Barrier-free document
Barrierefreies Dokument

Datenverarbeitungs- und Datenübermittlungsverträge zur Einhaltung der Datenschutz-Grundverordnung (DS-GVO), UK-Datenschutzgesetze (Großbritannien), DSG (Schweiz), CCPA/CPRA (Kalifornien), PDPL (VAE), PIPL (China) und anderer Datenschutz-Gesetze, und zur Vertraulichkeit von Geschäftsgeheimnissen

Die enthaltenen Datenverarbeitungs- und Datenübermittlungsverträge werden automatisch zum wesentlichen Bestandteil jeder vertraglichen Vereinbarung oder der getroffenen Abreden (im Folgenden „Hauptvertrag" oder ähnlich), die zwischen unserem Unternehmen (im Folgenden „Anbieter", „Exporter", „Business", "Personal Information Handler", „uns", „unser" oder mit ähnlichen Wörtern benannt), wie im Impressum dieser oder einer unserer Webseite(n) oder E-Mail(s) und/oder im Hauptvertrag angegeben, und Ihrem Unternehmen (im Folgenden „Geschäftspartner", „Vertragspartner", „Lieferant", „Kunde", „Importer", „Contractor", „Overseas Recipient", „Ihnen" oder mit ähnlichen Wörtern benannt) 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 oder Übermittlung personenbezogener Daten (nachfolgend "Daten" genannt) im Rahmen des Hauptvertrags erforderlich ist und die von der Verarbeitung betroffenen Personen in einem der Länder ansässig sind für die in diesem Vertragswerk Verträge enthalten sind, oder anderweitig durch die entsprechenden Gesetze 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 bei einer Vereinbarung oder der Bekanntgabe dieses Vertragswerks, die auch per E-Mail oder mittels eines Links erfolgen kann, oder bei einer Einbeziehung in den Hauptvertrag automatisch (1) der "EU-Standardvertrag 2021/915 - Verantwortlicher zu Auftragsverarbeiter", wenn ein Auftragsverarbeitungsverhältnis zwischen den Vertragsparteien besteht oder zustande kommen soll, und beide Parteien ihren Sitz innerhalb der Europäischen Union oder im EWR haben und/oder (2) der "EU-Standardvertrag 2021/914 - MODUL EINS: Übermittlung Verantwortlicher zu Verantwortlicher", wenn eine der Parteien ihren Sitz außerhalb der Europäischen Union oder des EWR hat und Daten als Verantwortlicher von der anderen Vertragspartei übermittelt bekommt, und die andere Vertragspartei ebenfalls ein Verantwortlicher ist und

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ihren Sitz in der Europäischen Union oder im EWR hat, oder Daten von Betroffenen aus der Europäischen Union oder dem EWR übermittelt werden, und/oder (3) der "EU-Standardvertrag 2021/914 - MODUL ZWEI: Übermittlung Verantwortlicher zu Auftragsverarbeiter", wenn der Auftragsverarbeiter seinen Sitz außerhalb der Europäischen Union oder dem EWR hat und Daten von der anderen Vertragspartei als Verantwortlicher übermittelt bekommt, die ihren Sitz in der Europäischen Union oder im EWR hat, oder Daten von Betroffenen aus der Europäischen Union oder dem EWR übermittelt werden, und/oder (4) der "EU-Standardvertrag 2021/914 - MODUL DREI: Übermittlung Auftragsverarbeiter zu Auftragsverarbeiter", wenn die Datenübermittlerin als Auftragsverarbeiter für einen anderen Verantwortlichen oder einen Auftragsverarbeiter aus der Europäischen Union oder dem EWR tätig ist, und Daten an die andere Vertragspartei als weiteren Auftragsverarbeiter übermittelt, oder Daten von Betroffenen aus der Europäischen Union oder dem EWR übermittelt werden, und/oder (5) der "EU-Standardvertrag 2021/914 - MODUL VIER: Übermittlung Auftragsverarbeiter zu Verantwortlicher", wenn die Datenübermittlerin als Auftragsverarbeiter für einen anderen Verantwortlichen oder einen Auftragsverarbeiter aus der Europäischen Union oder dem EWR tätig ist, und Daten an die andere Vertragspartei als Verantwortlichen außerhalb der Europäischen Union oder dem EWR übermittelt, oder Daten von Betroffenen aus der Europäischen Union oder dem EWR übermittelt werden, und/oder (6) das "International Data Transfer Agreement", wenn die Datenübermittlerin in Großbritannien ansässig ist und Daten an die andere Vertragspartei außerhalb von Großbritannien übermittelt, oder Daten von Betroffenen aus Großbritannien übermittelt werden, und/oder (7) das "International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers", wenn die Datenübermittlerin in Großbritannien ansässig ist und Daten an die andere Vertragspartei außerhalb von Großbritannien übermittelt, und zuvor bereits ein EU-Standardvertrag ohne Zuhilfenahme dieses Vertragswerks abgeschlossen wurde, und/oder (8) das "Data Processing Agreement for the United Kingdom", wenn ein Auftragsverarbeitungsverhältnis zwischen den Vertragsparteien besteht oder zustande kommen soll und beide Vertragsparteien in Großbritannien ansässig sind, und/oder (9) das "CCPA-CPRA CONTRACTOR AGREEMENT", wenn Daten von Verbrauchern (Consumer) aus Kalifornien, oder zuvor nach Kalifornien übermittelte Daten, (zurück-)übermittelt werden, und/oder (10) die "Verschwiegenheitsvereinbarung und Wahrung des Datengeheimnisses für Lieferanten", wenn Ihr Unternehmen ein Lieferant aber kein Auftragsverarbeiter unseres Unternehmens ist, und/oder (11) basierend auf separat abgegebenen Willenserklärungen beider Parteien, die "Verschwiegenheitsvereinbarung und Wahrung des Datengeheimnisses für Kunden", wenn Ihr Unternehmen ein Kunde von uns ist, und auf unsere Geschäftsbeziehung kein Standardvertrag oder ein anderer in diesem Vertragswerk enthaltener Vertrag anwendbar

© All rights reserved by Heiko Maniero.

ist, und/oder (12) das "Data Processing Agreement, Joint Controllership Agreement and Cross-Border Personal Data Transfer and Sharing Agreement for the United Arab Emirates", wenn Daten aus den Vereinigten Arabischen Emiraten, oder zuvor in die Vereinigten Arabischen Emirate übermittelte Daten, (zurück-)übermittelt werden, und/oder (13) der "Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China) (Vertragssprache: Chinese)", wenn Daten aus der People's Republic of China an einen Empfänger aus einem anderen Land übermittelt werden, oder Daten von Betroffenen aus der People's Republic of China übermittelt werden, und/oder (14) das "Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China) (Vertragssprache: Chinese)", wenn ein Auftragsverarbeitungsverhältnis zwischen den Vertragsparteien besteht oder zustande kommen soll, und beide Parteien ihren Sitz in der People's Republic of China haben.

© All rights reserved by Heiko Maniero.

In diesem Vertragswerk sind folgende Verträge und Anlagen enthalten:

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)

Anlage 17 – Data Processing Agreement, Joint Controllership Agreement and Cross-Border Personal Data Transfer and Sharing Agreement for the United Arab Emirates (Vertragssprache: Englisch)

Anlage 18 – Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China) (Vertragssprache: Englisch)

Anlage 19 – Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China) (Vertragssprache: Chinese)

Anlage 20 – Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China) (Vertragssprache: Englisch)

Die geltenden Standardvertragsklauseln oder andere hier enthaltene Verträge regeln 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 Datenschutzgesetze, das DSG, der CCPA/CPRA oder andere in diesem Vertragswerk enthaltene Gesetze 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 Standardvertragsklauseln oder die anderen enthaltenen Verträge nicht durch neue Gesetze oder Verordnungen ersetzt wurden, die

© All rights reserved by Heiko Maniero.

vom zuständigen 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.

© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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);

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(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.

© All rights reserved by Heiko Maniero.

Klausel 10

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ANHANG I

Liste der Parteien

SIEHE ANLAGE 7

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ANHANG II

Beschreibung der Verarbeitung

SIEHE ANLAGE 8

Powered by ICB International Certification Body.

Document Owner: Heiko Maniero.
Information Contained: Business Data

© All rights reserved by Heiko Maniero.

Approved by: Heiko Maniero, Ulrich Baumann.
Date: 2025-05-05

ANHANG III

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ANNEX IV

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

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

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(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**).

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(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.

© All rights reserved by Heiko Maniero.

(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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

ANHANG I

A. LISTE DER PARTEIEN

SIEHE ANLAGE 7

© All rights reserved by Heiko Maniero.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

SIEHE ANLAGE 8

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

SIEHE ANLAGE 10

© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(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:

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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)**.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

ANHANG I

A. LISTE DER PARTEIEN

SIEHE ANLAGE 7

© All rights reserved by Heiko Maniero.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

SIEHE ANLAGE 8

© All rights reserved by Heiko Maniero.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

SIEHE ANLAGE 10

© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ANHANG III
LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

SIEHE ANLAGE 6

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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,

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

(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)

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

(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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

ANHANG I

A. LISTE DER PARTEIEN

SIEHE ANLAGE 7

© All rights reserved by Heiko Maniero.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

SIEHE ANLAGE 8

© All rights reserved by Heiko Maniero.

B. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

SIEHE ANLAGE 10

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ANHANG III
LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

SIEHE ANLAGE 6

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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]

© All rights reserved by Heiko Maniero.

Klausel 14

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

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

(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

© All rights reserved by Heiko Maniero.

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**.**

© All rights reserved by Heiko Maniero.

A. LISTE DER PARTEIEN

SIEHE ANLAGE 7

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

SIEHE ANLAGE 8

© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ANLAGE 7 – LISTE DER PARTEIEN

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ANLAGE 8 – BESCHREIBUNG DER DATENÜBERMITTLUNG ODER VERARBEITUNG

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.

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

ANLAGE 9 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

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

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

IT-Sicherheitsrichtlinie
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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Ermöglichung der Datenübertragbarkeit
Richtiger Umgang mit Betroffenenrechten
Sichere Datenlöschung und Datenträgervernichtung

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
Übermittlung an Unternehmen die nach dem EU-U.S. Data Privacy Framework zertifiziert sind, wenn möglich und in Kraft
Übermittlung an Unternehmen die nach dem Swiss-U.S. Data Privacy Framework zertifiziert sind, wenn möglich und in Kraft
Übermittlung an Unternehmen die nach der UK Extension to the EU-U.S. Data Privacy Framework zertifiziert sind, wenn möglich und in Kraft

© All rights reserved by Heiko Maniero.

ANLAGE 10 – ZUSTÄNDIGE AUFSICHTSBEHÖRDE

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

© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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;

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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).

© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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).

© All rights reserved by Heiko Maniero.

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):

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

	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

© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

	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 Importer may	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: there are no specific restrictions.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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

Part 3: Commercial Clauses

Commercial Clauses	see Main-Agreement

© All rights reserved by Heiko Maniero.

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:

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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;

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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;

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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:

© All rights reserved by Heiko Maniero.

- 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:

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

What happens if there is a breach of this IDTA?

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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:

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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);

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

- 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).

How to bring a legal claim under this IDTA

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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);

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

- **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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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;

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	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.
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.

© All rights reserved by Heiko Maniero.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
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 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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
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.
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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
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.
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.

© All rights reserved by Heiko Maniero.

Information Commissioner's Office

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

	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:

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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;

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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:

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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).

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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:

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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).

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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).

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

Schedule 2 – Specific security measures

See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES

© All rights reserved by Heiko Maniero.

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**

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

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-

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

© All rights reserved by Heiko Maniero.

Data Processing Agreement, Joint Controllership Agreement and Cross-Border Personal Data Transfer and Sharing Agreement for the United Arab Emirates

This Data Processing Agreement, Joint Controllership Agreement and Cross-Border Personal Data Transfer and Sharing Agreement for the United Arab Emirates (**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 **Other Party**, named with its Company details as a Party in the Services Agreement.

(together the **Parties**)

1. Preamble

1.1 The Other Party is a provider of professional services (**Services**) and/or provides its Services as a Joint-Controller. The Parties entered into an agreement which describes the Services provided by the Other Party acting on behalf of the Controller or as an Other Controller, or acting jointly with the Controller, in detail (**Services Agreement**).

