Textes der Anlage vor der Weitergabe einer Kopie unkenntlich machen; sie legen 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.

(d) Die Buchstaben a bis c gelten unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.3. Richtigkeit und Datenminimierung

(a) Jede Partei stellt sicher, dass die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind. Der Datenimporteur trifft alle angemessenen Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die im Hinblick auf den/die Zweck(e) der Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

(b) Stellt eine der Parteien fest, dass die von ihr übermittelten oder erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet sie unverzüglich die andere Partei.

(c) Der Datenimporteur stellt sicher, dass die personenbezogenen Daten angemessen und erheblich sowie auf das für den/die Zweck(e) ihrer Verarbeitung notwendige Maß beschränkt sind.

8.4. Speicherbegrenzung

Der Datenimporteur speichert die personenbezogenen Daten nur so lange, wie es für den/die Zweck(e), für den/die sie verarbeitet werden, erforderlich ist. Er trifft geeignete technische oder organisatorische Maßnahmen, um die Einhaltung dieser Verpflichtung sicherzustellen; hierzu zählen auch die Löschung oder Anonymisierung der Daten und aller Sicherungskopien am Ende der Speicherfrist.

8.5. Sicherheit der Verarbeitung

(a) Der Datenimporteur und — während der Datenübermittlung — auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen 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 den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie 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 betroffene Person gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

(b) Die Parteien haben sich auf die in **Anhang II** aufgeführten technischen und organisatorischen Maßnahmen geeinigt. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

(c) Der Datenimporteur gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(d) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(e) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, meldet der Datenimporteur die Verletzung unverzüglich sowohl dem Datenexporteur als auch der gemäß **Klausel 13** festgelegten zuständigen Aufsichtsbehörde. Diese Meldung enthält i) 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), ii) ihre wahrscheinlichen Folgen, iii) die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und iv) die Kontaktdaten einer Anlaufstelle, bei der weitere Informationen eingeholt werden können. Soweit es dem Datenimporteur nicht möglich ist, alle

Informationen zur gleichen Zeit bereitzustellen, kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(f) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Datenimporteur ebenfalls die jeweiligen betroffenen Personen unverzüglich von der Verletzung des Schutzes personenbezogener Daten und der Art der Verletzung, erforderlichenfalls in Zusammenarbeit mit dem Datenexporteur, unter Angabe der unter Buchstabe e Ziffern ii bis iv genannten Informationen, es sei denn, der Datenimporteur hat Maßnahmen ergriffen, um das Risiko für die Rechte oder Freiheiten natürlicher Personen erheblich zu mindern, oder die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. Im letzteren Fall gibt der Datenimporteur stattdessen eine öffentliche Bekanntmachung heraus oder ergreift eine vergleichbare Maßnahme, um die Öffentlichkeit über die Verletzung des Schutzes personenbezogener Daten zu informieren.

(g) Der Datenimporteur dokumentiert alle maßgeblichen Fakten im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, einschließlich ihrer Auswirkungen und etwaiger ergriffener Abhilfemaßnahmen, und führt Aufzeichnungen darüber.

8.6. Sensible Daten

Sofern 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 oder Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Datenimporteur spezielle Beschränkungen und/oder zusätzliche Garantien an, die an die spezifische Art der Daten und die damit verbundenen Risiken angepasst sind. Dies kann die Beschränkung des Personals, das Zugriff auf die personenbezogenen Daten hat, zusätzliche Sicherheitsmaßnahmen (wie Pseudonymisierung) und/oder zusätzliche Beschränkungen in Bezug auf die weitere Offenlegung umfassen.

8.7. Weiterübermittlungen

Der Datenimporteur darf die personenbezogenen Daten nicht an Dritte weitergeben, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union ansässig sind (im Folgenden „Weiterübermittlung“), es sei denn, der Dritte ist im Rahmen des betreffenden Moduls an diese Klauseln gebunden oder erklärt sich mit der Bindung daran einverstanden. Andernfalls ist eine Weiterübermittlung durch den Datenimporteur nur in folgenden Fällen zulässig:

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

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

iii) der Dritte geht mit dem Datenimporteur ein bindendes Instrument ein, mit dem das gleiche Datenschutzniveau wie gemäß diesen Klauseln gewährleistet wird, und der Datenimporteur stellt dem Datenexporteur eine Kopie dieser Garantien zur Verfügung,

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

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

vi) falls keine der anderen Bedingungen erfüllt ist — der Datenimporteur hat die ausdrückliche Einwilligung der betroffenen Person zu einer Weiterübermittlung in einem speziellen Fall eingeholt, nachdem er sie über den/die Zweck(e), die Identität des Empfängers und die ihr mangels geeigneter Datenschutzgarantien aus einer solchen Übermittlung möglicherweise erwachsenden Risiken informiert hat. In diesem Fall unterrichtet der Datenimporteur den Datenexporteur und übermittelt ihm auf dessen Verlangen eine Kopie der Informationen, die der betroffenen Person bereitgestellt wurden.

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

8.8. Verarbeitung unter der Aufsicht des Datenimporteurs

Der Datenimporteur stellt sicher, dass jede ihm unterstellte Person, einschließlich eines Auftragsverarbeiters, diese Daten ausschließlich auf der Grundlage seiner Weisungen verarbeitet.

8.9. Dokumentation und Einhaltung der Klauseln

(a) Jede Partei muss nachweisen können, dass sie ihre Pflichten gemäß diesen Klauseln erfüllt. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die unter seiner Verantwortung durchgeführten Verarbeitungstätigkeiten.

(b) Der Datenimporteur stellt der zuständigen Aufsichtsbehörde diese Aufzeichnungen auf Verlangen zur Verfügung.

[Klausel 9: entfällt]

Klausel 10

Rechte betroffener Personen

(a) Der Datenimporteur bearbeitet, gegebenenfalls mit Unterstützung des Datenexporteurs, alle Anfragen und Anträge einer betroffenen Person im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und der Ausübung ihrer Rechte gemäß diesen Klauseln unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang der Anfrage oder des Antrags. Der Datenimporteur trifft geeignete Maßnahmen, um solche Anfragen und Anträge und die Ausübung der Rechte betroffener Personen zu erleichtern. Alle Informationen, die der betroffenen Person zur Verfügung gestellt werden, müssen in verständlicher und leicht zugänglicher Form vorliegen und in einer klaren und einfachen Sprache abgefasst sein.

(b) Insbesondere unternimmt der Datenimporteur auf Antrag der betroffenen Person folgende Handlungen, wobei der betroffenen Person keine Kosten entstehen:

i) Er legt der betroffenen Person eine Bestätigung darüber vor, ob sie betreffende personenbezogene Daten verarbeitet werden, und, falls dies der Fall ist, stellt er ihr eine Kopie der sie betreffenden Daten und die in **Anhang I** enthaltenen Informationen zur Verfügung; er stellt, falls personenbezogene Daten weiterübermittelt wurden oder werden, Informationen über die Empfänger oder Kategorien von Empfängern (je nach Bedarf zur Bereitstellung aussagekräftiger Informationen), an die die personenbezogenen Daten weiterübermittelt wurden oder werden, sowie über den Zweck dieser Weiterübermittlung und deren Grund gemäß **Klausel 8.7** bereit; er informiert die betroffene Person über ihr Recht, gemäß **Klausel 12 Buchstabe c Ziffer i** bei einer Aufsichtsbehörde Beschwerde einzulegen;

ii) Er berichtigt unrichtige oder unvollständige Daten über die betroffene Person;

iii) Er löscht personenbezogene Daten, die sich auf die betroffene Person beziehen, wenn diese Daten unter Verstoß gegen eine dieser Klauseln, die Rechte als Drittbegünstigte

gewährleisten, verarbeitet werden oder wurden oder wenn die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung stützt, widerruft.

(c) Verarbeitet der Datenimporteur die personenbezogenen Daten für Zwecke der Direktwerbung, so stellt er die Verarbeitung für diese Zwecke ein, wenn die betroffene Person Widerspruch dagegen einlegt.

(d) Der Datenimporteur trifft keine Entscheidung, die ausschließlich auf der automatisierten Verarbeitung der übermittelten personenbezogenen Daten beruht (im Folgenden „automatisierte Entscheidung"), welche rechtliche Wirkung für die betroffene Person entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen würde, es sei denn, die betroffene Person hat hierzu ihre ausdrückliche Einwilligung gegeben oder eine solche Verarbeitung ist nach den Rechtsvorschriften des Bestimmungslandes zulässig und in diesen sind angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person festgelegt. In diesem Fall muss der Datenimporteur, erforderlichenfalls in Zusammenarbeit mit dem Datenexporteur,

i) die betroffene Person über die geplante automatisierte Entscheidung, die angestrebten Auswirkungen und die damit verbundene Logik unterrichten und

ii) geeignete Garantien umsetzen, die mindestens bewirken, dass die betroffene Person die Entscheidung anfechten, ihren Standpunkt darlegen und eine Überprüfung durch einen Menschen erwirken kann.

(e) Bei exzessiven Anträgen einer betroffenen Person — insbesondere im Fall von häufiger Wiederholung — kann der Datenimporteur entweder eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten für die Erledigung des Antrags verlangen oder sich weigern, aufgrund des Antrags tätig zu werden.

(f) Der Datenimporteur kann den Antrag einer betroffenen Person ablehnen, wenn eine solche Ablehnung nach den Rechtsvorschriften des Bestimmungslandes zulässig und in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele zu schützen.

(g) Beabsichtigt der Datenimporteur, den Antrag einer betroffenen Person abzulehnen, so unterrichtet er die betroffene Person über die Gründe für die Ablehnung und über die Möglichkeit, Beschwerde bei der zuständigen Aufsichtsbehörde einzulegen und/oder einen gerichtlichen Rechtsbehelf einzulegen.

Klausel 11

Rechtsbehelf

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

(f) Der Datenimporteur 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) Jede Partei haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den die Partei der betroffenen Person verursacht, indem sie deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs gemäß der Verordnung (EU) 2016/679.

(c) 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.

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

(e) Der Datenimporteur kann sich nicht auf das Verhalten eines Auftragsverarbeiters oder Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung zu entziehen.

Klausel 13

Aufsicht

(a) [Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist:] Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in **Anhang I.C**).

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt hat:] Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 niedergelassen ist, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in **Anhang I.C**).

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 2 der Verordnung (EU) 2016/679 benennen zu müssen:] 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 Datenimporteur 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.

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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteurs 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 Datenimporteur 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 Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur 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 Datenimporteurs gemäß **Klausel 14 Buchstabe e**.

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

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

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

(b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur 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 in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

iii) der Datenimporteur 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.

(d) 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 bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur 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.

(e) 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 eines der EU-Mitgliedstaaten, sofern dieses Recht Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von Deutschland.

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 Deutschland sind.

(c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur 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.

A. LISTE DER PARTEIEN

SIEHE ANLAGE 7

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

SIEHE ANLAGE 8

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

SIEHE ANLAGE 10

ANHANG II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

SIEHE ANLAGE 9

Standardvertragsklauseln 2021/914
MODUL ZWEI: Übermittlung Verantwortlicher zu Auftragsverarbeiter

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 2016zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

(b) Die Parteien:

i) die in **Anhang I.A** 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 „**Datenimporteur**“),

haben sich mit diesen Standardvertragsklauseln (im Folgenden „**Klauseln**“) einverstanden erklärt.

(c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß **Anhang I.B**.

(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 nicht 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 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.

Klausel 3

Drittbegünstigte

(a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit 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 personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in **Anhang I.B** aufgeführt

Klausel 7

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und **Anhang I.A** unterzeichnet.

b) Nach Ausfüllen der Anlage und Unterzeichnung von **Anhang I.A** wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in **Anhang I.A.**

c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

Klausel 8

Datenschutzgarantien

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

8.1. Weisungen

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

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

8.2. Zweckbindung

Der Datenimporteur 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 Datenimporteur fest, dass die erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet er unverzüglich den Datenexporteur. In diesem Fall arbeitet der Datenimporteur 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 Datenimporteur 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 Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Datenimporteur 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 Datenimporteurs 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 Datenimporteur 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 Datenimporteur mindestens die in **Anhang II** aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

b) Der Datenimporteur 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 Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Datenimporteur 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 Datenimporteur zur Verfügung stehenden Informationen arbeitet der Datenimporteur 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 Datenimporteur die in **Anhang I.B** beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8. Weiterübermittlungen

Der Datenimporteur 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(4)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 Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

8.9. Dokumentation und Einhaltung der Klauseln

(a) Der Datenimporteur 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 Datenimporteur geeignete Aufzeichnungen über die im Auftrag des Datenexporteurs durchgeführten Verarbeitungstätigkeiten.