1.2 The Parties have agreed to enter into this Agreement in relation to the Processing of Personal Data by the Other Party, or jointly by the Other Party and the Controller, 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 **PDPL** means the Decree Law No. 45 of 2021 as issued at the Presidential Palace in Abu Dhabi and published in the Official Gazette which is in force since 2nd of January 2022, as amended or superseded from time to time. The legal definitions from Art. 1 PDPL apply and shall have the meanings given to them by Data Protection Legislation.

2.2 **Other Controller** means an establishment or natural person acting as a Controller, who has Personal Data and who, given the nature of his/her activity, specifies the method, criteria and purpose of Processing such Personal Data, whether individually or jointly with other persons or establishments, that is Processing Personal Data that originated from the Controller, whether the data is transferred in a Cross-Border Personal Data Transfer, Shared, or Processed within the United Arab Emirates.

2.3 **Joint-Controller** means an establishment or natural person who Processes Personal Data jointly with the Controller.

2.4 **Data Protection Legislation** means the Decree Law No. 45 of 2021 as well as any regulation adopted, published, administered, implemented, or enforced by the Government of the United Arab Emirates or by one of the seven emirates, as amended or superseded from time to time,

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

all related Executive Regulations regarding or concretizing the PDPL, and any related case-law.

3. Applicability of the Agreement

This Agreement shall apply to the Processing of Personal Data, whether totally or partially, through automatically operated electronic systems or other means, by (1) any Other Controller, Joint-Controller or Processor located in the United Arab Emirates who carries out the activities of Processing Personal Data of Data Subjects inside or outside the United Arab Emirates, and (2) any Other Controller, Joint-Controller or Processor located outside the United Arab Emirates who carries out the activities of Processing Personal Data of Data Subjects inside the United Arab Emirates, as long as (3) such Personal Data is or will be Processed on behalf of the Controller, or in Joint-Controllership with the Controller, or is or will be Subject to a Cross-Border Personal Data Transfer and/or Sharing for Processing Purposes executed or initiated by or jointly with the Controller.

4. Compliance with Data Protection Legislation

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

4.2 If the Other Party is a Processor, without prejudice to the generality of this Clause, the Controller will ensure that it has all necessary 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 of its obligations under the Services Agreement.

4.3 If the Other Party is a Processor, to the extent within the Controller's control having regard to the Processor's obligations under the Services Agreement, the Controller shall be responsible for the accuracy and quality of the Personal Data Processed by the Processor.

4.4 If the Other Party is a Processor, the Processor shall have an ongoing obligation throughout the duration of the Services Agreement to identify and report to the Controller best practice techniques relating to the Processing of Personal Data and the emergence of new and evolving technologies which could improve the availability, confidentiality and/or integrity of the Processing of Personal Data.

5. Sub-Processors

5.1 If the Processing involves more than one Processor (**Sub-Processor**), the Processing must be made in accordance with a contract or written agreement whereby their obligations, responsibilities and roles related to the Processing are clearly defined.

5.2 The Controller hereby authorizes the Other Party to appoint Sub-Processors (General Written Authorization). The Other Party shall name all its Sub-Processors to the Controller prior to initiation of Processing.

5.3 With respect to each Sub-Processor appointed by the Other Party under General Written Authorization, the Other Party shall (a) 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

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

this Agreement, and (b) 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 meet the requirements stipulated by PDPL.

5.4 In regard to the Agreement between the Controller and the Other Party, the Other Party remain fully liable to the Controller for all acts or omissions of its Sub-Processor as though they were its own.

5.5 To the extent that the Other Party has already appointed any Sub-Processors prior to the Processing of any Personal Data under this Agreement, the Other Party shall ensure that its obligations under this Section are met.

5.6 Where the Other Party 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 (a) the name of any Sub-Processor which it proposes to add or replace, and (b) the Processing activity or activities affected by the proposed change, and (c) the reasons for the proposed change; and (d) the proposed date for implementation of the change.

5.7 If within thirty (30) days of receipt of a notice the Controller (acting reasonably and in good faith) notifies the Other Party in writing of any objections to the proposed change, the Parties shall use their respective reasonable endeavors to resolve the Controller's objections. Where such resolution cannot be agreed within thirty (30) days of the Other Party'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 Other Party to terminate the Services Agreement (to the extent that the provision of the Services are or would be affected by the proposed change).

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

6. Data Subject's Consent and Exceptions

6.1 The Other Party shall Process Personal Data only with the Data Subject's Consent.

6.2 If the Other Party is a Processor, the Data Subject's Consent shall be obtained by the Controller. The Processor shall obtain proof of the Data Subject's Consent from the Controller before starting the Processing of Personal Data of Data Subject's.

6.3 If the Other Party and the Controller act as Joint-Controllers, the Data Subject's Consent may be obtained by either party. If the Data Subject's Consent was obtained by one of the Joint-Controllers, that Joint-Controller shall, before starting or initiating the Processing of Personal Data of Data Subject's, inform the second Joint-Controller about obtaining the required Consent.

6.4 If the Other Party is an Other Controller and/or in any case of a Cross-Border Personal Data Transfer and/or Sharing for Processing Purposes the Other Party shall obtain the Data Subject's Consent before starting the Processing of Personal Data of Data Subject's.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

6.5 In the following cases, in which Processing is considered lawful, the Other Party may Process without the Data Subject's Consent, namely (1) if the Processing is necessary to protect the public interest, or (2) if the Processing is for Personal Data that has become available and known to the public by an act of the Data Subject, or (3) if the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial or security procedures, or (4) if the Processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the United Arab Emirates, or (5) if the Processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs and medical devices, in accordance with the legislation in force in the United Arab Emirates, or (6) if the Processing is necessary for archival purposes or for scientific, historical and statistical studies, in accordance with the legislation in force in the United Arab Emirates, or (7) if the Processing is necessary to protect the interests of the Data Subject, or (8) if the Processing is necessary for the Controller or Data Subject to fulfill his/her obligations and exercise his/her legally established rights in the field of employment, social security or laws on social protection, to the extent permitted by those laws, or (9) if the Processing is necessary to perform a contract to which the Data Subject is a party or to take, at the request of the Data Subject, procedures for concluding, amending or terminating a contract, or (10) if the Processing is necessary to fulfill obligations imposed by other laws of the United Arab Emirates on Controllers, or (11) any other cases set by the Executive Regulations of PDPL.

7. Personal Data Processing Controls

The Other Party shall Process Personal Data only according to the following controls, namely (1) Processing must be made in a fair, transparent and lawful manner, and (2) Personal Data must be collected for a specific and clear purpose, and may not be Processed at any subsequent time in a manner incompatible with that purpose. However, Personal Data may be Processed if the purpose of Processing is similar or close to the purpose for which such data is collected, and (3) Personal Data must be sufficient for and limited to the purpose for which the Processing is made, and (4) Personal Data must be accurate and correct and must be updated whenever necessary, and (5) Appropriate measures and procedures must be in place to ensure erasure or correction of incorrect Personal Data, and (6) Personal Data must be kept securely and protected from any breach, infringement, or illegal or unauthorized Processing by establishing and applying appropriate technical and organizational measures and procedures in accordance with the laws and legislation in force in this regard, and (7) Personal Data may not be kept after fulfilling the purpose of Processing. It may only be kept in the event that the identity of the Data Subject is anonymized using the “Anonymization” feature, and (8) any other controls set by the Executive Regulations of PDPL.

8. Conditions for Consent to Data Processing

8.1 If the Other Party is an Other Controller or acts jointly as a Joint-Controller with the Controller, the Other Party shall be able to prove the Consent of the Data Subject to Process his/her Personal Data in the event that the Processing is based on such Consent.

8.2 If the Other Party is an Other Controller, or acts jointly as a Joint-Controller with the Controller, the Other Party shall be able to prove that Consent was given in a clear, simple, unambiguous and easily accessible manner, whether in writing or electronic form and that the Consent language indicated the right of the Data Subject to withdraw, at any time, its Consent and that

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

such withdrawal could be easily made, and that such withdrawal shall not affect the legality and lawfulness of the Processing made based on the Consent given prior to the withdrawal.

9. General Obligations of the Other Party

9.1 The Other Party shall take appropriate technical and organizational measures and procedures to apply the necessary standards to protect and secure Personal Data, in order to maintain its confidentiality and privacy and to ensure that it is not infringed, damaged, altered or tampered with, taking into account the nature, scope and purposes of Processing and the potential risks to the confidentiality and privacy of the Personal Data of the Data Subject. The Parties agreed on the required technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

9.2 The Other Party shall apply the appropriate measures, both when defining the means of Processing or during the Processing itself, in order to comply with the provisions of PDPL, including the controls stipulated in Article 5 PDPL. Such measures may include Pseudonymization.

9.3 The Other Party shall apply the appropriate technical and organizational measures with respect to default settings to ensure that the Processing of Personal Data is limited to its intended purpose. This obligation applies to the amount and type of Personal Data collected, the type of Processing to be made thereon, and the period of storage and accessibility of such data.

9.4 The Other Party shall maintain a special record of Personal Data which must include the data of the Controller and Data Protection Officer, as well as a description of the categories of Personal Data held thereby, data of the persons authorized to access such Personal Data, the Processing durations, restrictions and scope, the mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and Cross-Border Processing of such data, while indicating the technical and organizational procedures related to information security and Processing operations, provided that the Controller provides this record to the UAE Data Office whenever requested to do so.

9.5 The Other Party shall appoint only Processors who provide sufficient guarantees to apply technical and organizational measures in a manner that ensures that the Processing meets the Processing requirements, rules and controls stipulated by PDPL, the Executive Regulations of PDPL and decisions issued in implementation of PDPL.

9.6 The Other Party shall provide the UAE Data Office, based on a decision from the competent judicial authority, with any information requested thereby in exercise of its competencies stipulated by PDPL and the Executive Regulations of PDPL.

9.7 The Other Party shall fulfill any other obligations set by the Executive Regulations of PDPL. The Other Party shall monitor and abide the Executive Regulations of PDPL.

10. General Obligations of the Other Party if that Party acts as a Processor

10.1 This Section 10 applies only if the Other Party acts as a Processor and Processes Personal Data on behalf of the Controller. The Clauses of Section 10 of this Agreement shall supersede any conflicting Clauses in other Sections of this Agreement regarding to the Processor.

10.2 The Processor shall make and carry out the Processing in accordance with the instructions of the Controller and the contracts and agreements concluded between them that specify in

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

particular the scope, subject, purpose and nature of the Processing, the type of Personal Data and categories of Data Subjects. The Parties determined the scope, subject, purpose and nature of the Processing, the type of Personal Data and categories of Data Subjects in the Services Agreement and/or in APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER.

10.3 The Processor shall apply the appropriate technical and organizational measures and procedures to protect Personal Data at the design stage, both when defining the means of Processing or during the Processing itself, taking into consideration the cost of applying such measures and procedures and the nature, scope and purposes of the Processing. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

10.4 The Processor shall make the Processing according to the purpose and period set therefor and notify the Controller if the Processing exceeds the set period, in order to extend such period or issue the appropriate directions. Whenever required, the notifications shall be made within two working days after such event occurred or is determined.

10.5 The Processor shall not take any action that would disclose the Personal Data or the results of Processing, except in cases permitted by law.

10.6 The Processor shall protect and secure the Processing operation and secure the media and electronic devices used in the Processing and the Personal Data stored therein.

10.7 The Processor shall maintain a special record of Personal Data Processed on behalf of the Controller, which must include the data of the Controller, Processor and Data Protection Officer, as well as a description of the categories of Personal Data held thereby, data of the persons authorized to access such Personal Data, the Processing durations, restrictions and scope, the mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and Cross-Border Processing of such data, while indicating the technical and organizational procedures related to information security and Processing operations, provided that the Processor provides this record to the UAE Data Office whenever requested to do so.

10.8 The Processor shall provide all means to prove abidance thereby to the provisions of PDPL, at the request of the Controller or UAE Data Office.

10.9 The Processor shall make and carry out the Processing in accordance with the rules, requirements and controls set by PDPL and the Executive Regulations of PDPL, or as instructed by the UAE Data Office.

10.10 The Executive Regulations of PDPL shall set the procedures, controls, conditions, and technical and standard criteria related to the Processors obligations. The Processor shall monitor and abide the Executive Regulations of PDPL.