(c) Der Datenimporteur 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) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG. 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 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 Datenimporteur 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 Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß **Klausel 8.8** nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.

(c) Der Datenimporteur 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 Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

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

(e) Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Datenimporteur 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 betroffener Personen

a) Der Datenimporteur 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 Datenimporteur 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 Datenimporteur die Weisungen des Datenexporteurs.

Klausel 11

Rechtsbehelf

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

(f) Der Datenimporteur 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 Datenimporteur 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 Datenimporteur (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Datenimporteur den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Datenimporteurs 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 Datenimporteur kann sich nicht auf das Verhalten eines Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung entziehen.

Klausel 13

Aufsicht

(a) [Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist:] Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in **Anhang I.C).**

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt hat:] Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 niedergelassen ist, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in **Anhang I.C).**

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 2 der Verordnung (EU) 2016/679 benennen zu müssen:] 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 Datenimporteur 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.

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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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.

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

15.1. Benachrichtigung

(a) Der Datenimporteur 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 Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteurs 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 Datenimporteur 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 Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur 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 Datenimporteurs gemäß **Klausel 14 Buchstabe (e)**.

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

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

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

(b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur 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

(1) 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,

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

(3) der Datenimporteur 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.

(d) 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 bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur 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.

(e) 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 Deutschland 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 Deutschland sind.

(c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur 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.

A. LISTE DER PARTEIEN

SIEHE ANLAGE 7

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

SIEHE ANLAGE 8

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

SIEHE ANLAGE 10

ANHANG II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

SIEHE ANLAGE 9

ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

SIEHE ANLAGE 6

Standardvertragsklauseln 2021/914
MODUL DREI: Übermittlung Auftragsverarbeiter zu Auftragsverarbeiter

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, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

(b) Die Parteien:

i) die in **Anhang I.A** 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 „**Datenimporteur**“).

haben sich mit diesen Standardvertragsklauseln (im Folgenden „**Klauseln**“) einverstanden erklärt.

(c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß **Anhang I.B**.

(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 nicht 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 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.

Klausel 3

Drittbegünstigte

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

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

ii) Klausel 8.1 Buchstaben (a), (c) und (d) und Klausel 8.9 Buchstaben (a), (c), (d), (e), (f) und (g);

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 personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

Klausel 7

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und **Anhang I.A** unterzeichnet.

b) Nach Ausfüllen der Anlage und Unterzeichnung von **Anhang I.A** wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in **Anhang I.A.**

c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

Klausel 8

Datenschutzgarantien

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

8.1. Weisungen

a) Der Datenexporteur hat dem Datenimporteur mitgeteilt, dass er als Auftragsverarbeiter nach den Weisungen seines/seiner Verantwortlichen fungiert, und der Datenexporteur stellt dem Datenimporteur diese Weisungen vor der Verarbeitung zur Verfügung.

b) Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf der Grundlage dokumentierter Weisungen des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, sowie auf der Grundlage aller zusätzlichen dokumentierten Weisungen des Datenexporteurs. Diese zusätzlichen Weisungen dürfen nicht im Widerspruch zu den Weisungen des Verantwortlichen stehen. Der Verantwortliche oder der Datenexporteur kann während der gesamten Vertragslaufzeit weitere dokumentierte Weisungen im Hinblick auf die Datenverarbeitung erteilen.

c) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann. Ist der Datenimporteur nicht in der Lage, die Weisungen des Verantwortlichen zu befolgen, setzt der Datenexporteur den Verantwortlichen unverzüglich davon in Kenntnis.

d) Der Datenexporteur sichert zu, dass er dem Datenimporteur dieselben Datenschutzpflichten auferlegt hat, die im Vertrag oder in einem anderen Rechtsinstrument nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zwischen dem Verantwortlichen und dem Datenexporteur festgelegt sind.

8.2. Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Übermittlungszweck(e), sofern keine weiteren Weisungen seitens des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, oder seitens 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 personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage 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.

8.4. Richtigkeit

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

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 Datenimporteur nach Beendigung der Datenverarbeitungsdienste alle im Auftrag des Verantwortlichen 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 Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Datenimporteur 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 Datenimporteurs 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 Datenimporteur 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 sie 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 betroffene Person 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 oder des Verantwortlichen. Zur Erfüllung seinen Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

(b) Der Datenimporteur gewährt seinem Personal nur insoweit Zugang zu den 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 Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Außerdem meldet der Datenimporteur die Verletzung dem Datenexporteur und, sofern angemessen und machbar, dem

Verantwortlichen unverzüglich, nachdem ihm die Verletzung 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 des Schutzes der Daten, einschließlich 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 Datenimporteur zur Verfügung stehenden Informationen arbeitet der Datenimporteur mit dem Datenexporteur zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen, insbesondere den Verantwortlichen zu unterrichten, damit dieser wiederum die zuständige Aufsichtsbehörde und die betroffenen Personen benachrichtigen kann.

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 Datenimporteur die in Anhang I.B angegebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8. Weiterübermittlungen

Der Datenimporteur gibt die personenbezogenen Daten nur auf der Grundlage dokumentierter Weisungen des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, 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 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 Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

8.9. Dokumentation und Einhaltung der Klauseln

(a) Der Datenimporteur bearbeitet Anfragen des Datenexporteurs oder des Verantwortlichen, 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 Datenimporteur geeignete Aufzeichnungen über die im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten.

(c) Der Datenimporteur stellt dem Datenexporteur alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten Pflichten erforderlich sind, und der Datenexporteur stellt diese Informationen wiederum dem Verantwortlichen bereit.

(d) Der Datenimporteur ermöglicht dem Datenexporteur die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Gleiches gilt, wenn der Datenexporteur eine Prüfung auf Weisung des Verantwortlichen beantragt. Bei der Entscheidung über eine Prüfung kann der Datenexporteur einschlägige Zertifizierungen des Datenimporteurs berücksichtigen.

(e) Wird die Prüfung auf Weisung des Verantwortlichen durchgeführt, stellt der Datenexporteur die Ergebnisse dem Verantwortlichen zur Verfügung.

(f) 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.

(g) 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) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG. Der Datenimporteur besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Verantwortlichen mindestens 30 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Datenimporteur stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Der Datenimporteur unterrichtet den Datenexporteur über die Beauftragung des/der Unterauftragsverarbeiter/s.

(b) Beauftragt der Datenimporteur einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), 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 Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß **Klausel 8.8** nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.

(c) Auf Verlangen des Datenexporteurs oder des Verantwortlichen stellt der Datenimporteur 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 Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

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

(e) Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Datenimporteur 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 betroffener Personen

(a) Der Datenimporteur unterrichtet den Datenexporteur und gegebenenfalls den Verantwortlichen unverzüglich über jeden Antrag, den er von einer betroffenen Person erhält; er beantwortet diesen Antrag erst dann, wenn er vom Verantwortlichen dazu ermächtigt wurde.

(b) Der Datenimporteur unterstützt den Verantwortlichen, gegebenenfalls in Zusammenarbeit mit dem Datenexporteur, bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 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 Datenimporteur die Weisungen des Verantwortlichen, die ihm vom Datenexporteur übermittelt wurden.

Klausel 11

Rechtsbehelf

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

(f) Der Datenimporteur 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 Datenimporteur 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 Datenimporteur (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Datenimporteur den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Datenimporteurs 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 Datenimporteur kann sich nicht auf das Verhalten eines Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung entziehen.

Klausel 13

Aufsicht

(a) [Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist:] Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt hat:] Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 niedergelassen ist, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser

Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 2 der Verordnung (EU) 2016/679 benennen zu müssen:] 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 Datenimporteur 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.

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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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. Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.

(f) Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur 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 Datenimporteur ergreifen müssen, um Abhilfe zu schaffen, gegebenenfalls in Absprache mit dem Verantwortlichen. 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 vom Verantwortlichen oder 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 Datenimporteur 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.

Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.

(b) Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur 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 Datenimporteur 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.). Der Datenexporteur leitet die Informationen an den Verantwortlichen weiter.

(d) Der Datenimporteur 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 Datenimporteurs 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 Datenimporteur 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 Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur 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 Datenimporteurs gemäß **Klausel 14 Buchstabe (e)**.

(b) Der Datenimporteur 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. Der Datenexporteur stellt die Beurteilung dem Verantwortlichen zur Verfügung.

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

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

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

(b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur 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 in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

iii) der Datenimporteur 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 und den Verantwortlichen 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.

(d) 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 bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur 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.

(e) 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 Deutschland 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 Deutschland sind.

(c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur 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.

A. LISTE DER PARTEIEN

SIEHE ANLAGE 7

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

SIEHE ANLAGE 8

B. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

SIEHE ANLAGE 10

ANHANG II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

SIEHE ANLAGE 9

ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

SIEHE ANLAGE 6

Standardvertragsklauseln 2021/914
MODUL VIER: Übermittlung Auftragsverarbeiter zu Verantwortlicher

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 2016zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

(b) Die Parteien:

i) die in **Anhang I.A** 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 „**Datenimporteur**“),

haben sich mit diesen Standardvertragsklauseln (im Folgenden „**Klauseln**“) einverstanden erklärt.

(c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß **Anhang I.B**.

(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 nicht 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 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.

Klausel 3

Drittbegünstigte

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

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

ii) Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe (b)

[iii) und iv) entfällt]

v) Klausel 13

vi) Klausel 15.1 (c), (d) and (e);

vii) Klausel 16 (e);

viii) Klausel 18;

(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 personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in **Anhang I.B** aufgeführt.

Klausel 7

Kopplungsklausel

(a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und **Anhang I.A** unterzeichnet.

(b) Nach Ausfüllen der Anlage und Unterzeichnung von **Anhang I.A** wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in **Anhang I.A**.

(c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

Klausel 8

Datenschutzgarantien

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

8.1. Weisungen

(a) Der Datenexporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenimporteurs, der als sein Verantwortlicher fungiert.

(b) Der Datenexporteur unterrichtet den Datenimporteur unverzüglich, wenn er die betreffenden Weisungen nicht befolgen kann, u. a. wenn eine solche Weisung gegen die Verordnung (EU) 2016/679 oder andere Datenschutzvorschriften der Union oder eines Mitgliedstaats verstößt.

(c) Der Datenimporteur sieht von jeglicher Handlung ab, die den Datenexporteur an der Erfüllung seiner Pflichten gemäß der Verordnung (EU) 2016/679 hindern würde, einschließlich im Zusammenhang mit Unterverarbeitungen oder der Zusammenarbeit mit den zuständigen Aufsichtsbehörden.

(d) Nach Wahl des Datenimporteurs löscht der Datenexporteur nach Beendigung der Datenverarbeitungsdienste alle im Auftrag des Datenimporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenimporteur, dass dies erfolgt ist, oder gibt dem Datenimporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien.

8.2. Sicherheit der Verarbeitung

(a) Die Parteien treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen Daten, auch während der Übermittlung, sowie den Schutz vor einer Verletzung der Sicherheit zu gewährleisten, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie dem Stand der Technik, den Implementierungskosten, der Art der personenbezogenen Daten, 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 und ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Übermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

(b) Der Datenexporteur unterstützt den Datenimporteur bei der Gewährleistung einer angemessenen Sicherheit der Daten gemäß Buchstabe a. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Datenexporteur gemäß diesen Klauseln verarbeiteten personenbezogenen Daten meldet der Datenexporteur dem Datenimporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde, und unterstützt den Datenimporteur bei der Behebung der Verletzung.

(c) Der Datenexporteur gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.3. Dokumentation und Einhaltung der Klauseln

(a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

(b) Der Datenexporteur stellt dem Datenimporteur alle Informationen zur Verfügung, die für den Nachweis der Einhaltung seiner Pflichten gemäß diesen Klauseln erforderlich sind, und ermöglicht Prüfungen und trägt zu diesen bei.

[Klausel 9 entfällt]

Klausel 10

Rechte betroffener Personen

Die Parteien unterstützen sich gegenseitig bei der Beantwortung von Anfragen und Anträgen, die von betroffenen Personen gemäß den für den Datenimporteur geltenden lokalen Rechtsvorschriften oder — bei der Datenverarbeitung durch den Datenexporteur in der Union — gemäß der Verordnung (EU) 2016/679 gestellt werden.