11. General Obligations if the Parties act as Joint-Controllers

11.1 This Section 11 shall apply only if the Controller and the Other Party act jointly as Joint-Controllers. The Clauses of Section 11 of this Agreement shall supersede any conflicting Clauses in other Sections of this Agreement regarding to the Joint-Controllers.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

11.2 The Joint-Controllers determined the scope, subject, purpose and nature of the Processing, the type of Personal Data and categories of Data Subjects in the Services Agreement and/or in APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER.

11.3 The Joint-Controllers shall jointly ensure compliance with Data Protection Legislation when Processing Personal Data. Both controllers are equally responsible for the legality and lawfulness of joint Processing.

11.4 Regardless of the place of Business of each Joint-Controller, both Joint-Controllers agree that the UAE Data Office is the competent supervisory authority.

11.5 The Controller undertakes to provide the Data Subject's with all information regarding the Data Subject's Rights under PDPL. The Controller acts as the contact point for Data Subjects.

11.6 The Joint-Controllers shall jointly take the appropriate technical and organizational measures and procedures to apply the necessary standards to protect and secure Personal Data, in order to maintain its confidentiality and privacy and to ensure that it is not infringed, damaged, altered or tampered with, taking into account the nature, scope and purposes of Processing and the potential risks to the confidentiality and privacy of the Personal Data of the Data Subject. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

11.7 The Joint-Controllers shall jointly apply the appropriate measures, both when defining the means of Processing or during the Processing itself, in order to comply with the provisions of PDPL, including the controls stipulated in Article 5 PDPL. Such measures may include Pseudonymization.

11.8 The Joint-Controllers shall jointly apply the appropriate technical and organizational measures with respect to default settings to ensure that the Processing of Personal Data is limited to its intended purpose. This obligation applies to the amount and type of Personal Data collected, the type of Processing to be made thereon, and the period of storage and accessibility of such data. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

11.9 The Joint-Controllers shall jointly maintain a special record of Personal Data which must include the data of the Controller and Data Protection Officer, as well as a description of the categories of Personal Data held thereby, data of the persons authorized to access such Personal Data, the Processing durations, restrictions and scope, the mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and Cross-Border Processing of such data, while indicating the technical and organizational procedures related to information security and Processing operations, provided that the Controller provides this record to the UAE Data Office whenever requested to do so.

11.10 The Joint-Controllers shall jointly appoint only Processors who provide sufficient guarantees to apply technical and organizational measures in a manner that ensures that the Processing meets the Processing requirements, rules and controls stipulated by PDPL, the Executive Regulations of PDPL and decisions issued in implementation of PDPL.

11.11 The Joint-Controllers shall jointly provide the UAE Data Office, based on a decision from the competent judicial authority, with any information requested thereby in exercise of its competencies stipulated by PDPL and the Executive Regulations of PDPL.

© All rights reserved by Heiko Maniero.

11.12 The Joint-Controllers shall jointly appoint a Data Protection Officer in accordance with Section 13 of this Agreement.

12. Reporting a Personal Data Breach

12.1 The Other Party shall, immediately upon becoming aware of any infringement or breach of the Personal Data of the Data Subject that would prejudice the privacy, confidentiality and security of such data, report such infringement or breach and the results of the investigation to the Controller.

12.2 Such reporting shall be accompanied by the following data and documents, namely (a) the nature, form, causes, approximate number and records of the infringement or breach, and (b) the data of the Data Protection Officer appointed by the Other Party, and (c) the potential and expected effects of the infringement or breach, and (d) the procedures and measures taken thereby and proposed to be applied to address this infringement or breach and reduce its negative effects, and (e) documentation of the infringement or breach and the corrective actions taken by the Other Party, and (f) any other requirements that the UAE Data Office demands from the Controller.

12.3 The Other Party will assist the Controller by all means to allow the Controller to notify the Data Subject in the event that the infringement or breach would prejudice the privacy, confidentiality and security of his/her Personal Data and advise him/her of the procedures taken thereby, within such period and in accordance with such procedures and conditions as set by the Executive Regulations of PDPL.

13. Appointment of Data Protection Officer

13.1 The Other Party shall appoint a Data Protection Officer who has sufficient skills and knowledge of Personal Data Protection, in any of the following cases, namely (a) if the Processing would cause a high-level risk to the confidentiality and privacy of the Personal Data of the Data Subject as a result of adopting technologies that are new or associated with the amount of data, or (b) if the Processing will involve a systematic and comprehensive assessment of Sensitive Personal Data, including Profiling and Automated Processing, or (c) if the Processing will be made on a large amount of Sensitive Personal Data.

13.2 The Data Protection Officer may be employed or authorized by the Other Party, whether inside or outside the United Arab Emirates.

13.3 The Other Party shall specify the contact address of the Data Protection Officer and notify the UAE Data Office.

14. Responsibilities of the Data Protection Officer of the Other Party

14.1 The Data Protection Officer of the Other Party shall be responsible for ascertaining compliance by the Other Party with the provisions of PDPL, the Executive Regulations of PDPL, and the instructions issued by the UAE Data Office.

14.2 The Data Protection Officer of the Other Party shall, in particular, undertake the following duties and powers, namely (a) verifying the quality and validity of the procedures adopted by both the Controller and Processor, and (b) receiving requests and complaints related to Personal Data in accordance with the provisions of PDPL and the Executive Regulations of PDPL, and (c) providing technical advice related to the procedures of periodic evaluation and examination of

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Personal Data Protection systems and intrusion prevention systems of the Controller and Processor, documenting the results of such evaluation, and providing appropriate recommendations in this regard, including risk assessment procedures, and (d) acting as a liaison between the Controller or Processor, as the case may be, and the UAE Data Office regarding their implementation of the provisions of Personal Data Processing stipulated by PDPL, and (e) any other duties or powers specified under the Executive Regulations of PDPL.

14.3 The Data Protection Officer of the Other Party shall maintain the confidentiality of the information and data received thereby in implementation of the duties and powers given thereto pursuant to the provisions of PDPL and the Executive Regulations of PDPL and in accordance with the legislation in force in the United Arab Emirates.

15. Obligations of the Other Party towards the Data Protection Officer

15.1 The Other Party shall provide all means to ensure that the Data Protection Officer performs the responsibilities and duties assigned thereto, as stipulated in Article 11 PDPL, in a proper manner, including, in particular, the following, namely (a) ensuring that he/she is appropriately and timely engaged in all matters relating to Personal Data Protection, and (b) ensuring that he/she is provided with all the necessary resources and support to perform the duties assigned by PDPL, and (c) not to terminate his/her service or impose any disciplinary penalty for a reason related to the performance of his/her duties in accordance with the provisions of PDPL, and (d) ensuring that he/she is not assigned to duties that lead to a conflict of interest with the duties assigned under PDPL.

15.2 Data Subject's shall communicate directly with the Data Protection Officer of the Controller for any matters related to his/her Personal Data and the Processing under PDPL in order to exercise his/her rights in accordance with the provisions of PDPL. The Data Protection Officer of the Other Party shall refer Data Subject's to the Data Protection Officer of the Controller. Only where the Other Party acts as the Controller, the Data Protection Officer of the Other Party shall communicate directly with Data Subject's. If the Other Party and the Controller act as Joint-Controllers, the Data Protection Officers of both parties coordinate how to and who responds to Data Subject's.

16. Right to Obtain Information, Right to Request Personal Data Transfer, Right to Correction or Erasure of Personal Data, Right to Restrict Processing, Right to Stop Processing, Right to Processing and Automated Processing

16.1 The Other Party shall take all appropriate technical and organizational measures and procedures to ensure the Data Subject's Rights, and to allow the Controller to comply with any request made by any Data Subject regarding the Right to Obtain Information, Right to Request Personal Data Transfer, Right to Correction or Erasure of Personal Data, Right to Restrict Processing, Right to Stop Processing, Right to Processing and Automated Processing and any other Right granted by Data Protection Legislation.

16.2 The Other Party shall provide appropriate and clear ways and mechanisms to enable the Data Subject to communicate with the Other Party and place requests regarding the Data Subject's Rights stipulated by PDPL. The Other Party shall inform the Controller about any request of a Data Subject regarding any Data Subject Right without undue delay.

17. Personal Data Security

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

17.1 The Other Party shall establish and take appropriate technical and organizational measures and procedures to ensure achievement of the information security level that is commensurate with the risks associated with Processing, in accordance with the best international standards and practices, which may include (a) encryption of Personal Data and application of Pseudonymization, and (b) application of procedures and measures that ensure the confidentiality, safety, validity and flexibility of Processing systems and services, and (c) application of procedures and measures that ensure the timely retrieval and access of Personal Data in the event of any physical or technical failure, and (d) application of procedures that ensure a smooth testing, evaluation and assessment of the effectiveness of technical and organizational measures so as to ensure the security of Processing. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

17.2 When evaluating the level of information security, the Other Party shall be taken into account (a) risks associated with Processing, including Personal Data damage, loss, accidental or illegal modification, disclosure or unauthorized access, whether transmitted, stored or Processed, and (b) the costs, nature, scope and purposes of Processing, as well as the different potential risks to the privacy and confidentiality of the Personal Data of the Data Subject.

18. Assessment of Personal Data Protection Impact

18.1 Subject to the nature, scope and purposes of Processing, the Other Party shall, before starting the Processing, assess the impact of the proposed Processing on Personal Data Protection, when using any of the modern technologies that would pose a high risk to the privacy and confidentiality of the Personal Data of the Data Subject (**Impact Assessment**).

18.2 The Impact Assessment shall be required (a) if the Processing involves a systematic and comprehensive assessment of the personal aspects of the Data Subject based on Automated Processing, including Profiling, which would have legal consequences or would seriously affect the Data Subject, and (b) if the Processing will be made on a large amount of Sensitive Personal Data.

18.3 The Impact Assessment must include, at a minimum (a) a clear and systematic explanation of the impact of the proposed Processing on Personal Data Protection and the purpose of such Processing, and (b) an assessment of the necessity and suitability of Processing for the purpose of PDPL, and (c) an assessment of the potential risks to the privacy and confidentiality of the Personal Data of the Data Subject, and (d) the proposed procedures and measures to minimize the potential risks to Personal Data Protection.

18.4 The Other Party may make a single assessment for a set of Processing operations of similar natures and risks.

18.5 The Other Party shall coordinate with the Data Protection Officer when assessing the impact of Personal Data Protection.

18.6 The Other Party shall review the assessment outcomes periodically to ensure that the Processing is carried out in accordance with the assessment, in case the levels of risks associated with the Processing operations are different.

19. Cross-Border Personal Data Transfer and Sharing for Processing Purposes if there is an Adequate Level of Protection

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

The Other Party may transfer Personal Data outside the United Arab Emirates in the following cases approved by the Office, namely (1) if the country or territory to which the Personal Data is to be transferred has special legislation on Personal Data Protection therein, including the most important provisions, measures, controls, requirements and rules for protecting the privacy and confidentiality of the Personal Data of the Data Subject and his/her ability to exercise his/her rights, and provisions related to imposing appropriate measures on the Controller or Processor through a supervisory or judicial authority, and (2) if the United Arab Emirates accedes to bilateral or multilateral agreements related to Personal Data Protection with the countries to which the Personal Data is to be transferred.

20. Cross-Border Personal Data Transfer and Sharing for Processing Purposes if there is not an Adequate Level of Protection

20.1 With the exception of what is stated in Article 22 PDPL, the Other Party may transfer Personal Data outside the United Arab Emirates in the following cases: (a) In countries where there is no data protection law, Establishments operating in the United Arab Emirates and in those countries may transfer data under a contract or agreement that obliges the Establishment in those countries to implement the provisions, measures, controls and requirements set out by PDPL, including provisions related to imposing appropriate measures on the Controller or Processor through a competent supervisory or judicial authority in that country, which shall be specified in the contract, or (b) the express Consent of the Data Subject to transfer his/her Personal Data outside the United Arab Emirates in a manner that does not conflict with the security and public interest of the United Arab Emirates, or (c) if the transfer is necessary to fulfill obligations and establish, exercise or defend rights before judicial authorities, or (d) if the transfer is necessary to enter into or execute a contract between the Controller and Data Subject, or between the Controller and a other Party to achieve the Data Subject's interest, or (e) if the transfer is necessary to perform a procedure relating to international judicial cooperation, or (f) if the transfer is necessary to protect the public interest.