Klausel 11

Rechtsbehelf

Der Datenimporteur 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.

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) Jede Partei haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den die Partei der betroffenen Person verursacht, indem sie deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs gemäß der Verordnung (EU) 2016/679.

(c) 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.

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

(e) Der Datenimporteur kann sich nicht auf das Verhalten eines Auftragsverarbeiters oder Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung zu entziehen.

[Klausel 13 entfällt]

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

Wenn der in der EU ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden:

(a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteur 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

Wenn der in der EU ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden:

15.1. Benachrichtigung

(a) Der Datenimporteur 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 Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur 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 Datenimporteur 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 Datenimporteur 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 Datenimporteurs 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 Datenimporteur 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 Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur 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 Datenimporteurs gemäß **Klausel 14 Buchstabe e**.

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

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

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

(b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur 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,

i) der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

iii) der Datenimporteur 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.

(d) Von dem in der EU ansässigen Datenexporteur erhobene personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen unverzüglich

vollständig gelöscht werden, einschließlich aller Kopien. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur 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.

(e) 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 eines Landes, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von Deutschland ist.

Klausel 18

Gerichtsstand und Zuständigkeit

Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten von Deutschland beigelegt**.**

A. LISTE DER PARTEIEN

SIEHE ANLAGE 7

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

SIEHE ANLAGE 8

EIN AKTUELLE LISTE UNSERER AUFTRAGSVERARBEITER FINDEN SIE AUF UNSERER WEBSEITE ODER KANN GESONDERT ANGEFORDERT WERDEN.

Unsere Liste enthält folgende Angaben zu allen Auftragsverarbeitern:

Firmenname, Link zur Webseite, Angaben zur Dienstleistung oder Übermittlung, Land der Verarbeitung, Gegenstand der (Unter-)Auftragsverarbeitung, Art der (Unter-)Auftragsverarbeitung, Dauer der (Unter-)Auftragsverarbeitung, Abgeschlossener Vertrag bzw. geeignete Garantien nach Art. 44ff DS-GVO.

WENN SIE ANDERE AUFTRAGSVERARBEITER NUTZEN, DIE IN UNSERER LISTE NICHT ERWÄHNT UND/ODER VON UNS ZUGELASSEN SIND, SENDEN SIE UNS BITTE EINE LISTE IHRER AUFTRAGSVERARBEITER ZUR ÜBERPRÜFUNG UND/ODER GENEHMIGUNG.

Vertragspartei Nummer 1:

Name: Anbieter name, siehe Hauptvertrag

Anschrift: Anschrift des Anbieters, siehe Hauptvertrag

Name, Funktion und Kontaktdaten der Kontaktperson: Anbieter Kontaktperson, siehe Hauptvertrag

Tätigkeiten, die für die gemäß diesen Klauseln verarbeiteten oder übermittelten Daten von Belang sind: Sämtliche Tätigkeiten bei denen personenbezogene Daten verarbeitet oder übermittelt werden

Gegebenenfalls, Name und Kontaktdaten des Datenschutzbeauftragten: Siehe gegebenenfalls Webseite des Anbieters

Gegebenenfalls, Name und Kontaktdaten des Vertreters in der Europäischen Union: Siehe gegebenenfalls Webseite des Geschäftspartners

Beitrittsdatum/Datum: Siehe Datum des Hauptvertrags

Rolle: Verantwortlicher und/oder Auftragsverarbeiter, basierend auf dem jeweils anwendbaren Standardvertrag

Vertragspartei Nummer 2:

Name: Geschäftspartner name, siehe Hauptvertrag

Anschrift: Anschrift des Geschäftspartners, siehe Hauptvertrag

Name, Funktion und Kontaktdaten der Kontaktperson: Geschäftspartner Kontaktperson, siehe Hauptvertrag

Tätigkeiten, die für die gemäß diesen Klauseln verarbeiteten oder übermittelten Daten von Belang sind: Sämtliche Tätigkeiten bei denen personenbezogene Daten verarbeitet oder übermittelt werden

Gegebenenfalls, Name und Kontaktdaten des Datenschutzbeauftragten: Siehe gegebenenfalls Webseite des Geschäftspartners

Gegebenenfalls, Name und Kontaktdaten des Vertreters in der Europäischen Union: Siehe gegebenenfalls Webseite des Geschäftspartners

Beitrittsdatum/Datum: Siehe Datum des Hauptvertrags

Rolle: Verantwortlicher und/oder Auftragsverarbeiter, basierend auf dem jeweils anwendbaren Standardvertrag

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet oder übermittelt werden

Kunden, Interessenten, Mitarbeiter, Geschäftspartner, Lieferanten.

Kategorien der personenbezogenen Daten, die verarbeitet oder übermittelt werden

Kundendaten, Interessentendaten, Mitarbeiterdaten, Geschäftspartner-Daten, Lieferantendaten.

Verarbeitete oder übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

Verarbeitete oder übermittelte sensible Daten

Keine.

Angewandte Beschränkungen oder Garantien

Keine, da keine sensiblen Daten verarbeitet oder übertragen werden.

Häufigkeit der Übermittlung:

Die Daten werden während der Laufzeit des Main-Agreements kontinuierlich übertragen.

Art der Verarbeitung

Siehe Hauptvertrag, es könnte zu den folgenden Verarbeitungen kommen: Erheben, Anpassung, Offenlegung durch Übermittlung, Einschränkung, Erfassen, Veränderung, Verbreitung, Löschen, Organisation, Auslesen, andere Form der Bereitstellung, Vernichtung, Ordnen, Abfragen, Abgleich, Speicherung, Verwendung, Verknüpfung.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet oder übermittelt werden

Siehe Hauptvertrag.

Dauer der Verarbeitung

Dauer des Hauptvertrags.

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

Die Kriterien für die Festlegung der Speicherdauer ergeben sich aus dem Hauptvertrag und gesetzlichen Aufbewahrungsfristen.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Gegenstand der (Unter-)Auftragsverarbeitung: SIEHE ANLAGE 6

Art der (Unter-)Auftragsverarbeitung: SIEHE ANLAGE 6

Dauer der (Unter-)Auftragsverarbeitung: SIEHE ANLAGE 6

Die im Folgenden genannten technischen und organisatorischen Sicherheitsmaßnahmen sind das von Ihnen geforderte Minimum und werden auch von uns erfüllt. Sollten Sie diese technischen und organisatorischen Sicherheitsmaßnahmen nicht umgesetzt haben, informieren Sie uns bitte unverzüglich. Darüber hinaus übermitteln Sie uns bitte eine Liste aller zusätzlichen technischen und organisatorischen Sicherheitsmaßnahmen, die Sie ggf. ergriffen haben.

1. **Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten**

Pseudonymisierung von nicht mehr im Klartext benötigten personenbezogenen Daten

Verschlüsselung von Webseiten (SSL)

E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)

2. **Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung**

Vertraulichkeitsvereinbarungen mit Mitarbeitern

NDAs mit Dritten

Datenschutzverpflichtung der Mitarbeiter

Firewall

Antivirenprogramm

Regelmäßige Datensicherungen

3. **Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen**

Regelmäßige Backups des gesamten

Regelmäßiger Test Backup/Recovery

Regelmäßige Schulung des IT-Personals

4. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung**

Interne Kontrollen

Regelmäßige Überprüfung der IT-Prozesse

Regelmäßige Audits (z.B. durch den DSB)

5. **Maßnahmen zur Identifizierung und Autorisierung der Nutzer**

Authentisierung mit Benutzername / Passwort
Regelmäßige Prüfung von Berechtigungen
Passwort-Richtlinie
Begrenzung der Anzahl der Admins
Verwaltung der Rechte durch einen Admin

6. Maßnahmen zum Schutz der Daten während der Übermittlung

Einsatz von Verschlüsselungstechnologien
Protokollierung von Aktivitäten und Ereignissen
E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)
Verwendung nicht öffentlicher Laufwerke

7. Maßnahmen zum Schutz der Daten während der Speicherung

Protokollierung von Aktionen und Ereignissen
Begrenzung der Anzahl der Administratoren
Firewall

8. Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Manuelles Schließsystem
Sicherheitsschlösser
Verfahren zur Schlüsselausgabe

9. Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Protokollierung auf Applikationsebene
Regelmäßige manuelle Überprüfung der Protokolle

10. Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Prozess zu Konfigurationsänderungen
Datenschutzgerechte Voreinstellungen
Konfiguration durch Systemadministrator
Regelmäßige Schulung der IT-Mitarbeiter

11. Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Schulung der Mitarbeiter zur Datensicherheit

IT-Team mit klaren Rollen / Verantwortlichkeiten

12. Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Klarer Überblick über die für Produkte/Dienstleistungen/Prozesse geltenden Bestimmungen

Regelmäßige interne und/oder externe Audits

Zuweisung von Audit-Verantwortlichkeiten an zertifizierte Experten

13. Maßnahmen zur Gewährleistung der Datenminimierung

Identifikation des Zwecks der Verarbeitung

Bewertung des Zusammenhangs zwischen Verarbeitung und Zweck

Identifikation der geltenden Aufbewahrungsfristen

Sichere Löschung der Daten nach Ablauf der Aufbewahrungsfrist

14. Maßnahmen zur Gewährleistung der Datenqualität

Protokollierung Eingabe/Änderung Daten

Rechtevergabe zur Dateneingabe

Nachvollziehbarkeit der Benutzer bei Eingabe,

15. Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Regelmäßige Schulungen

Regelmäßige Prüfung und Bewertung der gespeicherten Daten

16. Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Schulungen / Sensibilisierung

Regelmäßige Kontrollen und Prüfungen

Angemessene Richtlinien zum Datenschutz

Abschluss von Standardvertragsklauseln

17. Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Speicherung in einem strukturiertem Format

Überwachung gesetzlicher Fristen

Einhaltung von Aufbewahrungsfristen

Ermöglichung der Datenübertragbarkeit

Richtiger Umgang mit Betroffenenrechten

Sichere Datenlöschung und Datenträgervernichtung gewährleistet durch Beauftragung der Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Deutschland, E-Mail: info@notebook12.com

18. **Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-) Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.**

Standardvertragsklauseln (SCCs) werden unterzeichnet oder vereinbart

Vertraglich vereinbarte, wirksame Kontrollrechte

Vertraglich vereinbarte Unterstützung des Verantwortlichen

Die für den ersten Verantwortlichen örtlich zuständige Aufsichtsbehörde ist zuständig. Sitzt der erste Verantwortliche außerhalb der Europäischen Union oder des EWR vereinbaren die Parteien hiermit unwiderruflich die Zuständigkeit der folgenden Aufsichtsbehörde:

BayLDA - Das Bayerische Landesamt für Datenschutzaufsicht

Promenade 18

91522 Ansbach

Deutschland

Verschwiegenheitsvereinbarung und Wahrung des Datengeheimnisses für Lieferanten

Zwischen unserem Unternehmen

- Auftraggeber -

und Ihrem Unternehmen

- Vertragspartner -

wird Folgendes vereinbart:

1. Der Vertragspartner ist verpflichtet, Geschäfts- und Betriebsgeheimnisse sowie betriebliche Angelegenheiten vertraulicher Natur, die vom Auftraggeber schriftlich oder mündlich als solche bezeichnet werden bzw. offensichtlich als solche zu erkennen sind, geheim zu halten und ohne ausdrückliche Genehmigung des Auftraggebers keinen Dritten zugänglich zu machen. Die Geheimhaltungsverpflichtung gilt auch gegenüber Mitarbeitern des Auftraggebers und Auftragnehmers, Dritten und anderen Vertragspartnern des Auftraggebers und des Auftragnehmers und deren Mitarbeitern, sofern diese mit dem betreffenden Sachverhalt nicht unmittelbar befasst sind.