20.2 The Other Party shall observe and comply with the Executive Regulations of PDPL that set the controls and requirements for the cases referred above, which must be met for transferring Personal Data outside the United Arab Emirates.

20.3 Whereas the Other Party is an Establishment in a country where there is no data protection law, and receives Personal Data in a Cross-Border Personal Data Transfer from the Controller and/or receives Personal Data that is Shared for Processing Purposes by the Controller, the Other Party agrees to implement the provisions, measures, controls and requirements set out by PDPL, including provisions related to imposing appropriate measures on the Other Party through a competent supervisory or judicial authority. The competent judicial authority is the arbitral tribunal referred to in Section 23 of this Agreement. The parties agree that the UAE Data Office is the competent supervisory authority.

21. Obligations upon expiry or termination of the Services Agreement

21.1 Notwithstanding the Other Party’s obligations under the Services Agreement following its expiry or termination, the Other Party shall promptly and in any event within thirty (30) days of the expiry or termination of the Services Agreement, at the Controller’s option 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 Other Party and/or its Sub-Processors on behalf of the Controller or originating from the Controller.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

21.2 Where the Controller has instructed the Other Party to delete the Personal Data, the Other Party shall do so in accordance with best industry practice for the reliable and secure deletion of data and for the secure destruction of confidential material.

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

21.4 The Controller may require the Other Party to provide a written certificate confirming that it has complied with its obligations under this Section.

22. Liability and indemnification

22.1 The Other Party shall be liable for any violation of Data Protection Legislation or this Agreement by the Other Party or its Sub-Processors.

22.2 The Other Party agrees to indemnify, defend, and hold harmless the Controller 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 Other Party, and/or its negligence or willful misconduct, or its Sub-Processors.

23. Arbitration Clause

23.1 All disputes arising out of or in connection with this contract or its validity shall be finally settled under the rules of arbitration of the German Institution for Arbitration e. V. (DIS), excluding ordinary legal action.

23.2 The arbitral tribunal consists of a single arbitrator. The parties hereby irrevocably agree that the sole arbitrator may be appointed by attorney-at-law Mr. Ulrich Baumann and / or Prof. Dr. h.c. Heiko Jonny Maniero, whereby the above-mentioned persons can appoint themselves also to the arbitrator in the respective arbitration procedure, as far as the own designation no conflicts of interests stand against. The seat of the arbitral tribunal is Abu Dhabi.

23.3 The language of the proceedings is German.

23.4 The law applicable in the case is the Law of the United Arab Emirates.

24. General provisions

24.1 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.

24.2 A Person who is not a Party to this Agreement shall not have any rights to enforce any terms of this Agreement.

24.3 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,

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

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.

24.4 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).

© All rights reserved by Heiko Maniero.

Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China)

The Personal Information Handler and the Overseas Recipient will carry out the activities concerning the outbound cross-border transfer of Personal Information in accordance with this Contract. The Parties have entered into or agreed to enter into a commercial contract to further the commercial acts related to such activities, namely the Main-Agreement on the date of conclusion of the Main-Agreement.

The major body of this Contract is drafted in accordance with the requirements of the *Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information*. Other agreements between the Parties, if any, may be specified in Appendix II. The Appendix forms an integrated part of this Contract.

Article 1 Definitions

In this Contract, unless the context otherwise requires:

1. "Personal Information Handler" refers to any organization or individual that independently decides the purpose and method of the Personal Information handling activities and transfers Personal Information outside the territory of the People's Republic of China.

2. "Overseas Recipient" refers to an organization or individual outside the territory of the People's Republic of China that receives Personal Information from the Personal Information Handler.

3. Personal Information Handler or Overseas Recipient are referred to individually as a "Party", and collectively as the "Parties".

4. "Personal Information Subject" refers to a natural person identified by or associated with the Personal Information.

5. "Personal Information" refers to all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized.

6. "Sensitive Personal Information" refers to the Personal Information that, once leaked or illegally used, is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety, including biometric recognition, religious belief, specific identity, medical health, financial account, personal whereabouts, and the Personal Information of minors under the age of 14.

7. "Regulatory Authority" refers to the Cyberspace Administration of the People's Republic of China at the provincial level or above.

8. "Relevant Laws and Regulations" refer to the laws and regulations of the People's Republic of China, such as the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, the *Civil Code of the People's Republic of China*, *Civil Procedure Law of the People's Republic of China*, and *Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information*.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

9. The meanings of other terms not defined in the Contract are in line with those stipulated in the Relevant Laws and Regulations.

Article 2 Obligations of the Personal Information Handler

The Personal Information Handler shall perform the following obligations:

1. Handle Personal Information in accordance with the Relevant Laws and Regulations. The Personal Information to be transferred overseas shall be limited to the minimum scope required for the purpose of handling.

2. Inform the Personal Information Subject of matters such as the name and contact information of the Overseas Recipient, the purpose of handling, method of handling, type of Personal Information, retention periods, and the methods and procedures for the Personal Information Subject to exercise his/her rights specified in Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*". Where Sensitive Personal Information is transferred overseas, the Personal Information Subject shall be informed of the necessity of the outbound cross-border transfer of Sensitive Personal Information and the impact on the rights and interests of the Personal Information Subject, unless otherwise provided in the laws and administrative regulations that such notification is not required.

3. If Personal Information is transferred overseas based on the consent of the individual, the separate consent of the Personal Information Subject shall be obtained. Where the Personal Information involves that of a minor under the age of 14, the separate consent of the minor's parent or any other guardian, shall be obtained. Where written consent is required by laws and administrative regulations, the written consent shall be obtained.

4. Inform the Personal Information Subject that the Personal Information Handler and the Overseas Recipient have agreed that the Personal Information Subject is a third-party beneficiary under this Contract, and if the Personal Information Subject fails to raise an express rejection within thirty days, the Personal Information Subject shall be entitled to act as a third-party beneficiary in accordance with the Contract.

5. Make reasonable efforts to ensure that the Overseas Recipient has taken the following technical and organizational measures to perform its obligations under this Contract (taking into account potential Personal Information security risks that may be caused by the purpose of Personal Information handling, the type, scale, scope and sensitivity of the Personal Information, the scale and frequency of the transfer, the period of the outbound cross-border transfer of Personal Information, the period of retention by the Overseas Recipient, and other matters that may lead to a Personal Information security risk): APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

6. Provide copies of Relevant Laws and Regulations and technical standards to the Overseas Recipient upon request.

7. Reply to inquiries from the Regulatory Authority about the Overseas Recipient's handling activities.

8. Carry out a Personal Information Protection Impact Assessment in accordance with the Relevant Laws and Regulations regarding the proposed transfer of Personal Information to the Overseas Recipient. The assessment shall focus on the following matters:

   (1) the legality, legitimacy and necessity of the purpose, scope and method of handling Personal Information by the Personal Information Handler and Overseas Recipient;

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(2) the scale, scope, type, and sensitivity of Personal Information to be transferred overseas, and the risks that the outbound cross-border transfer may pose to Personal Information rights and interests;

(3) the obligations that the Overseas Recipient undertakes to assume, and whether the organizational and technical measures and capabilities to perform such obligations are sufficient to ensure the security of the Personal Information to be transferred overseas;

(4) risk of Personal Information being tampered with, destroyed, leaked, lost, illegally used, etc. after the outbound cross-border transfer, and whether there are channels for individuals to smoothly exercise Personal Information rights and interests etc.;

(5) in accordance with Article 4 hereof, to evaluate whether the performance of this Contract will be affected by the local policies and regulations with respect to protection of Personal Information; and

(6) other matters that may affect the security of outbound cross-border transfer of Personal Information.

The Personal Information Protection Impact Assessment Report shall be kept for at least three years.

9. Provide a copy of this Contract to the Personal Information Subject upon the Personal Information Subject 's request. If trade secrets or confidential business information are involved, the relevant contents of the copy of this Contract may be appropriately redacted, provided that such redaction will not affect the understanding of the Personal Information Subject.

10. Assume a burden of proof for the performance of obligations under this Contract.

11. In accordance with Relevant Laws and Regulations, provide the Regulatory Authority with all information as described in Article 3.11, including all compliance audit results.

Article 3 Obligations of the Overseas Recipient

The Overseas Recipient shall perform the following obligations:

1. Handle the Personal Information in accordance with Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*". Where the Overseas Recipient handles the Personal Information in a way beyond the purpose and method of the Personal Information handling, and types of the Personal Information as agreed, it shall obtain the separate consent of the Personal Information Subject in advance if the handling of Personal Information is based on the consent of the Personal Information Subject; where the Personal Information of a minor under the age of 14 is involved, the separate consent of the minor's parent, or any other guardian, shall be obtained.

2. Where the Overseas Recipient is contracted by the Personal Information Handler to handle Personal Information, the Overseas Recipient shall handle the Personal Information in accordance with the agreement with the Personal Information Handler and shall not handle the Personal Information in a way beyond the purpose or method of the Personal Information handling.

3. Provide a copy of this Contract to the Personal Information Subject upon the Personal Information Subject's request. If trade secrets or other confidential business information are

© All rights reserved by Heiko Maniero.

involved, relevant parts of this Contract may be appropriately redacted, provided that such redaction will not affect the understanding of the Personal Information Subject.

4. Handle the Personal Information in a manner that has the least impact on the rights and interests of the Personal Information Subject.

5. The retention period of Personal Information shall be the minimum period necessary for achieving the purpose of handling. Upon expiry of the retention period, the Personal Information (including all back-up copies) shall be deleted. Where the handling of Personal Information is contracted by the Personal Information Handler, and the personal information handling agreement fails to become effective, becomes null and void, or is cancelled or terminated, the Personal Information being handled shall be returned to the Personal Information Handler or deleted, and a written statement shall be provided to the Personal Information Handler. If it is technically difficult to delete the Personal Information, the handling of the Personal Information, other than the storage and any necessary measures taken for security protection, shall be ceased.

6. Ensure the security of Personal Information handling in the following ways:

   (1) take technical and organizational measures including but not limited to those listed in Article 2.5 of this Contract and carry out regular inspections to ensure the security of Personal Information; and

   (2) ensure that the personnel authorized to handle Personal Information perform their confidentiality obligations and establish access control permissions of minimum authorization.

7. In the event that Personal information is or may be tampered with, destroyed, leaked, lost, illegally used, provided or accessed without authorization, the Overseas Recipient shall:

   (1) promptly take appropriate measures to mitigate the adverse impact on the Personal Information Subject;

   (2) immediately notify the Personal Information Handler and report to the Regulatory Authority in accordance with the Relevant Laws and Regulations. The notice shall contain the following contents:

      i. the type of Personal Information to which the tampering with, destruction, leakage, loss, illegal use, unauthorized provision or access occurs or may occur, the cause of such event or potential event, and the potential harm;

      ii. remedial measures that have been taken;

      iii. measures that can be taken by the Personal Information Subject to mitigate harm; and

      iv. contact information of the person, or team, in charge of handling the situation.

   (3) where the Relevant Laws and Regulations require the notification of the Personal Information Subject, the content of the notice shall include the foregoing contents in Article 3.7. (2) above; where the handling of Personal Information is contracted by the Personal Information Handler, the Personal Information Handler shall notify the Personal Information Subject;

   (4) record and retain all the situations thereof relating to the occurrence or potential occurrence of tampering, destruction, leakage, loss, illegal use, unauthorized provision or access, including all remedial measures taken.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

8. The Overseas Recipient may provide Personal Information to the third party located outside the territory of the People's Republic of China only, if all of the following requirements are met:

   (1) there is a necessity from the business perspective;

   (2) the Personal Information Subject has been informed of such third party's name, contact information, the purpose of handling, method of handling, type of Personal Information, retention periods, and the methods and procedures for the Personal Information Subject to exercise his/her rights. Where Sensitive Personal Information is provided to such third party, the Personal Information Subject should also be informed of the necessity of the outbound cross-border transfer of Sensitive Personal Information and the impact on the rights and interests of the Personal Information Subject. However, unless otherwise provided by laws and administrative regulations that such notification is not required;

   (3) where the handling of Personal Information is based on the consent of the Personal Information Subject, the separate consent of the Personal Information Subject shall be obtained; where the Personal Information of a minor under the age of 14 is involved, the separate consent of the minor's parent, or any other guardian, shall be obtained. Where written consent is required by laws and administrative regulations, such written consent shall be obtained;

   (4) enter into a written agreement with the third party to ensure that the handling of Personal Information by the third party meets the standards for protection of Personal Information required by the Relevant Laws and Regulations of the People's Republic of China, and the Overseas Recipient will assume the liability for the infringement of Personal Information Subject's rights due to the provision of Personal Information to the third party located outside the territory of the People's Republic of China;

   (5) provide a copy of the above agreement to the Personal Information Subject upon the Personal Information Subject's request. If trade secrets or other confidential business information are involved, relevant parts of the agreement may be appropriately redacted provided that such redaction will not affect the understanding of the Personal Information Subject.