   Betriebs- und Geschäftsgeheimnis ist jede Information, die

   a) weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

   b) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

   c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

   Geschäftsgeheimnis im Sinne der globalen Geschäftsgeheimnis-Gesetze und damit vertraulich sind insbesondere Informationen betreffend Preisen, Planzahlen, Umsatz-/Gewinn-/Ertragszahlen, ökonomische Kennzahlen, laufende und geplante Projekte, programmtechnische und konzeptionelle Strukturen, Analysetätigkeiten, Softwarearchitektur und Schnittstellen, Datensätze und deren Verwendung, Passwörter, Berechtigungen, Beschäftigten-, Lieferanten und Kundendaten, Daten sonstiger Geschäftspartner sowie insbesondere sämtliche vertraulichen Informationen betreffend Kunden oder Lieferanten des Auftraggebers, zu denen der Vertragspartner im Rahmen der Vorbereitung und Durchführung des Auftrags oder für Kunden oder Lieferanten der Auftraggeber Zugang erhalten hat, wie beispielsweise Informationen betreffend Kunden oder Lieferanten des Auftraggebers, Geschäftsabläufe, Infrastruktur, Geschäftspläne und -produkte, Software, Programme sowie jegliche Informationen, die der Vertragspartner unter Verwendung vertraulicher Informationen erarbeitet hat. Der Verschwiegenheitspflicht unterliegen nicht solche Informationen, die

jedermann zugänglich oder allgemein bekannt sind. In Zweifelsfällen hat der Vertragspartner eine Weisung des Auftraggebers zur Vertraulichkeit bestimmter Tatsachen einzuholen.

2. Der Vertragspartner ist verpflichtet, das Bankgeheimnis, das Fernmeldegeheimnis, die Vertraulichkeit der Kommunikation, das Postgeheimnis, das Sozialgeheimnis, das Briefgeheimnis und alle anderen Geheimnisvorschriften und Gesetze zu wahren.

3. Die Verschwiegenheitspflicht gilt nicht gegenüber Dritten, soweit diesen gegenüber eine gesetzliche Offenbarungspflicht besteht. Sie gilt auch nicht gegenüber standesrechtlich zur Verschwiegenheit verpflichteten Personen, soweit die Offenbarung der geheim zu haltenden Tatsachen zur berechtigten Interessenwahrnehmung des Vertragspartners notwendig ist.

4. Die Verschwiegenheitspflicht erstreckt sich auch auf Angelegenheiten anderer Unternehmen, mit denen der Auftraggeber wirtschaftlich oder organisatorisch verbunden ist.

5. Die Verpflichtung zur Verschwiegenheit besteht auch nach Beendigung des Vertragsverhältnisses fort. Sollte die nachvertragliche Verpflichtung zur Verschwiegenheit den Vertragspartner unangemessen in seinem beruflichen Fortkommen behindern, hat er einen Anspruch gegen den Auftraggeber auf Freistellung von dieser Verpflichtung.

6. Der Vertragspartner wurde darauf hingewiesen, dass Geheimnisverrat nach geltenden Gesetzen zum Schutz von Geschäftsgeheimnissen strafbar sein kann.

7. Der Vertragspartner ist zur Wahrung der Vertraulichkeit personenbezogener Daten verpflichtet, zu denen er im Rahmen seiner Tätigkeit Zugang erhält oder Kenntnis erlangt. Dem Vertragspartner ist es untersagt, personenbezogene Daten, also alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann, unbefugt zu verarbeiten, insbesondere zu erheben, erfassen, organisieren, ordnen, speichern, anpassen oder verändern, auslesen, abfragen, verwenden, offenzulegen durch Übermittlung, verbreiten oder eine andere Form der Bereitstellung, abgleichen oder verknüpfen, einschränken, löschen oder vernichten.

   Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung dieser Daten gestatten.

   Personenbezogene Daten müssen immer:

   a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
   b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
   c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
   d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

8. Die Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung des Auftragsverhältnisses fort.

9. Der Vertragspartner wurde darauf hingewiesen, dass die Verletzung des Schutzes personenbezogener Daten nach geltenden Datenschutzgesetzen geahndet werden kann.

10. Der Vertragspartner wird Vorschriften der Kunden der Auftraggeber über den Umgang mit vertraulichen Angelegenheiten und personenbezogenen Daten und deren Sicherung beachten.

11. Mängel im Datenschutz- oder Datensicherheitssystem sind unaufgefordert und unverzüglich der Geschäftsführung oder dem Datenschutzbeauftragten des Auftraggebers zu melden.

12. Spezielle Geheimhaltungsvereinbarungen bzw. –vorgaben (z.B. projekt- oder kundenbezogene Vereinbarungen) bleiben unberührt und gelten neben den Verpflichtungen aus dieser Verschwiegenheitsvereinbarung.

13. Dem Vertragspartner ist bekannt, dass der Auftraggeber im Verhältnis zu seinen Kunden selbst umfassend zur Verschwiegenheit verpflichtet ist und harte Sanktionen drohen (Auftragsverlust, Strafzahlungen, Schadensersatz usw.), wenn diese Pflichten durch den Auftraggeber oder den Vertragspartner verletzt werden.

14. Ein Verstoß gegen die vorstehenden Verpflichtungen kann den Auftraggeber zur außerordentlichen und ggf. fristlosen Kündigung des Vertragsverhältnisses berechtigen und Schadensersatzverpflichtungen des Vertragspartners auslösen.

Dieses Dokument beinhaltet allgemeine Geschäftsbedingungen. Sie werden durch Publikation und nach schriftlicher Einbeziehung in den Hauptvertrag wirksam (z.B. Einbeziehung durch Versand eines Links per E-Mail).

Verschwiegenheitsvereinbarung und Wahrung des Datengeheimnisses für Kunden

Zwischen unserem Unternehmen

- Anbieter -

und Ihrem Unternehmen

- Kunde -

gemeinschaftlich die - Parteien -

wird Folgendes vereinbart:

1. Die Parteien sind verpflichtet, Geschäfts- und Betriebsgeheimnisse sowie betriebliche Angelegenheiten vertraulicher Natur, die von der anderen Partei schriftlich oder mündlich als solche bezeichnet werden bzw. offensichtlich als solche zu erkennen sind, geheim zu halten und ohne ausdrückliche Genehmigung der anderen Partei keinen Dritten zugänglich zu machen. Die Geheimhaltungsverpflichtung gilt auch gegenüber Mitarbeitern der Parteien, Dritten und anderen Vertragspartnern der Parteien und deren Mitarbeitern, sofern diese mit dem betreffenden Sachverhalt nicht unmittelbar befasst sind.

   Betriebs- und Geschäftsgeheimnis ist jede Information, die

   a) weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

   b) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

   c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

   Geschäftsgeheimnis im Sinne der globalen Geschäftsgeheimnis-Gesetze und damit vertraulich sind insbesondere Informationen betreffend Preisen, Planzahlen, Umsatz-/Gewinn-/Ertragszahlen, ökonomische Kennzahlen, laufende und geplante Projekte, programmtechnische und konzeptionelle Strukturen, Analysetätigkeiten, Softwarearchitektur und Schnittstellen, Datensätze und deren Verwendung, Passwörter, Berechtigungen, Beschäftigten-, Lieferanten und Kundendaten, Daten sonstiger Geschäftspartner sowie insbesondere sämtliche vertraulichen Informationen betreffend Kunden oder Lieferanten einer Partei, zu denen die andere Partei im Rahmen der Vorbereitung und Durchführung des Auftrags oder für Kunden oder Lieferanten der anderen Partei Zugang erhalten hat, wie beispielsweise Informationen betreffend Kunden oder Lieferanten einer Partei, Geschäftsabläufe, Infrastruktur, Geschäftspläne und -produkte, Software, Programme sowie jegliche Informationen, welche die andere Partei unter Verwendung vertraulicher Informationen erarbeitet hat. Der Verschwiegenheitspflicht unterliegen nicht solche Informationen, die

jedermann zugänglich oder allgemein bekannt sind. In Zweifelsfällen hat eine Partei die Weisung der anderen Partei zur Vertraulichkeit bestimmter Tatsachen einzuholen.

2. Beide Parteien sind verpflichtet, das Bankgeheimnis, das Fernmeldegeheimnis, die Vertraulichkeit der Kommunikation, das Postgeheimnis, das Sozialgeheimnis, das Briefgeheimnis und alle anderen Geheimnisvorschriften und Gesetze zu wahren.

3. Die Verschwiegenheitspflicht gilt nicht gegenüber Dritten, soweit diesen gegenüber eine gesetzliche Offenbarungspflicht besteht. Sie gilt auch nicht gegenüber standesrechtlich zur Verschwiegenheit verpflichteten Personen, soweit die Offenbarung der geheim zu haltenden Tatsachen zur berechtigten Interessenwahrnehmung einer Partei notwendig ist.

4. Die Verschwiegenheitspflicht erstreckt sich auch auf Angelegenheiten anderer Unternehmen, mit denen die andere Partei wirtschaftlich oder organisatorisch verbunden ist.

5. Die Verpflichtung zur Verschwiegenheit besteht auch nach Beendigung des Vertragsverhältnisses fort. Sollte die nachvertragliche Verpflichtung zur Verschwiegenheit eine Partei unangemessen in ihrem beruflichen Fortkommen behindern, hat diese Partei einen Anspruch gegen die andere Partei auf Freistellung von dieser Verpflichtung.

6. Den Parteien ist bekannt, dass Geheimnisverrat nach geltenden Gesetzen zum Schutz von Geschäftsgeheimnissen strafbar sein kann.

7. Beide Parteien sind zur Wahrung der Vertraulichkeit hinsichtlich der personenbezogenen Daten verpflichtet, zu denen sie im Rahmen ihrer Tätigkeiten Zugang erhalten oder über die sie Kenntnis erlangen. Beiden Parteien ist es untersagt, personenbezogene Daten, also alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann, unbefugt zu verarbeiten, insbesondere zu erheben, erfassen, organisieren, ordnen, speichern, anpassen oder verändern, auslesen, abfragen, verwenden, offenzulegen durch Übermittlung, verbreiten oder eine andere Form der Bereitstellung, abgleichen oder verknüpfen, einschränken, löschen oder vernichten.

   Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung dieser Daten gestatten.

   Personenbezogene Daten müssen immer:

   a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
   b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
   c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
   d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick

auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

8. Die Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung des Auftragsverhältnisses fort.

9. Beide Parteien sind darüber informiert, dass die Verletzung des Schutzes personenbezogener Daten nach geltenden Datenschutzgesetzen geahndet werden kann.

10. Beide Parteien werden Vorschriften der Kunden der anderen Partei über den Umgang mit vertraulichen Angelegenheiten und personenbezogenen Daten und deren Sicherung beachten.

11. Mängel im Datenschutz- oder Datensicherheitssystem sind unaufgefordert und unverzüglich der Geschäftsführung oder dem Datenschutzbeauftragten der anderen Partei zu melden.

12. Spezielle Geheimhaltungsvereinbarungen bzw. –vorgaben (z.B. projekt- oder kundenbezogene Vereinbarungen) bleiben unberührt und gelten neben den Verpflichtungen aus dieser Verschwiegenheitsvereinbarung.

13. Den Parteien ist bekannt, dass die andere Partei im Verhältnis zu ihren Kunden selbst umfassend zur Verschwiegenheit verpflichtet ist und harte Sanktionen drohen (Auftragsverlust, Strafzahlungen, Schadensersatz usw.), wenn diese Pflichten durch eine der Parteien verletzt werden.

14. Ein Verstoß gegen die vorstehenden Verpflichtungen kann die andere Partei zur außerordentlichen und ggf. fristlosen Kündigung des Vertragsverhältnisses berechtigen und Schadensersatzverpflichtungen auslösen.

Dieses Dokument beinhaltet allgemeine Geschäftsbedingungen. Sie werden durch Publikation und nach schriftlicher Einbeziehung in den Hauptvertrag wirksam (z.B. Einbeziehung durch Versand eines Links per E-Mail).