9. Where the Overseas Recipient is contracted by the Personal Information Handler to handle Personal Information, and the Overseas Recipient intends to sub-contract the handling to a third party, the Overseas Recipient shall obtain the consent of the Personal Information Handler in advance and shall ensure that the sub-contractor will not handle Personal Information in a way beyond the purpose and method of the handling as specified in Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*", and shall monitor the Personal Information handling activities of the third party.

10. When making use of Personal Information for automated decision-making, the Overseas Recipient shall ensure the transparency of decision-making and fair and impartial results, and shall not carry out unreasonable or differential treatment of the Personal Information Subject in terms of transaction conditions, such as transaction price. Where automated decision-making is used for pushing information and commercial marketing to the Personal Information Subject, the Overseas Recipient shall also provide the Personal Information Subject with options that are not specific to the individuals' characteristics, or a convenient way for the Personal Information Subject to reject the automated decision-making.

11. Undertake to provide the Personal Information Handler with all necessary information required to comply with the obligations under this Contract, provide the Personal Information Handler access to review the necessary data documents, and files, or conduct a compliance audit of the

© All rights reserved by Heiko Maniero.

handling activities under this Contract, and the Overseas Recipient shall facilitate the compliance audit conducted by the Personal Information Handler.

12. Maintain an accurate record of the Personal Information handling activities carried out for at least 3 years and provide the relevant records and documents to the Regulatory Authority directly or through the Personal Information Handler, as required by the Relevant Laws and Regulations.

13. Agree to be subject to supervision by the Regulatory Authority during an enforcement procedure related to supervising the implementation of this Contract, including but not limited to responding to inquiries and inspections by the Regulatory Authority, following the actions taken or decisions made by the Regulatory Authority, and providing written confirmation that necessary measures have been taken etc.

Article 4 The Impact of Personal Information Protection Policies and Regulations in the Overseas Recipient's Country or Region on the Performance of this Contract

1. The Parties warrant that they have exercised reasonable care when entering into this Contract and are not aware of Personal Information protection policies and regulations in the Overseas Recipient's country or region (including any requirements on providing Personal Information or authorizing public authorities to access Personal Information) that would have an impact on the Overseas Recipient's performance of its obligations under this Contract.

2. The Parties declare that, when making the warranties in Article 4.1, they have conducted the assessment in conjunction with the following circumstances:

   (1) the specific circumstances of outbound cross-border transfer, including the purpose of handling the Personal Information, the types, scale, scope and sensitivity of the Personal Information transferred, the scale and frequency of transfer, the period of the outbound cross-border transfer of Personal Information and the retention period of the Overseas Recipient, the previous experience of the Overseas Recipient with respect to outbound cross-border transfer and handling of similar Personal Information, whether any Personal Information security incident had occurred to the Overseas Recipient and whether such incident was timely and effectively handled, whether the Overseas Recipient has received any request to provide Personal Information to the public authority of the country or region where it is located and how the Overseas Recipient has responded to such request;

   (2) the Personal Information protection policies and regulations of the country or region where the Overseas Recipient is located, including the following elements:

      i. the existing Personal Information protection laws, regulations and generally applicable standards of the country or region;

      ii. the regional or global organizations of Personal Information protection that the country or region accedes to, and binding international commitments made by the country or region; and

      iii. the mechanisms for Personal Information protection implemented in the country or region, such as whether there are supervision and enforcement authorities and relevant judicial authorities responsible for protecting Personal Information.

   (3) the Overseas Recipient's security management system and technical capabilities.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

3. The Overseas Recipient warrants that it has used its best efforts to provide the Personal Information Handler with the necessary relevant information for the assessment under Article 4.2.

4. The Parties shall keep a record of any such assessment carried out under Article 4.2 as well as the assessment results.

5. Where the Overseas Recipient is unable to perform this Contract due to any change in the policies and regulations on Personal Information protection of the country or region where the Overseas Recipient is located (including any change of laws or mandatory measures in the country or region where the Overseas Recipient is located), the Overseas Recipient shall notify the Personal Information Handler immediately after being aware of the aforesaid change.

6. If the Overseas Recipient receives a request for provision of Personal Information under this Contract from a governmental authority or judicial authority in the country or region where the Overseas Recipient is located, it shall promptly notify the Personal Information Handler.

Article 5 Rights of the Personal Information Subject

The Parties agree that the Personal Information Subject shall be entitled to the following rights as a third-party beneficiary under this Contract.

1. The Personal Information Subject, in accordance with Relevant Laws and Regulations, has the right to know and to make decisions on the handling of the Personal Information, the right to restrict or refuse handling of the Personal Information Subject's Personal Information by others, the right to request access to, copy, correct, supplement or delete the Personal Information, and the right to request others to explain the rules for the handling of the Personal Information Subject's Personal Information.

2. When the Personal Information Subject requests to exercise the above-mentioned rights regarding their Personal Information that has been transferred overseas, the Personal Information Subject may request the Personal Information Handler to take appropriate measures for the realization of those rights, or directly make the request to the Overseas Recipient. If the Personal Information Handler is unable to realize those rights, it shall notify the Overseas Recipient and request the Overseas Recipient to assist in the realization.

3. The Overseas Recipient shall, as notified by the Personal Information Handler or requested by the Personal Information Subject, realize the rights that the Personal Information Subject is entitled to within a reasonable period and in accordance with the Relevant Laws and Regulations.

   The Overseas Recipient shall inform the Personal Information Subject about the relevant information which shall be true, accurate and complete, in an obvious way and using clear and understandable language.

4. If the Overseas Recipient intends to refuse the request of the Personal Information Subject, it shall inform the Personal Information Subject the reasons of the refusal, as well as the channels for the Personal Information Subject to raise complaints with the relevant Regulatory Authority and seek judicial remedies.

5. The Personal Information Subject, as a third-party beneficiary to this Contract, has the right to claim against one or both, the Personal Information Handler and the Overseas Recipient, in accordance with this Contract and require them to perform the following clauses under this Contract relating to the rights of the Personal Information Subject:

   (1) Article 2, except for Articles 2.5, 2.6 and 2.7;

© All rights reserved by Heiko Maniero.

(2) Article 3, except for Articles 3.7(2) and 3.7(4), 3.9, 3.11, 3.12 and 3.13;

(3) Article 4, except for Articles 4.5 and 4.6;

(4) Article 5;

(5) Article 6;

(6) Article 8.2 and 8.3; and

(7) Article 9.5.

The above agreement shall not affect the rights and interests of the Personal Information Subject in accordance with the Personal Information Protection Law of the People's Republic of China.

Article 6 Remedies

1. The Overseas Recipient shall identify a contact person who is authorized to respond to enquiries or complaints concerning the handling of Personal Information, and it shall promptly deal with any enquiries or complaints from the Personal Information Subject. The Overseas Recipient shall notify the Personal Information Handler of the contact information and shall inform the Personal Information Subject of the contact information in a manner which is easy to understand, by separate notice or announcement on its website. To be specific: The contact person who is authorized to respond to enquiries or complaints concerning the handling of Personal Information is the Data Protection Officer of the Overseas Recipient, that can be contacted over the phone number and email address published on the website of the Overseas Recipient. For more details, see Appendix "CAC", that will be or is filed with the local CAC.

2. If a dispute arises between either Party and the Personal Information Subject with respect to the performance of this Contract, such Party shall notify the other Party and the Parties shall cooperate to resolve the dispute.

3. If the dispute cannot be resolved amicably and the Personal Information Subject exercises the rights as a third-party beneficiary in accordance with Article 5, the Overseas Recipient shall accept that the Personal Information Subject may safeguard his/her rights through either of the following means:

   (1) lodging a complaint with the Regulatory Authority; and

   (2) bringing a lawsuit to the court specified in Article 6.5.

4. The Parties agree that when the Personal Information Subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, if the Personal Information Subject chooses to apply the Relevant Laws and Regulations of the People's Republic of China, such choice shall prevail.

5. The parties agree that if the Personal Information Subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, the Personal Information Subject may file a lawsuit with a competent court in accordance with the Civil Procedure Law of the People's Republic of China.

6. The Parties agree that the choices made by the Personal Information Subject to safeguard his/her rights will not impair the rights of the Personal Information Subject to seek remedies in accordance with other laws and regulations.

Article 7 Termination of the Contract

© All rights reserved by Heiko Maniero.

1. If the Overseas Recipient breaches the obligations specified in this Contract or the Overseas Recipient is unable to perform this Contract due to a change in the policies and regulations on Personal Information protection in the Overseas Recipient's country or region (including amendment to the laws or adoption of compulsory measures in the Overseas Recipient's country or region), the Personal Information Handler may suspend the provision of Personal Information to the Overseas Recipient until the breach is corrected or the Contract is terminated.

2. In case of any of the following circumstances, the Personal Information Handler shall be entitled to terminate this Contract and notify the Regulatory Authority where necessary:

   (1) where the Personal Information Handler has suspended the provision of Personal Information to the Overseas Recipient for more than one month in accordance with Article 7.1;

   (2) the Overseas Recipient's compliance with this Contract will violate the laws and regulations of its own country or region;

   (3) the Overseas Recipient seriously or persistently breaches the obligations under this Contract;

   (4) the Overseas Recipient or the Personal Information Handler have breached this Contract pursuant to a final decision of a competent court or the regulatory body supervising the Overseas Recipient; and

   The Overseas Recipient may also terminate this Contract in case of sub-paragraph (1), (2) or (4) of above.

3. The Contract may be terminated upon mutual agreement by the Parties, provided that such termination shall not exempt the Parties from the obligations of protecting Personal Information during the handling of the Personal Information.

4. If the Contract is terminated, the Overseas Recipient shall promptly return or delete the Personal Information (including all back-up copies) received hereunder and provide the Personal Information Handler with a written statement. If it is technically difficult to delete the Personal Information, any handling of the Personal Information, other than the storage and taking necessary security protection measures, shall be ceased.

Article 8 Liability for Breach of the Contract

1. Each Party shall be liable to the other Party for any damage as a result of its breach of this Contract.

2. Each Party shall bear civil liabilities to the Personal Information Subject if its breach of this Contract infringes the rights of the Personal Information Subject, without prejudice to the administrative, criminal or other legal liabilities that shall be assumed by the Personal Information Handler under the Relevant Laws and Regulations.

3. The Parties shall assume joint and several liability in accordance with the law. The Personal Information Subject shall have the right to request each Party or the Parties to assume liability. When the liability assumed by one Party exceeds the liability such Party shall be assumed, it shall have the right to claim against the other Party accordingly.

Article 9 Miscellaneous

1. If this Contract conflicts with any other legal documents existing between the Parties, the provisions of this Contract shall prevail.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

2. The formation, validity, performance and interpretation of this Contract and any dispute between the Parties arising from this Contract shall be governed by the Relevant Laws and Regulations of the People's Republic of China.

3. All notices shall be promptly transmitted or posted by electronic mail, cable, telex, facsimile (confirmation copy sent by airmail), or registered airmail to (specified address in the Main Agreement or such other address as may be substituted for such address by written notice). Receipt of any notice under this Contract shall be deemed to have been received seven days after its postmark-date in the case of registered airmail and three working days after dispatch in the case of e-mail, cable, telex or facsimile transmission.