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Agreement

VERSION A1.0, in force 21 March 2022

This IDTA 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 and signatures

Start date	see Main-Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: see Main-Agreement Trading name (if different): if applicable, see Main-Agreement Main address (if a company registered address): see Main-Agreement Official registration number (if any) (company number or similar identifier):	Full legal name: see Main-Agreement Trading name (if different): if applicable, see Main-Agreement Main address (if a company registered address): see Main-Agreement Official registration number (if any) (company number or similar identifier):

	if applicable, see Main-Agreement	if applicable, see Main-Agreement
Key Contact	Full Name (optional): if applicable, see Main-Agreement Job Title: if applicable, see Main-Agreement Contact details including email: if applicable, see Main-Agreement	Full Name (optional): if applicable, see Main-Agreement Job Title: if applicable, see Main-Agreement Contact details including email: if applicable, see Main-Agreement
Importer Data Subject Contact		Job Title: see Main-Agreement Contact details including email: see Main-Agreement
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the **Exporter** set out above Signed: see Main-Agreement Date of signature: see Main-Agreement Full name: see Main-Agreement Job title: see Main-Agreement	Signed for and on behalf of the **Importer** set out above Signed: see Main-Agreement Date of signature: see Main-Agreement Full name: see Main-Agreement Job title: see Main-Agreement

Table 2: Transfer Details

UK country's law that governs the IDTA:	England and Wales, Northern Ireland, or Scotland see Main-Agreement, or alternatively, place on the main establishment of the Exporter, or alternatively, based on the place of residence of the majority of data subjects

Primary place for legal claims to be made by the Parties	England and Wales, Northern Ireland, or Scotland see Main-Agreement, or alternatively, place on the main establishment of the Exporter, or alternatively, based on the place of residence of the majority of data subjects
The status of the Exporter	In relation to the Processing of the Transferred Data: Exporter is a Controller / or / Exporter is a Processor or Sub-Processor – based on the nature of the Main Agreement, and the Agreement with another Controller
The status of the Importer	In relation to the Processing of the Transferred Data: Importer is a Controller / or / Importer is the Exporter's Processor or Sub-Processor / or / Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller) - based on the nature of the Main Agreement, and the Agreement with another Controller or Third Party
Whether UK GDPR applies to the Importer	UK GDPR applies to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: Name of agreement: if any, see Main-Agreement Date of agreement: if any, see Main-Agreement Parties to the agreement: if any, see Main-Agreement Reference (if any): if any, see Main-Agreement **Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: Name of agreement: if any, see Main-Agreement Date of agreement: if any, see Main-Agreement

	Parties to the agreement: if any, see Main-Agreement Reference (if any): if any, see Main-Agreement **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: Name of agreement: if any, see Main-Agreement Date of agreement: if any, see Main-Agreement Parties to the agreement: if any, see Main-Agreement Reference (if any): if any, see Main-Agreement
Term	The Importer may Process the Transferred Data for the following time period: the period for which the Linked Agreement is in force
Ending the IDTA before the end of the Term	The Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: neither Party
Can the Importer make further transfers of the Transferred Data?	The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: there are no specific restrictions.

Importer may transfer on the Transferred Data	
Review Dates	Each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment.

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: none
Relevant Data Subjects	The Data Subjects of the Transferred Data are: The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.
Purpose	The Importer may Process the Transferred Data for the following purposes: To fulfil the Main-Agreement.

Table 4: Security Requirements

Security of Transmission	See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES

Security of Storage	See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES
Security of Processing	See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES
Organisational security measures	See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES
Technical security minimum requirements	See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES
Updates to the Security Requirements	The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	None
(i) Extra technical security protections	See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES
(ii) Extra organisational protections	None
(iii) Extra contractual protections	None

Commercial Clauses	see Main-Agreement

Part 4: Mandatory Clauses

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

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

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

1.2.2 Part two: Extra Protection Clauses;

1.2.3 Part three: Commercial Clauses; and

1.2.4 Part four: Mandatory Clauses.

1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.

1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.

2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. You have provided all the information required

3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.

3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:

3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and

3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA

4.1 The Parties may choose to each sign (or execute):

4.1.1 the same copy of this IDTA;

4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;

4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;

5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors

and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;

5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or

5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

6.1 This IDTA 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.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

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

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

6.9 References to:

6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;

6.9.2 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 IDTA has been signed; and

6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:

8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and

8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.

8.2 The Exporter must:

8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.

8.3 The Importer must:

8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data

when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and

8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 The Importer must ensure that at the Start Date and during the Term:

8.4.1 the Importer Information is accurate;

8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

9. Reviews to ensure the Appropriate Safeguards continue

9.1 Each Party must:

9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:

9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;

9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter's obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

12. General Importer obligations

12.1 The Importer must:

12.1.1 only Process the Transferred Data for the Purpose;

12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;

12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;

12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;

12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's

Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and

15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.2.1.1 a description of the nature of the Importer Personal Data Breach;

15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.2.1.3 likely consequences of the Importer Personal Data Breach;

15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.2.1.5 contact point for more information; and

15.2.1.6 any other information reasonably requested by the Exporter,

15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data

Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.3.1 a description of the nature of the Importer Personal Data Breach;

15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.3.3 likely consequences of the Importer Personal Data Breach;

15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.3.5 contact point for more information; and

15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.

15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

16.1.2 the third party has been added to this IDTA as a Party; or

16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or

16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or

16.1.5 the transfer is to the UK or an Adequate Country.

16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

17. Importer's responsibility if it authorises others to perform its obligations

17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).

17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.

17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.

17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

What rights do individuals have?

18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

20.5 If a Relevant Data Subject requests, the Importer must:

20.5.1 rectify inaccurate or incomplete Transferred Data;

20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;

20.5.3 cease using it for direct marketing purposes; and

20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.

20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:

20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or

20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or

20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor

21.1 Where the Importer is the Exporter's Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data

and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

26. Breaches of this IDTA

26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:

26.1.1 has breached this IDTA; or

26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer

27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.

27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and

27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

28. Breaches of this IDTA by the Exporter

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

Ending the IDTA

29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

29.1.1 at the end of the Term stated in Table 2: Transfer Details; or

29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

29.1.3 at any time that the Parties agree in writing that it will end; or

29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

29.2.1 its direct costs of performing its obligations under the IDTA; and/or

29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA 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 IDTA.

30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or

30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer; and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One's breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);

- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in

34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).

34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details

34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	**Legal definition (this is how this word or phrase must be interpreted in the IDTA)**
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: • a territory; • one or more sectors or organisations within a third country; • an international organisation; which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's 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 IDTA	The template IDTA A1.0 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 5.4.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	Processed by the Importer, including for the Exporter to carry out any TRA.
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
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.
Without Undue Delay	Without undue delay, as that phase is interpreted in the UK GDPR.

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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	see Main-Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: see Main-Agreement Trading name (if different): if applicable, see Main-Agreement Main address (if a company registered address): see Main-Agreement	Full legal name: see Main-Agreement Trading name (if different): if applicable, see Main-Agreement Main address (if a company registered address): see Main-Agreement

	Official registration number (if any) (company number or similar identifier): if applicable, see Main-Agreement	Official registration number (if any) (company number or similar identifier): if applicable, see Main-Agreement
Key Contact	Full Name (optional): if applicable, see Main-Agreement Job Title: if applicable, see Main-Agreement Contact details including email: if applicable, see Main-Agreement	Full Name (optional): if applicable, see Main-Agreement Job Title: if applicable, see Main-Agreement Contact details including email: if applicable, see Main-Agreement
Signature (if required for the purposes of Section 2)	if applicable, see Main-Agreement	if applicable, see Main-Agreement

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: see above, Additional conditions for compliance with the General Data Protection Regulation (GDPR), UK-GDPR and Confidentiality of Trade Secrets Reference (if any): if applicable, see Main-Agreement Other identifier (if any): if applicable, see Main-Agreement

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: see APPENDIX 7 – LIST OF PARTIES
Annex 1B: Description of Transfer: see APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES
Annex III: List of Sub processors (Modules 2 and 3 only): if applicable, separate list of our sub-processors must be requested separately

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 19: 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 18.
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.

Data Processing Agreement for the United Kingdom

This Data Processing Agreement is concluded on the same date as the Services Agreement (as defined below) and is concluded by and between

(1) the **Controller**, named with its Company details as a Party in the Services Agreement; and

(2) the **Processor**, named with its Company details as a Party in the Services Agreement.

(each a **Party** and together the **Parties**)

1. Preamble

The Processor is a provider of professional services (**Services**). The Parties entered into an Agreement which describes the Services provided by the Processor to or on behalf of the Controller in more detail (**Services Agreement**).

The Parties have agreed to enter into this Agreement in relation to the Processing of Personal Data by the Processor in the course of providing the Services. The terms of this Agreement are intended to apply in addition to and not in substitution of the terms of the Services Agreement.

2. Definitions and interpretation

2.1. In this Agreement the terms **Controller**, **Processor**, **Personal Data**, **Special Categories Of Personal Data**, **Processing**, **Pseudonymisation, Encryption, Personal Data Breach**, **Supervisory Authority, Categories of Data Subject, Types of Personal Data, Scope,** and **Purpose** shall have the meanings given to them by Data Protection Legislation (as defined below).

2.2. In addition to those terms, the following definitions shall apply:

Affiliates means in relation to the Controller, each and any business entity or undertaking under the Controller's direction and in relation to either Party, any entity that directly or indirectly controls, is controlled by or is under common control with that Party (where control is defined as the direct or indirect ownership or control of more than 50% of the shares or other equity securities, of an entity or of the power to direct or significantly influence the direction of the management, policies and voting interests of an entity whether by contract or otherwise).

Authorised Person means the Person(s) be nominated by the Controller from time to time in writing.

Business Day means a day other than a Saturday, Sunday or public holiday in England when banks in the City of London are generally open for business.

Data Protection Legislation means the UK-GDPR and any national laws, regulations and secondary legislation in the UK; all applicable laws and regulations relating to the Processing of Personal Data and privacy; and where applicable, the guidance and codes of practice issued by the UK Information Commissioner's Office (ICO) or any other Supervisory Authority (and the equivalent of any of the foregoing in any relevant jurisdiction).

EEA means the European Economic Area including, for the Purposes of this Agreement, the UK.

Personnel means in relation to a Party, those of its employees, workers, agents, consultants, contractors, sub-contractors, representatives or other Persons employed or engaged by that Party on whatever terms.

Sub-Processor means any entity (whether or not an Affiliate of the Processor, but excluding the Processor's Personnel) appointed by or on behalf of the Processor to process Personal Data on behalf of the Controller under this Agreement.

2.3. Clause, schedule and paragraph headings shall not affect the interpretation of this Agreement.

2.4. A **Person** includes a natural Person, corporate or unincorporated body (whether or not having separate legal personality). A reference to a **Company** shall include any Company, corporation or other body corporate, wherever and however incorporated or established.

2.5. Unless the context otherwise requires, any reference to a Party shall be deemed to include that Party's Affiliates and where an obligation is imposed on a Party under this Agreement, it will be required to procure compliance with such obligation by that Party's Affiliates where appropriate.

2.6. Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular and a reference to one gender shall include a reference to the other genders.

2.7. A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time and shall include all subordinate legislation made from time to time under that statute or statutory provision.

2.8. Unless the context otherwise requires, a reference to writing or written includes email but not fax.

2.9. Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

2.10. In the event of any ambiguity or inconsistency between the terms of this Agreement (including its Schedules) and the terms of the Services Agreement, the terms of this Agreement shall take precedence.

3. Roles and responsibilities

Schedule 1 sets out the Scope and Purpose of the Processing of Personal Data by the Processor, the duration of the Processing and the Types of Personal Data and Categories of Data Subject concerned.

4. Compliance with Data Protection Legislation

4.1. Each Party shall comply with all applicable requirements of the Data Protection Legislation. This clause is in addition to, and does not relieve any Party from complying with, a Party's obligations under the Data Protection Legislation.

4.2. Without prejudice to the generality of this clause, the Controller will ensure that it has all necessary appropriate consents and notices in place to enable the lawful transfer to and Processing of the Personal Data by the Processor in connection with the performance by the Processor of its obligations under the Services Agreement and this Agreement.

4.3. To the extent within the Controller's control having regard to the Processor's obligations under the Services Agreement and this Agreement, the Controller shall be responsible for the accuracy and quality of the Personal Data processed by the Processor under this Agreement.

4.4. The Processor shall have an ongoing obligation throughout the duration of the Services Agreement to identify and report to the Controller:

4.4.1. best practice techniques relating to the Processing of Personal Data under this Agreement; and
4.4.2. the emergence of new and evolving technologies which could improve the availability, confidentiality and/or integrity of the Processing of Personal Data under this Agreement.

5. Processing of Personal Data by the Processor

5.1. The Processor shall only process Personal Data:

5.1.1. for the Purposes expressly specified in the Services Agreement;
5.1.2. otherwise in accordance with the Controller's documented instructions as given by an Authorised Person,

unless the Processor is required by any applicable law to which the Processor is subject, to process Personal Data for any other Purposes (in which case the Processor shall, to the extent permitted by such applicable law, inform the Controller of such legal requirement before undertaking such Processing).

5.2. The Controller shall ensure that any Authorised Person is fully aware of the terms of the Services Agreement and this Agreement such that the Processor shall be entitled to assume that any instruction given by any Authorised Person to the Processor shall be given with the Controller's full authority. The Controller further acknowledges and agrees that the Processor shall not be under any duty to investigate the completeness, accuracy or sufficiency of any instructions given to it by any Authorised Person.