4. Any dispute arising from this Contract between the Parties, the Personal Information Handler and the Overseas Recipient, as well as a claim by either Party against the other for recovery of compensation already paid to the Personal Information Subject, shall be resolved by the Parties through negotiation; if such negotiation fails, either Party may adopt any of the following methods to resolve the dispute (check the box for the chosen arbitration institution, if arbitration is required):

   (1) Arbitration. The dispute shall be submitted to:

   ☐ China International Economic and Trade Arbitration Commission
   ☐ China Maritime Arbitration Commission
   ☐ Beijing Arbitration Commission (Beijing International Arbitration Center)
   ☐ Shanghai International Arbitration Center
   X Other arbitration institutions that are members of the Convention on the Recognition and Enforcement of Overseas Arbitral Awards

   The arbitration shall be conducted in Munich, Germany (the place of arbitration) in accordance with its arbitration rules then in force.

   (2) Litigation. Submit the dispute to a Chinese court with jurisdiction in accordance with the applicable laws.

5. This Contract shall be interpreted in accordance with Relevant Laws and Regulations and shall not be interpreted in a manner inconsistent with the rights and obligations set forth in Relevant Laws and Regulations.

6. This Contract shall be executed in two originals, and the Parties, the Personal Information Handler and the Overseas Recipient, shall each hold one original(s), with equal legal effect.

   This contract is signed or concluded online (implemented as terms and conditions and is and original and valid without signature).

Personal Information Handler: Authorized Person, that signed the Main Agreement

Date: Date of Main Agreement

Overseas Recipient: Authorized Person, that signed the Main Agreement

Date: Date of Main Agreement

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Appendix I

Description of the Outbound Cross-border Transfer of Personal Information

The details of the outbound cross-border transfer of Personal Information under this Contract are as follows:

1. Purpose of handling: see APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER

2. Method of handling: published as “Nature of (sub-) processing” in APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER

3. The scale of Personal Information to be transferred overseas: Processing and transfer on a small scale. For more details, see Appendix "CAC", that will be or is filed with the local CAC.

4. Type of Personal Information to be transferred overseas (please refer to the *Information Security Technologies - Personal Information Security Specifications (GB/T 35273)* and relevant standards):

   Personal Information (3.1 in GB/T 35273-2020)
   PI Subject (3.3 in GB/T 35273-2020)
   PI Controller (3.4 in GB/T 35273-2020)
   Explicit consent (3.6 in GB/T 35273-2020)
   Consent (3.7 in GB/T 35273-2020)
   Personalized display (3.16 in GB/T 35273-2020)
   Business function (3.17 in GB/T 35273-2020)

   For more details, see Appendix "CAC", that will be or is filed with the local CAC.

5. Type of Sensitive Personal Information to be transferred abroad (please refer to the *Information Security Technologies - Personal Information Security Specifications (GB/T 35273)* and relevant standards, if applicable): None.

6. The Overseas Recipient transfers Personal Information only to the following third parties outside the People's Republic of China (if applicable): N/A.

7. Method of transfer: Online Transfer.

8. Retention period after the cross-border transfer:

   From date of Main Agreement to Date of Termination of Main Agreement (which cannot be determined yet).

9. Storage location after the outbound cross-border transfer: Office und legal entity address of Overseas Recipient, or its sub-processors storage locations.

10. Other matters (to be filled in as appropriate): None.

Appendix II

Other Terms as Agreed by the Parties (If Necessary): None.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Powered by ICB International Certification Body.
Document Owner: Heiko Maniero.
Information Contained: Business Data
© All rights reserved by Heiko Maniero.
Approved by: Heiko Maniero, Ulrich Baumann.
Date: 2025-05-05

Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China)

为了确保境外接收方处理个人信息的活动达到中华人民共和国相关法律法规规定的个人信息保护标准，明确个人信息处理者和境外接收方个人信息保护的权利和义务，经双方协商一致，订立本合同。

双方确认并同意，本合同的中文版本为双方签订的正式版本。 非正式的英文翻译版本仅供无法阅读中文的人士理解参考。 如果双方同意签订本合同的英文版本，该等同意应被理解为双方已经签订了本合同的中文版本。

个人信息处理者：见附件 7-相关方名单

地址：见附件 7-相关方名单

联系方式：见附件 7-相关方名单

联系人：见附件 7-相关方名单　　职务：见附件 7-相关方名单

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

境外接收方：见附件 7-相关方名单

地址：见附件 7-相关方名单

联系方式：见附件 7-相关方名单

联系人：见附件 7-相关方名单 职务：见附件 7-相关方名单

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

个人信息处理者与境外接收方依据本合同约定开展个人信息出境活动，与此活动相关的商业行为，双方【已】/【约定】于【主协议签订日期】订立一份商业合同，即主协议。

本合同正文根据《个人信息出境标准合同办法》的要求拟定，在不与本合同正文内容相冲突的前提下，双方如有其他约定可在附录二中详述，附录构成本合同的组成部分。

第一条 定义

在本合同中，除上下文另有规定外：

（一）"个人信息处理者"是指在个人信息处理活动中自主决定处理目的、处理方式的，向中华人民共和国境外提供个人信息的组织、个人。

（二）"境外接收方"是指在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人。

（三）个人信息处理者或者境外接收方单称"一方"，合称"双方"。

（四）"个人信息主体"是指个人信息所识别或者关联的自然人。

（五）"个人信息"是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

（六）"敏感个人信息"是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

（七）"监管机构"是指中华人民共和国省级以上网信部门。

© All rights reserved by Heiko Maniero.

（八）"相关法律法规"是指《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国民法典》《中华人民共和国民事诉讼法》《个人信息出境标准合同办法》等中华人民共和国法律法规。

（九）本合同其他未定义术语的含义与相关法律法规规定的含义一致。

第二条 个人信息处理者的义务

个人信息处理者应当履行下列义务：

（一）按照相关法律法规规定处理个人信息，向境外提供的个人信息仅限于实现处理目的所需的最小范围。

（二）向个人信息主体告知境外接收方的名称或者姓名、联系方式、附录一"个人信息出境说明"中处理目的、处理方式、个人信息的种类、保存期限，以及行使个人信息主体权利的方式和程序等事项。向境外提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

（三）基于个人同意向境外提供个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

（四）向个人信息主体告知其与境外接收方通过本合同约定个人信息主体为第三方受益人，如个人信息主体未在 30 日内明确拒绝， 则可以依据本合同享有第三方受益人的权利。

（五）尽合理地努力确保境外接收方采取如下技术和管理措施

（综合考虑个人信息处理目的、个人信息的种类、规模、范围及敏感程度、传输的数量和频率、个人信息传输及境外接收方的保存期限等可能带来的个人信息安全风险），以履行本合同约定的义务：详见附件 9 – 技术和管理措施

（六）根据境外接收方的要求向境外接收方提供相关法律规定和技术标准的副本。

（七）答复监管机构关于境外接收方的个人信息处理活动的询问。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

（八）按照相关法律法规对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。重点评估以下内容：

1.个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性。

2.出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险。

3.境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全。

4.个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等。

5.按照本合同第四条评估当地个人信息保护政策和法规对合同履行的影响。

6.其他可能影响个人信息出境安全的事项。保

存个人信息保护影响评估报告至少 3 年。

（九）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（十）对本合同义务的履行承担举证责任。

（十一）根据相关法律法规要求，向监管机构提供本合同第三条第十一项所述的信息，包括所有合规审计结果。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

第三条 境外接收方的义务

境外接收方应当履行下列义务：

（一）按照附录一“个人信息出境说明”所列约定处理个人信息。如超出约定的处理目的、处理方式和处理的个人信息种类，基于个人同意处理个人信息的，应当事先取得个人信息主体的单独同意；涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。

（二）受个人信息处理者委托处理个人信息的，应当按照与个人信息处理者的约定处理个人信息，不得超出与个人信息处理者约定的处理目的、处理方式等处理个人信息。

（三）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（四）采取对个人权益影响最小的方式处理个人信息。

（五）个人信息的保存期限为实现处理目的所必要的最短时间， 保存期限届满的，应当删除个人信息（包括所有备份）。受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销或者终止的，应当将个人信息返还个人信息处理者或者予以删除，并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

（六）按下列方式保障个人信息处理安全：

1.采取包括但不限于本合同第二条第五项的技术和管理措施，并定期进行检查，确保个人信息安全。

2.确保授权处理个人信息的人员履行保密义务，并建立最小授权的访问控制权限。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

（七）如处理的个人信息发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问，应当开展下列工作：

1.及时采取适当补救措施，减轻对个人信息主体造成的不利影响。

2.立即通知个人信息处理者，并根据相关法律法规要求报告监管机构。通知应当包含下列事项：

（1）发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问的个人信息种类、原因和可能造成的危害。

（2）已采取的补救措施。

（3）个人信息主体可以采取的减轻危害的措施。

（4）负责处理相关情况的负责人或者负责团队的联系方式。

3.相关法律法规要求通知个人信息主体的，通知的内容包含本项第2目的事项。受个人信息处理者委托处理个人信息的，由个人信息处理者通知个人信息主体。

4.记录并留存所有与发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问有关的情况，包括采取的所有补救措施。

（八）同时符合下列条件的，方可向中华人民共和国境外的第三方提供个人信息：

1.确有业务需要。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

2.已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向第三方提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

3.基于个人同意处理个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

4.与第三方达成书面协议，确保第三方的个人信息处理活动达到中华人民共和国相关法律法规规定的个人信息保护标准，并承担因向中华人民共和国境外的第三方提供个人信息而侵害个人信息主体享有权利的法律责任。

5.根据个人信息主体的要求向个人信息主体提供该书面协议的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对该书面协议相关内容进行适当处理。

© All rights reserved by Heiko Maniero.

（九）受个人信息处理者委托处理个人信息，转委托第三方处理的，应当事先征得个人信息处理者同意，要求该第三方不得超出本合同附录一"个人信息出境说明"中约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督。

（十）利用个人信息进行自动化决策的，应当保证决策的透明度和结果公平、公正，不得对个人信息主体在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人信息主体进行信息推送、商业营销的，应当同时提供不针对其个人特征的选项，或者向个人信息主体提供便捷的拒绝方式。

（十一）承诺向个人信息处理者提供已遵守本合同义务所需的必要信息，允许个人信息处理者对必要数据文件和文档进行查阅，或者对本合同涵盖的处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利。

（十二）对开展的个人信息处理活动进行客观记录，保存记录至少3 年，并按照相关法律法规要求直接或者通过个人信息处理者向监

管机构提供相关记录文件。

（十三）同意在监督本合同实施的相关程序中接受监管机构的监督管理，包括但不限于答复监管机构询问、配合监管机构检查、服从监管机构采取的措施或者作出的决定、提供已采取必要行动的书面证明等。

第四条
境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响

（一）双方应当保证在本合同订立时已尽到合理注意义务，未发现境外接收方所在国家或者地区的个人信息保护政策和法规（包括任何提供个人信息的要求或者授权公共机关访问个人信息的规定）影响境外接收方履行本合同约定的义务。

（二）双方声明，在作出本条第一项的保证时，已经结合下列情形进行评估：

1.出境的具体情况，包括个人信息处理目的、传输个人信息的种类、规模、范围及敏感程度、传输的规模和频率、个人信息传输及境外接收方的保存期限、境外接收方此前类似的个人信息跨境传输和处理相关经验、

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

境外接收方是否曾发生个人信息安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况。

2.境外接收方所在国家或者地区的个人信息保护政策和法规，包括下列要素：

（1） 该国家或者地区现行的个人信息保护法律法规及普遍适用的标准。

（2） 该国家或者地区加入的区域性或者全球性的个人信息保护方面的组织，以及所作出的具有约束力的国际承诺。

（3） 该国家或者地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。

3.境外接收方安全管理制度和技术手段保障能力。

（三）境外接收方保证，在根据本条第二项进行评估时，已尽最大努力为个人信息处理者提供了必要的相关信息。

（四）双方应当记录根据本条第二项进行评估的过程和结果。

（五）因境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，境外接收方应当在知道该变化后立即通知个人信息处理者。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

（六）境外接收方接到所在国家或者地区的政府部门、司法机构关于提供本合同项下的个人信息要求的，应当立即通知个人信息处理者。

第五条 个人信息主体的权利

双方约定个人信息主体作为本合同第三方受益人享有以下权利：

（一）个人信息主体依据相关法律法规，对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理， 有权要求查阅、复制、更正、补充、删除其个人信息，有权要求对其个人信息处理规则进行解释说明。