6. Processor's Personnel

6.1. The Processor shall take reasonable steps to ensure the reliability of those of its Personnel who may have access to any Personal Data.

6.2. The Processor shall ensure that those of its Personnel authorised to process Personal Data under this Agreement:

6.2.1. are aware of the confidential nature of the Personal Data;
6.2.2. are bound by obligations of confidentiality by virtue of a written Agreement between the Processor and such Persons; and
6.2.3. have received appropriate training on the handling of Personal Data and on their responsibilities in relation to the Processing of Personal Data.

6.3. The Processor shall implement appropriate technical and organisational measures to ensure that those of its Personnel only have access to such part or parts of the Personal Data as is strictly necessary for the performance of their duties and obligations.

7. Security of the Processing

7.1. Taking into account the state of the art, the costs of implementation and the nature, Scope, context and Purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the data subjects the Processor shall, in relation to the Processing of Personal Data under this Agreement, implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate:

7.1.1. the Pseudonymisation and Encryption of Personal Data;
7.1.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
7.1.3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
7.1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

7.2. In assessing the appropriate level of security, the Processor shall take into account any risks that are presented by the Processing, in particular, from a Personal Data Breach.

7.3. The Processor shall implement the specific security measures set out in **Schedule 2**. The Processor may add to, amend, or replace the specific security measures for security reasons and shall notify the Controller in writing where it has done so.

8. Sub-Processors

8.1. The Controller hereby authorises the Processor to appoint Sub-Processors (**General Written Authorisation**). The Processor shall name all its Sub-Processors to the Controller prior to initiation of Processing.

8.2. With respect to each Sub-Processor appointed by the Processor under General Written Authorisation, the Processor shall:

8.2.1. undertake appropriate due diligence prior to the Processing of Personal Data by such Sub-Processor to ensure that it is capable of providing the level of protection for Personal Data required by the terms of the Services Agreement and this Agreement;
8.2.2. enter into a written Agreement with the Sub-Processor incorporating terms which are substantially similar (and no less onerous) than those set out in this Agreement and which meets the requirements stipulated in article 28(3) of the UK-GDPR; and
8.2.3. as between the Controller and the Processor, remain fully liable to the Controller for all acts or omissions of such Sub-Processor as though they were its own.

8.3. To the extent that the Processor has already appointed any Sub-Processors prior to the Processing of any Personal Data under this Agreement, the Processor shall ensure that its obligations under clause 8.2 are met as soon as practicable.

8.4. Where the Processor proposes any changes concerning the addition or replacement of any Sub-Processor, it shall notify the Controller in writing as soon as reasonably practicable prior to implementing such change specifying:

8.4.1. the name of any Sub-Processor which it proposes to add or replace;
8.4.2. the Processing activity or activities affected by the proposed change;
8.4.3. the reasons for the proposed change; and
8.4.4. the proposed date for implementation of the change.

8.5. If within thirty (30) days of receipt of a notice under clause 8.4 the Controller (acting reasonably and in good faith) notifies the Processor in writing of any objections to the proposed change, the Parties shall use their respective reasonable endeavours to resolve the Controller's objections. Where such resolution cannot be agreed within thirty (30) days of the Processor's receipt of the Controller's objections (or such longer period as the Parties may agree in writing) the Controller may, notwithstanding the terms of the Services Agreement, serve written notice on the Processor to terminate the Services Agreement (to the extent that the provision of the Services is or would be affected by the proposed change).

8.6. The Processor shall, upon the Controller's request, provide the Controller with copies of any Agreements between the Processor and its Sub-Processors (which may be redacted to remove information which is confidential to the Processor and/or its Sub-Processors and which is not relevant to the terms of this Agreement).

9. Rights of data subjects

9.1. Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights under the Data Protection Legislation.

9.2. Without prejudice to the generality of clause 9.1, the Processor shall implement measures intended to uphold the rights of data subjects.

9.3. The Processor shall:

9.3.1. promptly and in any case within one (1) Business Day] notify the Controller if it (or any of its Sub-Processors) receives a request from a data subject under the Data Protection Legislation in respect of any Personal Data processed by the Processor under the terms of the Services Agreement or this Agreement; and
9.3.2. give to the Controller its full co-operation and assistance in relation to any request made by a data subject to have access to their Personal Data.

10. Notification of Personal Data Breaches

10.1. The Processor shall notify the Controller without undue delay after becoming aware of any Personal Data Breach affecting the Personal Data processed by the Processor under this Agreement, providing sufficient information to enable the Controller to evaluate the impact of such Personal Data Breach and to meet any obligations on the Controller to report the Personal Data Breach to a Supervisory Authority and/or notify the affected data subjects in accordance with the Data Protection Legislation.

10.2. The Processor shall provide the Controller with such assistance as the Controller may reasonably request and take such reasonable commercial steps as the Controller may request in order to evaluate, investigate, mitigate and remediate any Personal Data Breach (including, where applicable, communicating any Personal Data Breach to affected data subjects).

11. Data Protection Impact Assessments and Prior Consultation

The Processor shall provide the Controller with such assistance as the Controller may reasonably request with any data protection (or privacy) impact assessments and prior consultation with any Supervisory Authority or other competent authorities which the Controller considers necessary pursuant to Articles 35 and 36 of the UK-GDPR respectively. The Processor's assistance shall, in each case, be limited to the Processing of Personal Data under this Agreement.

12. Obligations upon expiry or termination of the Services Agreement

12.1. Notwithstanding the Processor's obligations under the Services Agreement following its expiry or termination, the Processor shall promptly and in any event within thirty (30) days of the expiry or termination of the Services Agreement, at the Controller's option (given by any Authorised Person) either delete or return (in such format and on such media or by such means as the Parties shall agree in writing) all copies of the Personal Data processed by the Processor and/or its Sub-Processors on behalf of the Controller under this Agreement.

12.2. Where the Controller has instructed the Processor to delete the Personal Data under clause 12.1, the Processor shall do so in accordance with best industry practice for the reliable and secure deletion of data for the secure destruction of confidential material.

12.3. The Processor (and those of its Sub-Processors, as appropriate) may retain a copy of the Personal Data processed by it under this Agreement to the extent required by any applicable law to which the Processor (or any Sub-Processor) is subject and only for such period as shall be required by such applicable law. Where applicable, the Processor shall notify the Controller of such requirement and shall ensure that such Personal Data are kept confidential and not processed for any other Purpose.

12.4. The Controller may require the Processor to provide a written certificate confirming that it has complied with its obligations under this clause 12.

13. Record-keeping requirements and audit rights

13.1. The Processor shall maintain a record of all categories of processing activities carried out by it on behalf of the Controller under this Agreement in accordance with Data Protection Legislation (**Processing Records**).

13.2. The Processor shall permit the Controller, any Authorised Person or any other auditor mandated by the Controller, on reasonable notice and during the Processor's normal business hours (but without notice, in the case of any reasonably suspected breach of this clause 13) to:

13.2.1. gain access to, and take copies of, the Processing Records and any other information held at the Processor's premises; and

13.2.2. inspect all Processing Records, documents and electronic data and the Processor's systems, facilities and equipment,

for the Purpose of auditing and certifying the Processor's compliance with its obligations under this Agreement. Such audit rights may be exercised only once in any calendar year during the term of the Services Agreement and for a period of three years following the expiry or termination of the Services Agreement.

13.3. The Processor shall give all necessary assistance to the conduct of any audits under clause 13.2.

13.4. The Processor further agrees that it shall provide the Controller with such assistance as it may reasonably request in connection with any compulsory or voluntary audit or inspection by a Supervisory Authority or other competent authority.

13.5. The Processor shall immediately inform the Controller if, in its opinion, any instruction infringes the Data Protection Legislation.

14. Transfers of Personal Data outside of the EEA

14.1. For the Purposes of this clause 14, the **Transfer of any Personal Data** shall include:

14.1.1. storing Personal Data on servers located or co-located outside the EEA;
14.1.2. appointing any Sub-Processor which is located outside the EEA (in accordance with clause 8; or
14.1.3. granting access rights to any of the Processor's Personnel who are located outside the EEA.

14.2. The Processor shall not transfer any Personal Data processed under this Agreement outside of the EEA except with the Controller's prior written consent and provided that the Controller is satisfied that the following conditions have been met:

14.2.1. the Controller, the Processor and/or any Sub-Processor (as appropriate) have (1) the International Data Transfer Agreement (published by the ICO) or (2) the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers (published by the ICO) and the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council or Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council) in place;
14.2.2. the data subject has enforceable rights and effective legal remedies in relation to the Processing of Personal Data relating to them; and
14.2.3. the Processor and/or Sub-Processor (as appropriate) complies with its obligations under the Data Protection Legislation by providing an adequate level of protection for any Personal Data that are transferred.

15. General provisions

15.1. Term and termination: Except in respect of any provision of this Agreement that expressly or by implication is intended come into or continue in force on or after the expiry or termination of the Services Agreement, this Agreement shall be coterminous with the Services Agreement.

15.2. Third Party rights: A Person who is not a Party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any terms of this Agreement.

15.3. Severance

15.3.1. If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Agreement.

15.3.2. If any provision or part-provision of this Agreement is invalid, illegal or unenforceable, the Parties shall negotiate in good faith to amend such provision so that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the intended commercial result of the original provision.

15.4. Variation: Except as expressly provided in this Agreement, no variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

15.5. Governing law: This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law.

15.6. Jurisdiction: Each Party irrevocably agrees that the English courts shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).

Schedule 1 – Summary of the Processing activities

1. Processing by the Processor

   a. Scope of the Processing

      See Services Agreement

   b. Purpose of the Processing

      See Services Agreement

   c. Duration of the Processing

      Duration of Services Agreement

2. Types of Personal Data

   Customer data, data of potential customers, employee data, data of business partners, supplier data.

3. Categories of Data Subject

   Customers, potential customers, employees, business partners, suppliers.

See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES

CCPA-CPRA CONTRACTOR AGREEMENT

This CCPA-CPRA Contractor Agreement is concluded on the same date as the Services Agreement (as defined below) and is concluded by and between

(1) the **Business**, named with its contact details as a Party in the Services Agreement; and

(2) the **Contractor**, named with its contact details as a Party in the Services Agreement.

For the purpose of this **Agreement** the term **Contractor** shall include an **Independent Contractor** and/or a **Service Provider** and/or a **Third Party** as defined by CCPA where required to include such parties and/or to allow the conclusion of this Agreement with them as contractual partners.

(each a **Party** and together the **Parties**)

1. Preamble

1.1. The Contractor is a provider of professional Services (**Services**). The Parties entered into an Agreement which describes the Services provided by the Contractor to or on behalf of the Business in more detail (**Services Agreement**).

1.2. The Parties have agreed to enter into this Agreement in relation to the Processing of Personal Information by the Contractor in the course of providing the Services. The terms of this Agreement are intended to apply in addition to and not in substitution of the terms of the Services Agreement.

2. Definitions and interpretation

2.1. In this Agreement, in CCPA related written or verbal communication, in the Services Agreement and in any of its amendments the terms **Advertising and Marketing, Aggregate Consumer Information, Biometric Information, Business, Business Associate, Business Controller Information, Business Purpose, Collected, Collection, Collects, Commercial Credit Reporting Agency, Commercial Purposes, Common Branding, Consent, Consumer, Consumer Privacy Fund, Contractor, Control, Controlled, Covered Person, Cross-Context Behavioral Advertising, Dark Pattern, Deidentified, Designated Methods For Submitting Requests, Device, Director, Family, Fraudulent Concealment, Health Care Operations, Homepage, Household, Identifiable Private Information, Independent Contractor, Individually Identifiable Health Information, Infer, Inference, Intentionally Interacts, Management Employee, Medical Information, Nonpersonalized Advertising, Officer, Owner, Ownership Information, Patient Information, Payment, Person, Personal Information, Precise Geolocation, Processing, Profiling, Protected Health Information, Provider Of Health Care, Pseudonymization, Pseudonymize, Publicly Available, Reidentify, Research, Right To Opt-Out, Sale, Security and Integrity, Sell, Selling, Sensitive Personal Information, Service, Services, Share, Shared, Sharing, Sold, Specific Pieces Of Information, Specific Pieces Of Information Obtained From The Consumer, Third Party, Treatment, Unique Identifier, Unique Personal Identifier, Vehicle Information, Verifiable Consumer Request, Vessel Dealer, Vessel Information** and **all other terms**

defined by or under Data Protection Legislation shall have the meanings given to them by Data Protection Legislation.