（二）当个人信息主体要求对已经出境的个人信息行使上述权利时，个人信息主体可以请求个人信息处理者采取适当措施实现，或者直接向境外接收方提出请求。个人信息处理者无法实现的，应当通知并要求境外接收方协助实现。

（三）境外接收方应当按照个人信息处理者的通知，或者根据个人信息主体的请求，在合理期限内实现个人信息主体依照相关法律法规所享有的权利。

境外接收方应当以显著的方式、清晰易懂的语言真实、准确、完整地告知个人信息主体相关信息。

（四）境外接收方拒绝个人信息主体的请求的，应当告知个人信息主体其拒绝的原因，以及个人信息主体向相关监管机构提出投诉和寻求司法救济的途径。

（五）个人信息主体作为本合同第三方受益人有权根据本合同条款向个人信息处理者和境外接收方的一方或者双方主张并要求履行本合同项下与个人信息主体权利相关的下列条款：

1.第二条，但第二条第五项、第六项、第七项、第十一项除外。

2.第三条，但第三条第七项第 2 目和第 4 目、第九项、第十一项、第十二项、第十三项除外。

3.第四条，但第四条第五项、第六项除外。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

4. 第五条。

5. 第六条。

6. 第八条第二项、第三项。

7. 第九条第五项。

上述约定不影响个人信息主体依据《中华人民共和国个人信息保护法》享有的权益。

第六条 救济

（一）境外接收方应当确定一个联系人，授权其答复有关个人信息处理的询问或者投诉，并应当及时处理个人信息主体的询问或者投诉。境外接收方应当将联系人信息告知个人信息处理者，并以简洁易懂的方式，通过单独通知或者在其网站公告，告知个人信息主体该联系人信息，具体为：境外接收方授权答复有关个人信息处理的询问或者投诉的联系人为境外接收方的数据保护人员。个人信息主体可通过境外接收方网站公布的电话及电子邮件联系该等人员。更多详情，请参见附件"中国互联网信息办公室"，该文件将向或已向当地的中国互联网信息办公室备案。

（二）一方因履行本合同与个人信息主体发生争议的，应当通知另一方，双方应当合作解决争议。

（三）争议未能友好解决，个人信息主体根据第五条行使第三方受益人的权利的，境外接收方接受个人信息主体通过下列形式维护权利：

1. 向监管机构投诉。

2. 向本条第五项约定的法院提起诉讼。

（四）双方同意个人信息主体就本合同争议行使第三方受益人权利，个人信息主体选择适用中华人民共和国相关法律法规的，从其选择。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

（五）双方同意个人信息主体就本合同争议行使第三方受益人权利的，个人信息主体可以依据《中华人民共和国民事诉讼法》向有管辖权的人民法院提起诉讼。

（六）双方同意个人信息主体所作的维权选择不会减损个人信息主体根据其他法律法规寻求救济的权利。

第七条 合同解除

（一）境外接收方违反本合同约定的义务，或者境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，个人信息处理者可以暂停向境外接收方提供个人信息，直到违约行为被改正或者合同被解除。

（二）有下列情形之一的，个人信息处理者有权解除本合同，并在必要时通知监管机构：

1.个人信息处理者根据本条第一项的规定暂停向境外接收方提供个人信息的时间超过 1 个月。

2.境外接收方遵守本合同将违反其所在国家或者地区的法律规定。

3.境外接收方严重或者持续违反本合同约定的义务。

4.根据境外接收方的主管法院或者监管机构作出的终局决定，境外接收方或者个人信息处理者违反了本合同约定的义务。

在本项第 1 目、第2 目、第4 目的情况下，境外接收方可以解除本合同。

（三）经双方同意解除本合同的，合同解除不免除其在个人信息处理过程中的个人信息保护义务。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

（四）合同解除时，境外接收方应当及时返还或者删除其根据本合同所接收到的个人信息（包括所有备份），并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

第八条 违约责任

（一）双方应就其违反本合同而给对方造成的损失承担责任。

（二）任何一方因违反本合同而侵害个人信息主体享有的权利， 应当对个人信息主体承担民事法律责任，且不影响相关法律法规规定个人信息处理者应当承担的行政、刑事等法律责任。

（三）双方依法承担连带责任的，个人信息主体有权请求任何一方或者双方承担责任。一方承担的责任超过其应当承担的责任份额时，有权向另一方追偿。

第九条 其他

（一）如本合同与双方订立的任何其他法律文件发生冲突，本合同的条款优先适用。

（二）本合同的成立、效力、履行、解释、因本合同引起的双方间的任何争议，适用中华人民共和国相关法律法规。

（三）发出的通知应当以电子邮件、电报、电传、传真（以航空信件寄送确认副本）或者航空挂号信发往（具体地址以主协议中载明的地址为准）

或者书面通知取代该地址的其它地址。如以航空挂号信寄出本合同项下的通知，在邮戳日期后的 7 天应当视为收讫；如以电子邮件、电报、电传或者传真发出，在发出以后的 3 个工作日应当视为收讫。

（四）双方因本合同产生的争议以及任何一方因先行赔偿个人信息主体损害赔偿责任而向另一方的追偿，双方应当协商解决；协商解决不成的，任何一方可以采取下列第_种方式加以解决（如选择仲裁，请勾选仲裁机构）：

1.仲裁。将该争议提交

□中国国际经济贸易仲裁委员会

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

□中国海事仲裁委员会

□北京仲裁委员会（北京国际仲裁中心）

□上海国际仲裁中心

√其他《承认及执行外国仲裁裁决公约》成员的仲裁机构_____

按其届时有效的仲裁规则在 德国慕尼黑 进行仲裁；

2.诉讼。依法向中华人民共和国有管辖权的人民法院提起诉讼。

（五）本合同应当按照相关法律法规的规定进行解释，不得以与相关法律法规规定的权利、义务相抵触的方式解释本合同。

（六）本合同正本一式贰份，双方各执 壹份，其法律效力相同。本合同于线上签订或签署（且可作为原始、有效的条款和条件执行，无需签名）

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

个人信息处理者：[签署主协议的授权签字人]_____

_____年_____月_____日[主协议签署日期]

境外接收方：[签署主协议的授权签字人]_____

_____年_____月_____日[主协议签署日期]

附录一

个人信息出境说明

根据本合同向境外提供个人信息的详情约定如下：

（一）处理目的：见附件 8-处理或传输说明

（二）处理方式：见附录 8-处理或传输说明中的“（次级）处理性质”

（三）出境个人信息的规模：小规模处理及传输个人信息。更多详情，请参见附件"中国互联网信息办公室"，该文件将向或已向当地的中国互联网信息办公室备案。

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

（四）出境个人信息种类（参 考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）：

个人信息（参考 GB/T 35273-2020 第 3.1 条）

个人信息主体（参考 GB/T 35273-2020 第 3.3 条）

个人信息控制者（参考 GB/T 35273-2020 第 3.4 条）

明示同意（参考 GB/T 35273-2020 第 3.6 条）

授权同意（参考 GB/T 35273-2020 第 3.7 条）

个性化展示（参考 GB/T 35273-2020 第 3.16 条）

业务功能（参考 GB/T 35273-2020 第 3.17 条）

更多详情，请参见附件"中国互联网信息办公室"，该文件将向或已向当地的中国互联网信息办公室备案。

（五）出境敏感个人信息种类（如适用，参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）：无

（六）境外接收方只向以下中华人民共和国境外第三方提供个人信息（如适用）：不适用

（七）传输方式：网络在线传输

（八）出境后保存期限：

自主协议生效之日至主协议终止之日（待确定）

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

（九）出境后保存地点：境外接收方的办公地址或注册地址，或其次级信息处理者的保存地点。

（十）其他事项（视情况填写）：无

附录二

双方约定的其他条款（如需要）

无。

© All rights reserved by Heiko Maniero.

Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China)

This Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China) (**Agreement**) is concluded on the same date as the Services Agreement (as defined below) and is concluded by and between

(1) the **Personal Information Handler**, named with its Company details as a Party in the Services Agreement (as defined below), and

(2) the **Entrusted Person**, named with its Company details as a Party in the Services Agreement (as defined below).

(together the **Parties**)

1. Preamble

1.1 The Entrusted Person is a provider of professional services (**Services**) and/or provides its Services as a Joint-Controller and is based in the People's Republic of China. The Personal Information Handler is also based in the People's Republic of China. The Parties entered into an agreement which describes the Services provided by the Entrusted Person acting on behalf of the Personal Information Handler, or acting jointly with the Personal Information Handler, 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 Entrusted Person, or jointly by the Entrusted Person and the Personal Information Handler, 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.

1.3 This Agreement applies to all activities involving the Handling of Personal Information of natural persons within the borders of the People's Republic of China.

2. Definitions and interpretation

2.1 **PIPL** means the Personal Information Protection Law of the People's Republic of China, passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021, that entered into force on November 1, 2021, as amended or superseded from time to time. The legal definitions from Article 73 PIPL shall apply.

2.2 **Personal Information** means all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization Handling.

2.3 **Personal Information Handling** includes Personal Information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

2.4 **Sensitive Personal Information** means Personal Information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the Personal Information of minors under the age of 14.

2.5 **Data Protection Officer** means the Personal Information Protection Officer.

2.6 **Joint-Controller** means an Entrusted Person that qualifies as a Second PI Handler that jointly decides with the Personal Information Handler on the Personal Information Handling purposes and Handling methods.

2.7 **Data Protection Legislation** means the Personal Information Protection Law of the People's Republic of China as well as any regulation adopted, published, administered, implemented, or enforced by the Government of the People's Republic of China, as amended or superseded from time to time, and any related case-law.

3. General Obligations

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

3.2 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, without prejudice to the generality of this Clause, the Personal Information Handler will ensure that it has all necessary Consents and notices in place to enable the lawful transfer of the Personal Information to the Entrusted Person in connection with the performance of its obligations under the Services Agreement.

3.3 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, to the extent within the Personal Information Handler's control having regard to the Entrusted Person's obligations under the Services Agreement, the Personal Information Handler shall be responsible for the accuracy and quality of the Personal Information transferred to the Entrusted Person.

3.4 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, the Entrusted Person shall have an ongoing obligation throughout the duration of the Services Agreement to identify and report to the Personal Information Handler best practice techniques relating to the Handling of Personal Information and the emergence of new and evolving technologies which could improve the availability, confidentiality and/or integrity of the Handling of Personal Information.

4. Sub-Handlers

4.1 If the Handling involves more than one Entrusted Person (**Sub-Handler**), the Handling must be made in accordance with a contract or written agreement whereby their obligations, responsibilities and roles related to the Handling are clearly defined.

4.2 The Personal Information Handler hereby authorizes the Entrusted Person to appoint Sub-Handlers (General Written Authorization). The Entrusted Person shall name all its Sub-Handlers to the Personal Information Handler prior to initiation of Handling.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

4.3 With respect to each Sub-Handler appointed by the Entrusted Person under General Written Authorization, the Entrusted Person shall (a) undertake appropriate due diligence prior to the Handling of Personal Information by such Sub-Handler to ensure that it is capable of providing the level of protection for Personal Information required by the terms of the Services Agreement and this Agreement, and (b) enter into a written Agreement with the Sub-Handler incorporating terms which are substantially similar (and no less onerous) than those set out in this Agreement and which meet the requirements stipulated by PIPL.

4.4 In regard to the Agreement between the Personal Information Handler and the Entrusted Person, the Entrusted Person remain fully liable to the Personal Information Handler for all acts or omissions of its Sub-Handlers as though they were its own.

4.5 To the extent that the Entrusted Person has already appointed any Sub-Handlers prior to the Handling of any Personal Information under this Agreement, the Entrusted Person shall ensure that its obligations under this Section are met.

4.6 Where the Entrusted Person proposes any changes concerning the addition or replacement of any Sub-Handler, it shall notify the Personal Information Handler in writing as soon as reasonably practicable prior to implementing such change specifying (a) the name of any Sub-Handler which it proposes to add or replace, and (b) the Handling activity or activities affected by the proposed change, and (c) the reasons for the proposed change, and (d) the proposed date for implementation of the change.