2.2. In addition to those terms, the following definitions shall apply:

Affiliate or **Affiliates** means each and any Person or undertaking under the Parties direction and in relation to either Party, any Person that directly or indirectly controls, is controlled by or is under common control with that Party (where control is defined as the direct or indirect ownership or control of at least 50% of the shares (including joint-ventures and partners in which a business has at least a 40% interest) or other equity securities, of a Person or of the power to direct or significantly influence the direction of the management, policies and voting interests of a Person whether by contract or otherwise).

Authorized Person means the Person(s) be nominated by the Business from time to time in writing.

California Consumer Privacy Act or **CCPA** means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended or superseded from time to time.

California Privacy Rights Act or **CPRA** means the California Privacy Rights Act of 2020, (2020 Cal. Legis. Serv. Proposition 24, codified at Cal. Civ. Code §§ 1798.100 et seq.), and its implementing regulations, as amended or superseded from time to time.

Data Protection Legislation means CCPA and CPRA as well as any regulation adopted, published, administered, implemented, or enforced by the California Privacy Protection Agency or by the Attorney General to further the purposes of CCPA and/or CPRA, and any related case-law.

Natural Person means any living individual that is a subject to the Data Protection Legislation.

Personnel means in relation to a Party an employee of, a Management Employee of, Owner of, Director of, Officer of, Medical Staff Member of, or other Natural Person of that Party on whatever terms employed or engaged.

Sub-Contractor means any other Person (whether or not an Affiliate of the Contractor, but excluding the Contractor's Personnel) appointed by or on behalf of the Contractor or its Sub-Contractors to Process Personal Information for a Business Purpose on behalf of the Business under this Agreement or the Services Agreement, and any other Person engaged to assist the Contractor in Processing Personal Information for a Business Purpose on behalf of the Business, and any other Person engaged by the Contractor engages another Person to assist in Processing Personal Information for a Business Purpose.

2.3. For the purpose of this Agreement the term CCPA shall include CPRA.

2.4. Clause, schedule and paragraph headings shall not affect the interpretation of this Agreement.

2.5. A **Person** shall include a Natural Person, corporate or unincorporated body (whether or not having separate legal personality).

2.6. A reference to a **Company** shall include any Company, corporation or other body corporate, partnership, sole proprietorship, nonprofit, or government agency wherever and however incorporated or established.

2.7. Unless the context otherwise requires, any reference to a Party shall be deemed to include that Party's Affiliates and where an obligation is imposed on a Party under this Agreement, it will be required to procure compliance with such obligation by that Party's Affiliate where appropriate. For the avoidance of doubt, compliance shall be ensured by the Party that is affiliated with an Affiliate.

2.8. Unless the context otherwise requires, words in the singular shall include the plural and, in the plural, shall include the singular and a reference to one gender shall include a reference to the other genders.

2.9. A reference to a statute or statutory provision is a reference to it as amended, superseded, extended or re-enacted from time to time and shall include all subordinate legislation made from time to time under that statute or statutory provision, and the related case-law.

2.10. Unless the context otherwise requires, a reference to writing or written includes email but not fax.

2.11. Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

3. Scope of this Agreement

This Agreement shall apply only where, and to the extent that, the Contractor Processes Personal Information that is subject to Data Protection Legislation on behalf of the Business as a Contractor in course of providing Services pursuant to the Services Agreement.

4. Compliance with Data Protection Legislation

4.1. Each Party shall comply with all applicable requirements of Data Protection Legislation.

4.2. Without prejudice to the generality of this clause, the Business will ensure that it has all necessary appropriate Consents and notices in place to enable the lawful transfer to and Processing of the Personal Information by the Contractor in connection with the performance of the Contractor's obligations under the Services Agreement and this Agreement.

4.3. To the extent within the Business's Control having regard to the Contractor's obligations under the Services Agreement and this Agreement, the Business shall be responsible for the accuracy and quality of the Personal Information Processed by the Contractor under the Services Agreement and this Agreement.

5. Specification of the Personal Information which is disclosed to and/or Processed by the Contractor (1798.100 (d) (1) CCPA)

5.1. The Personal Information which is disclosed by the Business for limited and specified purposes are:

Types of Personal Information: Customer data, data of potential customers, employee data, data of business partners, supplier data, consumer data.

Categories of Data Subjects: Customers, potential customers, employees, business partners, suppliers, consumers.

Limited and specified purposes: To fulfill the contractual obligations described in the Services Agreement.

6. General obligations of the Contractor (1798.140 (j) (1) and (ag) (1) CCPA)

6.1. The Contractor shall not Sell or Share Personal Information.

6.2. The Contractor shall not retain, use, or disclose the Personal Information for any purpose other than for the Business Purposes specified in the Services Agreement or in this Agreement, including retaining, using, or disclosing the Personal Information for a Commercial Purpose other than the Business Purposes specified in the Services Agreement or in this Agreement, or as otherwise permitted by Data Protection Legislation.

6.3. The Contractor shall not retain, use, or disclose the information outside of the direct Business relationship between the Contractor and the Business.

6.4. The Contractor shall not combine the Personal Information that the Contractor receives pursuant to the Services Agreement with the Business with Personal Information that it receives from or on behalf of another Person or Persons, or Collects from its own interaction with the Consumer, provided that the Contractor may combine Personal Information to perform any Business Purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185 CCPA, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140 CCPA and in regulations adopted by the California Privacy Protection Agency.

6.5. The Contractor certifies that it understands the restrictions above and that the Contractor will comply with them.

6.6. The Contractor permits the Business to monitor the Contractor's compliance with the Services Agreement and this Agreement through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

6.7. The Contractor shall only Process Personal Information for the purposes expressly specified in the Services Agreement or this Agreement or otherwise in accordance with the Business's documented instructions as given by an Authorized Person, unless the Contractor is required by any applicable law to which the Contractor is subject, to Process Personal Information for any other purposes, in which case the Contractor shall, to the extent permitted by such applicable law, inform the Business of such legal requirement before undertaking such Processing.

7. Sub-Contractor (1798.140 (j) (2) and (ag) (2) CCPA)

7.1. If the Contractor engages any other Person to assist it in Processing Personal Information for a Business Purpose on behalf of the Business, or if any other Person engaged by the Contractor engages another Person to assist in Processing Personal Information for that Business Purpose, it shall notify the Business of that engagement, and the engagement shall be pursuant to the Services Agreement binding the other Person to observe all the requirements set forth in paragraph (1) of subdivision (j) of Section 1798.140 CCPA and/or paragraph (1) of subdivision (ag) of Section 1798.140 CCPA.

7.2. The Contractor has the Business's general authorization for the engagement of Sub-Contractor's from an agreed list that is subject to notification, and from time to time, after changes have been occurred, to re-notification. The Contractor shall specifically inform in

writing the Business of any intended changes of that list through the addition or replacement of Sub-Contractor's at least thirty (30) days in advance, thereby giving the Business sufficient time to be able to object to such changes prior to the engagement of the concerned Sub-Contractor(s). The Contractor shall provide the Business with the information necessary to enable the Business to exercise the right to object.

7.3. Where the Contractor engages a Sub-Contractor for carrying out specific processing activities for a Business Purpose on behalf of the Business, it shall do so by way of a contract which imposes on the Sub-Contractor, in substance, the same privacy obligations as the ones imposed on the Contractor in accordance with the Services Agreement and this Agreement and Data Protection Legislation. The Contractor shall ensure that the Sub-Contractor complies with the obligations to which the Contractor is subject pursuant to the Services Agreement and this Agreement and to Data Protection Legislation.

7.4. At the Business's request, the Contractor shall provide a copy of such a Sub-Contractor agreement and any subsequent amendments to the Business. To the extent necessary to protect business secrets or other confidential information, including Personal Information, the Contractor may redact the text of the agreement prior to sharing the copy.

7.5. The Contractor shall remain fully responsible to the Business for the performance of the Sub-Contractor's obligations in accordance with its contract with the Contractor. The Contractor shall notify the Business of any failure by the Sub-Contractor to fulfill its contractual obligations.

7.6. The Contractor shall with regards to any Sub-Contractor undertake appropriate due diligence prior to Processing of Personal Information that is Processed for a Business Purpose on behalf of the Business by the Sub-Contractor to ensure that the Sub-Contractor is capable of providing the level of protection for Personal Information as it is required by the Services Agreement, this Agreement and Data Protection Legislation.

7.7. The Contractor shall ensure that the Personnel of all its Sub-Contractors and their other Sub-Contractors and all individuals responsible for handling Consumer inquiries about the Business' privacy practices or the Business' compliance with Data Protection Legislation are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and 1798.130 CCPA, and how to direct Consumers to exercise their rights under those sections (see paragraph (6) of subdivision (a) of Section 1798.130).

8. Obligation of Contractor to comply with applicable obligations (1798.100 (d) (2) CCPA)

8.1. The Contractor is obliged to comply with all applicable obligations of, and to provide the same level of privacy protection as required by Data Protection Legislation.

8.2. The Contractor certifies to be, and to take from time to time all steps to stay at all times, in full compliance with Data Protection Legislation whenever acting as a Contractor on behalf of the Business as well as when acting as a Business in the meaning given in subdivision (d) of Cal. Civ. Code 1798.140 for its own Commercial Purposes and/or Business Purposes whenever the Contractor is Processing Personal Information of Personnel of the Business.

9. Right to help ensure compliance with Business' obligations (1798.100 (d) (3) CCPA)

9.1. The Contractor grants the Business the right to take reasonable and appropriate steps to help ensure that the Contractor uses the Personal Information transferred in a manner consistent with the Business' obligations under Data Protection Legislation.

10. Right to audit (1798.140 (j) (1) (C) CCPA)

10.1. The Contractor permits the Business, any Authorized Person or any other auditor mandated by the Business, on reasonable notice and during the Contractor's normal Business hours (but without notice, in the case of any reasonably suspected breach of this Agreement) to (a) gain access to, and take copies of, the processing records and any other information held at the Contractor's premises; and (b) inspect documents and electronic data and the Contractor's systems, facilities and equipment, for the purpose of auditing and certifying the Contractor's compliance with its obligations under the Services Agreement and this Agreement.

10.2. Such audit rights may be exercised only once in any calendar year during the term of the Services Agreement and for a period of three years following the expiry or termination of the Services Agreement. The Contractor shall give all necessary assistance to the conduct of any audits.

10.3. The Contractor further agrees that it shall provide the Business with such assistance as it may reasonably request in connection with any compulsory or voluntary audit or inspection by the California Privacy Protection Agency or by the Attorney General.

11. Notification of failure to comply with Data Protection Legislation (1798.100 (d) (4) CCPA)

11.1. The Contractor shall notify the Business if it makes the determination that it can no longer meet its obligations under Data Protection Legislation.

12. Stop and remediate unauthorized use of Personal Information (1798.100 (d) (5) CCPA)

12.1. The Contractor grants the Business the right, upon notice, including under Section 1798.100 (d) (4) CCPA, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information.

13. Deletion of Consumer's Personal Information (1798.105 (c) (3) and (d) CCPA)

13.1. The Contractor shall cooperate with the Business in responding to a Verifiable Consumer Request, and at the direction of the Business, shall delete, or enable the Business to delete and shall notify any of its own Service Providers or Contractors to delete Personal Information about the Consumer Collected, Used, Processed, or Retained by the Contractor.

13.2. The Contractor shall notify any Service Providers, Contractors, or Third Parties who may have accessed Personal Information from or through the Contractor, unless the information was accessed at the direction of the Business, to delete the Consumer's Personal Information unless this proves impossible or involves disproportionate effort.

13.3. The Contractor shall not be required to comply with a deletion request submitted by the Consumer directly to the Contractor to the extent that the Contractor has Collected, Used, Processed, or Retained the Consumer's Personal Information in its role as a Contractor to the Business.

13.4. The Contractor acting pursuant to its Services Agreement with the Business, another Service Provider, or another Contractor, is not required to comply with a Consumer's request to delete the Consumer's Personal Information if it is reasonably necessary for the Business or

Contractor to maintain the Consumer's Personal Information in order to (1) complete the transaction for which the Personal Information was Collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the Consumer, or reasonably anticipated by the Consumer within the context of a Business' ongoing Business relationship with the Consumer, or otherwise perform a contract between the Business and the Consumer, or (2) help to ensure security and integrity to the extent the use of the Consumer's Personal Information is reasonably necessary and proportionate for those purposes, or (3) debug to identify and repair errors that impair existing intended functionality, or (4) exercise free speech, ensure the right of another Consumer to exercise that Consumer's right of free speech, or exercise another right provided for by law, or (5) comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code, or (6) engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the Business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the Consumer has provided informed Consent, or (7) enable solely internal uses that are reasonably aligned with the expectations of the Consumer based on the Consumer's relationship with the Business and compatible with the context in which the Consumer provided the information, or (8) comply with a legal obligation.

14. Sell or Share of Personal Information by another Service Provider, another Contractor or Third Party (1798.115 (d) CCPA)

14.1. The Contractor shall contractually prevent any other Service Provider, or other Contractor or Third Party from Selling or Sharing Personal Information about a Consumer that has been Sold to, or Shared with, the other Service Provider, or other Contractor or the Third Party by the Contractor unless the Consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120 CCPA.

14.2. Where the Contractor acts, based on the relationship between the Business to a client of the Business (for the avoidance of doubt, where the Business is a Contractor for another Business) as another Service Provider, or other Contractor or Third Party, the Contractor shall not Sell or Share Personal Information about a Consumer that has been Sold to, or Shared with, the Contractor by the Business, unless the Consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120 CCPA.

15. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information (1798.121 (a) and (c) CCPA)

15.1. In case the Contractor assists the Business in performing the purposes authorized by subdivision (a) of Section 1798.121 CCPA, the Contractor shall not use the Sensitive Personal Information after it has received instructions from the Business and to the extent it has actual knowledge that the Personal Information is Sensitive Personal Information for any other purpose.

15.2. The Contractor shall limit its use of the Consumer's Sensitive Personal Information that are Processed on behalf of the Business under this Agreement to that use which is necessary to perform the Services or provide the goods, and shall Process only in accordance with documented instructions given by the Business. The Contractor shall not disclose the Consumer's sensitive Personal Information to any Third Party.

16. Disclosure, Correction, and Deletion requirements (1798.130 CCPA)

16.1. In case the Business receives a Verifiable Consumer Request pursuant to Section 1798.110 CCPA or 1798.115 CCPA the Contractor shall assist the Business in answering such request.

16.2. The Contractor shall not comply with a Verifiable Consumer Request received directly from a Consumer or a Consumer's Authorized Agent, pursuant to Section 1798.110 CCPA or 1798.115 CCPA, to the extent that the Contractor has Collected Personal Information about the Consumer in its role as a Contractor. In such case the Contractor shall inform the Business without undue delay about receiving the Verifiable Consumer Request.

16.3. The Contractor shall provide assistance to the Business with respect to the Business' response to a Verifiable Consumer Request, including, but not limited to, by providing to the Business the Consumer's Personal Information in the Contractor's possession, which the Contractor obtained as a result of providing Services to the Business, and by correcting inaccurate information or by enabling the Business to do the same.

16.4. The Contractor shall disclose and deliver the required information to the Business free of charge, correct inaccurate Personal Information, or delete a Consumer's Personal Information, based on the Consumer's request, within fifteen (15) days of receiving a Request from the Business.

16.5. The Contractor shall assist the Business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) to (f), inclusive, of Section 1798.100 CCPA, taking into account the nature of the Processing.

17. General Assistance by the Contractor, Assistance with Consumer Rights

Whenever required, the Contractor shall assist the Business to comply with Data Protection Legislation, including, but not limited to, assisting to comply with the obligations imposed on Businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.125, 1798.130, and 1798.135 CCPA.

18. Opt-Out and Advertising and Marketing (1798.140 (e) (6) CCPA)

18.1. The Contractor shall not combine the Personal Information of opted-out Consumers that the Contractor receives from, or on behalf of, the Business with Personal Information that the Contractor receives from, or on behalf of, another Person or Persons or Collects from its own interaction with the Consumer for the purpose of providing advertising and marketing to the Consumer.

19. Processing of other Personal Information by the Business and the Contractor for their own Business Purposes (1798.145 (m) (1) and (n) (1) CCPA)

19.1. The Business is collecting and Processing Personal Information about Natural Persons in the course of these Natural Persons acting as a job applicant to, employee of, Owner of, Director of, Officer of, Medical Staff Member of, Independent Contractor of, another Service Provider of, another Contractor of, or Third Party of the Contractor or its Sub-Contractors to the extent that the Natural Person's Personal Information is Collected and used by the Business solely within the context of the Natural Person's role or former role as a job applicant to, employee of, Owner of, Director of, Officer of, Medical Staff Member of, an Independent Contractor of, another

Service Provider of, another Contractor of, or Third Party of the Contractor and/or its Sub-Contractors. The Personal Information may include, but is not limited to, emergency contact information and information that is necessary for the Business to retain to administer benefits for another Natural Person.

19.2. The Business is collecting and Processing Personal Information reflecting written or verbal communications or transactions between the Business and the Consumer, where the Consumer is a Natural Person who acted or is acting as a job applicant to, an employee, Owner, Director, Officer, or Independent Contractor, another Service Provider of, another Contractor of, or Third Party of a Company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transactions with the Business occur solely within the context of the Business conducting due diligence regarding, or providing or receiving a product or service to or from such Company, partnership, sole proprietorship, nonprofit, or government agency.

19.3. The Contractor shall inform any job applicant to, employee of, Owner of, Director of, Officer of, Medical Staff Member of, Independent Contractor of, another Service Provider of, another Contractor of, or Third Party of such Company, partnership, sole proprietorship, nonprofit, or government agency that is engaged with the Contractor for a Business Purpose on behalf of the Business, the Contractor and/or its Sub-Contractors about the transparency document published by the Business on its Homepage that contains information in regards to obligations imposed on Businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.125, 1798.130, and 1798.135 CCPA for these groups of Natural Persons.

19.4. The Contractor shall publish a document on its Homepage that contains information in regards to the obligations imposed on Businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.125, 1798.130, and 1798.135 CCPA and inform any job applicant to, employee of, Owner of, Director of, Officer of, Medical Staff Member of, Independent Contractor of, another Service Provider of, another Contractor of, or Third Party of the Business of whose Personal Information is Collected or Processed by the Contractor for its own Business Purposes about its own publication.

20. Reliability of and contract with the Contractor's Personnel, access limitation, training, and information requirements

20.1. The Contractor shall take reasonable steps to ensure reliability of those of its Personnel who may have access to any Personal Information that is Processed for a Business Purpose on behalf of the Business.

20.2. The Contractor shall ensure that those of its Personnel authorized to Process Personal Information under the Service Agreement or this Agreement (a) are aware of the confidential nature of the Personal Information, and (b) are bound by obligations of confidentiality by virtue of a written contract between the Contractor and such Persons; and (c) have received appropriate training on the handling of Personal Information and on their responsibilities in relation to the Processing of Personal Information.

20.3. The Contractor shall implement reasonable security procedures and practices as well as technical and organizational measures to ensure that those of its Personnel only have access to such part or parts of the Personal Information that is Processed for a Business Purpose on behalf of the Business as is strictly necessary for the performance of their duties and obligations.

20.4. The Contractor shall ensure that its Personnel and all individuals responsible for handling Consumer inquiries about the Business' privacy practices or the Business' compliance with Data Protection Legislation are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and 1798.130 CCPA, and how to direct Consumers to exercise their rights under those sections (see paragraph (6) of subdivision (a) of Section 1798.130).

21. Reasonable security procedures and practices (1798.150 (a) (1) CCPA)

21.1. Where appropriate and/or required to protect the rights and freedoms of Natural Persons, the Contractor shall encrypt and/or redact Personal Information that is Processed for a Business Purpose on behalf of the Business, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 CCPA.

21.2. To the extend such Personal Information is Processed for a Business Purpose on behalf of the Business, the Contractor shall encrypt email addresses, passwords, security questions and security answers that would permit access to an account.

21.3. The Contractor shall implement and maintain at all times reasonable security procedures and practices appropriate to the nature of the information to protect all Personal Information that is Processed for a Business Purpose on behalf of the Business, pursuant to Section 1798.81.5 CCPA.

21.4. The Contractor has implemented reasonable security procedures and practices and published them on its Homepage and/or communicated them to the Business. The Contractor may add to, amend, or replace the reasonable security procedures and practices for security reasons and shall notify the Business in writing where it has done so at least ten (10) days before such changes are in effect, thereby giving the Business sufficient time to be able to object to such changes prior to them becoming effective. The Contractor shall provide the Business with the information necessary to enable the Business to exercise the right to object.

21.5. The Contractor shall, in relation to the Personal Information that is Processed for a Business Purpose on behalf of the Business, ensure ongoing confidentiality, integrity, availability and resilience of processing systems and Services, and the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident.

22. Liability and indemnification (1798.145. (i) (1) and (2) CCPA)

22.1. The Business shall not be liable under CCPA if the Contractor receiving Personal Information from the Business uses it in violation of the restrictions set forth in CCPA. At the time of disclosing the Personal Information, the Business does not have actual knowledge, or reason to believe, that the Service Provider or Contractor intends to commit such a violation.

22.2. The Contractor agrees to indemnify, defend, and hold harmless the Business from and against any loss, cost, or damage of any kind (including reasonable outside attorneys' fees) to the extent arising out of any breach of Data Protection Legislation by the Contractor, and/or its negligence or willful misconduct.

23. Obligations upon expiry or termination of the Services Agreement

23.1. Notwithstanding the Contractor's obligations under the Services Agreement following its expiry or termination, the Contractor shall promptly and in any event within thirty (30) days of the expiry or termination of the Services Agreement, at the Business's option (given by any Authorized Person) either delete or return (in such format and on such media or by such means as the Parties shall agree in writing) all copies of the Personal Information Processed by the Contractor and/or its Sub-Contractors for a Business Purpose on behalf of the Business under this Agreement or the Services Agreement.

23.2. Where the Business has instructed the Contractor to delete the Personal Information, the Contractor shall do so in accordance with best industry practices for the reliable and secure deletion of data or for the secure destruction of confidential material.

23.3. The Contractor (and those of its Sub-Contractors, as appropriate) may retain a copy of the Personal Information Processed for a Business Purpose on behalf of the Business under this Agreement or the Services Agreement to the extent required by any applicable law to which the Contractor (or any Sub-Contractor) is subject and only for such period as shall be required by such applicable law. Where applicable, the Contractor shall notify the Business of such requirement and shall ensure that such Personal Information are kept confidential and not Processed for any other purpose.

23.4. The Business may require the Contractor to provide a written certificate confirming that it has complied with its obligations under this paragraph.

24. Notification of Personal Information Security Breaches

24.1. The Contractor shall notify the Business without undue delay after becoming aware of a Personal Information Security Breach affecting the Personal Information Processed for a Business Purpose on behalf of the Business under this Agreement or the Services Agreement, providing sufficient information to enable the Business to evaluate the impact of such Personal Information Security Breach and to meet any obligations of the Business in accordance with Data Protection Legislation.

24.2. The Contractor shall provide the Business with such assistance as the Business may reasonably request and take such reasonable commercial steps as the Business may request in order to evaluate, investigate, mitigate and remediate any Personal Information Security Breach (including, where applicable, communicating any Personal Information Security Breach to affected Consumers).

25. General provisions

25.1. Term and termination: Except in respect of any provision of this Agreement that expressly or by implication is intended come into or continue in force on or after the expiry or termination of the Services Agreement, this Agreement shall be coterminous with the Services Agreement.

25.2. Third Party rights: A Person who is not a Party to this Agreement shall not have any rights to enforce any terms of this Agreement.

25.3. Severance: If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this

Agreement. If any provision or part-provision of this Agreement is invalid, illegal or unenforceable, the Parties shall negotiate in good faith to amend such provision so that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the intended commercial result of the original provision.

25.4. Variation: Except as expressly provided in this Agreement, no variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorized representatives) or otherwise accepted by the Parties.

25.5. This Agreement supersedes any conflicting or inconsistent provisions in the Services Agreement or any other contract between the Parties related to the Processing of Personal Information subject to the Data Protection Legislation and, in the event of ambiguity, this Agreement will prevail. The Services Agreement or any other contract between the Parties, as amended and modified by this Agreement, otherwise remain in full force and effect.