4.7 If within thirty (30) days of receipt of a notice the Personal Information Handler (acting reasonably and in good faith) notifies the Entrusted Person in writing of any objections to the proposed change, the Parties shall use their respective reasonable endeavors to resolve the Personal Information Handler's objections. Where such resolution cannot be agreed within thirty (30) days of the Entrusted Person's receipt of the Personal Information Handler's objections (or such longer period as the Parties may agree in writing) the Personal Information Handler may, notwithstanding the terms of the Services Agreement, serve written notice on the Entrusted Person to terminate the Services Agreement (to the extent that the provision of the Services are or would be affected by the proposed change).

4.8 The Entrusted Person shall, upon the Personal Information Handler's request, provide the Personal Information Handler with copies of any Agreements between the Entrusted Person and its Sub-Handlers (which may be redacted to remove information which is confidential to the Entrusted Person and/or its Sub-Handlers and which is not relevant to the terms of this Agreement).

5. Obligations of the Entrusted Person (Art. 5, 6, 7, 8, 9, and 10 PIPL)

5.1 The Entrusted Person shall observe the principles of legality, propriety, necessity, and sincerity for Personal Information Handling. The Entrusted Person shall not Handle Personal Information in misleading, swindling, coercive, or other such ways.

5.2 The Entrusted Person shall Handle Personal Information only for clear and reasonable purposes, that shall be directly related to the Handling purpose, using methods with the smallest influence on individual rights and interests.

5.3 The Entrusted Person shall limit the collection of Personal Information to the smallest scope for realizing the Handling purpose, and not collect Personal Information excessive.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

5.4 The Entrusted Person shall observe the principles of openness and transparency in the Handling of Personal Information, disclose the rules for Handling Personal Information and clearly indicate the purpose, method, and scope of Handling.

5.5 The Entrusted Person shall ensure the quality of Personal Information and avoid adverse effects on individual rights and interests from inaccurate or incomplete Personal Information.

5.6 The Entrusted Person shall bear full responsibility for its own Personal Information Handling activities and adopt all necessary measures to safeguard the security of the Personal Information it Handles. The Parties agreed on the required technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

5.7 The Entrusted Person shall not illegally collect, use, process, or transmit other persons' Personal Information, or illegally sell, buy, provide, or disclose other persons' Personal Information, or engage in Personal Information Handling activities harming national security or the public interest.

6. Consent and Legal Grounds (Art. 13, 14, 15, and 16 PIPL)

6.1 In principle, the Entrusted Person shall Handle Personal Information with the individual's consent.

6.2 However, the Entrusted Person may Handle Personal Information without the individual's consent in cases (1) where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts, or (2) where necessary to fulfill statutory duties and responsibilities or statutory obligations, or (3) where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions, or (4) Handling Personal Information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest, or (5) when Handling Personal Information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of PIPL, or (6) in other circumstances provided in laws and administrative regulations.

6.3 Where Personal Information is Handled by the Entrusted Person based on the individual's consent, said consent shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Where laws or administrative regulations provide that separate consent or written consent shall be obtained to Handle Personal Information, those provisions are to be followed by the Entrusted Person.

6.4 Where the Entrusted Person changes the purpose of Personal Information Handling, the Handling method, or the categories of Handled Personal Information, the Entrusted Person shall obtain the individual's consent again.

6.5 Where Personal Information is Handled by the Entrusted Person based on the individual's consent, the Entrusted Person shall inform individuals about their right to rescind their consent. The Entrusted Person shall provide a convenient way to withdraw consent.

6.6 The Entrusted Person shall not refuse to provide products or services on the basis that an individual does not consent to the Handling of its Personal Information or rescinds its consent,

© All rights reserved by Heiko Maniero.

except where Handling Personal Information is necessary for the provision of products or services.

7. Transparency towards and Notifications of Individuals (Art. 17 and 18 PIPL)

7.1 The Entrusted Person shall, before Handling Personal Information, explicitly notify individuals truthfully, accurately, and fully, using clear and easily understood language, namely about (1) the name or personal name and contact method of the Entrusted Person, and (2) the purpose of Personal Information Handling and the Handling methods, the categories of Handled Personal Information, and the retention period, and (3) methods and procedures for individuals to exercise the rights provided by PIPL, and (4) other items that laws or administrative regulations provide shall be notified. Where the Entrusted Person Handles Personal Information exclusively for the Personal Information Handler, the Entrusted Person shall, before Handling Personal Information, explicitly notify and inform individuals by means of the Transparency Document that was published on the website of the Personal Information Handler.

7.2 Where a change occurs in the matters provided in the previous paragraph, individuals shall be notified by the Entrusted Person about the change.

7.3 Where the Entrusted Person notify the matters as provided under Section 7.1 through the method of formulating Personal Information Handling rules, the Handling rules shall be made public disclosed and convenient to read and store.

7.4 The Entrusted Person may not notify individuals about the items provided in Section 7.1 under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary.

7.5 Under emergency circumstances, where it is impossible to notify individuals in a timely manner in order to protect natural persons' lives, health, and the security of their property, the Entrusted Person shall notify them after the conclusion of the emergency circumstances.

8. Retention (Art. 19 PIPL)

8.1 The Entrusted Person shall, except where laws or administrative regulations provide otherwise, use the shortest period necessary to realize the purpose of the Personal Information Handling as retention period.

9. Rights and Obligations of each Party if the Parties act as Joint-Controllers (Art. 20 PIPL)

9.1 This Section 9 shall apply only if the Personal Information Handler and the Entrusted Person act jointly as Joint-Controllers. The Clauses of Section 9 of this Agreement shall supersede any conflicting Clauses in other Sections of this Agreement regarding to both Joint-Controllers.

9.2 This Agreement does not influence an individual's rights to demand any of the Joint-Controllers to perform under PIPL provisions.

9.3 Where the Joint-Controllers harm Personal Information rights and interests, resulting in damages, they bear joint liability according to the law.

9.4 The Joint-Controllers determined the scope, subject, purpose and nature of the Handling, the type of Personal Information and categories of individuals in the Services Agreement and/or in APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

9.5 The Joint-Controllers shall jointly ensure compliance with Data Protection Legislation when Handling Personal Information. Both controllers are equally responsible for the legality and lawfulness of joint Handling.

9.6 The Personal Information Handler undertakes to provide the individuals with all information regarding their rights under PIPL. The Personal Information Handler acts as the contact point for individuals.

9.7 The Joint-Controllers shall bear joint responsibility for Personal Information Handling activities and adopt all necessary measures to safeguard the security of the Personal Information they Handle jointly. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

9.8 The Joint-Controllers shall jointly appoint only Sub-Handlers which adopted necessary measures to safeguard the security of the Personal Information they Handle and comply with PIPL.

9.9 Each Joint-Controller shall appoint a Data Protection Officer. Both Data Protection Officers shall act jointly in good faith.

9.10 Where one of the Joint-Controllers provides a third party with Personal Information, that Joint-Controller shall notify individuals about the name or personal name of the recipient, their contact method, the Handling purpose, Handling method, and Personal Information categories, and obtain separate consent from the individuals.

9.11 Where one of the Joint-Controllers provides a third party with Personal Information, that third party shall Handle Personal Information within the scope of Handling purposes, Handling methods, Personal Information categories, etc. and when the third party is changing the original Handling purpose or Handling methods, that third party shall inform and obtain the individual's consent again.

10. General Obligations of the Entrusted Person (Art. 21 PIPL)

10.1 Where the Personal Information Handler entrust the Handling of Personal Information, it shall conclude an agreement with the Entrusted Person on the purpose for entrusted Handling, the time limit, the Handling method, categories of Personal Information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the Personal Information Handling activities of the Entrusted Person.

10.2 The time limit of Handling of Personal Information by the Entrusted Person is the duration of the Services Agreement. The protection measures are agreed on with APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

10.3 The Personal Information Handler published a "List of (sub) processors, recipients in third countries and international organizations" on its website. In this document, the "Purpose for entrusted Handling" is published as "Subject matter of (sub-) processing", the "Handling method" is published as "Nature of (sub-) processing", and the "Categories of Personal Information" are published as "Categories of Personal Data".

10.4 The Personal Information Handler is granted the right to conduct supervision of the Personal Information Handling activities of the Entrusted Person.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

10.5 The Entrusted Person shall Handle Personal Information exclusively according to this Agreement. The Entrusted Person shall not Handle Personal Information for Handling purposes or in Handling methods, etc., in excess of this Agreement.

10.6 If this Agreement does not take effect, is void, has been cancelled, or has been terminated, the Entrusted Person shall return the Personal Information to the Personal Information Handler or delete it, and may not retain it.

11. Mergers, separations, dissolution, declaration of bankruptcy, and other such reasons (Art. 22 PIPL)

11.1 The Entrusted Person shall not transfer any Personal Information Handled on behalf or for the Personal Information Handler due to mergers, separations, dissolution, declaration of bankruptcy, and other such reasons. Wherever such reason may occur, the Personal Information Handler is to be informed and shall decide on the transfer of Personal Information, the return of the Personal Information to the Personal Information Handler or the deletion of the Personal Information.

12. Notifications where Personal Information Handlers provide other Personal Information Handlers with the Personal Information they Handle (Art. 23 PIPL)

12.1 Where the Entrusted Person provide other Personal Information Handlers with the Personal Information it Handles, the Entrusted person shall notify individuals about the name or personal name of the recipient, their contact method, the Handling purpose, Handling method, and Personal Information categories, and obtain separate consent from the individual.

12.2 Where the Entrusted Person provide other Personal Information Handlers with the Personal Information it Handles, the Entrusted person shall make sure by means of a contract that all recipients that Handle Personal Information within the above-mentioned scope of Handling purposes, Handling methods, Personal Information categories, etc. and where recipients change the original Handling purpose or Handling methods, the Entrusted Person shall make sure by means of a contract, that the recipients obtain the individual's consent again.

13. Automated Decision-Making (Art. 24 PIPL)

13.1 The Entrusted Person shall not use any methods for or engage with any automated decision-making regarding the Personal Information that is Handled for or on behalf of the Personal Information Handler.

14. Non Disclosure of Personal Information (Art. 25 PIPL)

14.1 The Entrusted Person shall not disclose any Personal Information Handled on behalf of the Personal Information Handler to third parties. Sub-Handlers are not considered to be third parties.

15. Major influence on individual rights and interests (Art. 27 PIPL)

15.1 Where the Entrusted Person Handles Personal Information that has been disclosed by the persons themselves or was otherwise lawfully disclosed, except where the person clearly refuses, and that may have a major influence on individual rights and interests, the Entrusted Person shall obtain personal consent in accordance with the provisions of PIPL.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

16. Sensitive Personal Information (Art. 28, 29, 30, 31, and 32 PIPL)

16.1 In general, the Entrusted Person shall not Handle Sensitive Personal Information on behalf of the Personal Information Handler. However, if the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, it may do so only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures.

16.2 If the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall obtain the individual's separate consent. Where laws or administrative regulations provide that written consent shall be obtained for Handling Sensitive Personal Information, those provisions are to be followed by the Entrusted Person.

16.3 If the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall, in addition to the items set out in Article 17, Paragraph 1, of PIPL, also notify individuals of the necessity and influence on the individual's rights and interests of Handling the Sensitive Personal Information, except where PIPL provides that it is permitted not to notify the individuals.

16.4 In general, the Entrusted Person shall not Handle Personal Information of minors under the age of 14 on behalf of the Personal Information Handler. However, if the Entrusted Person would Handle Personal Information of minors under the age of 14 in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall obtain the consent of the parent or other guardian of the minor. Where the Entrusted Person Handle the Personal Information of minors under the age of 14, the Entrusted Person shall formulate specialized Personal Information Handling rules.

16.5 Where laws or administrative regulations provide that relevant administrative licenses shall be obtained or other restrictions apply to the Handling of Sensitive Personal Information, those provisions are to be followed by the Entrusted Person.

17. Cross-Border Provision of Personal Information (Art. 38, 39, 40, 41, 42 and 43 PIPL)

17.1 Where the Entrusted Person, on behalf of the Personal Information Handler, truly need to provide Personal Information outside the borders of the People's Republic of China for business or other such requirements, the Entrusted Person shall meet all requirements of PIPL.

17.2 In particular, in such case, the Entrusted Person shall meet one of the following conditions: (1) passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of PIPL, or (2) undergoing Personal Information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department, or (3) concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides, or (4) meet other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

17.3 Where treaties or international agreements that the People's Republic of China has concluded or acceded to contain relevant provisions such as conditions on providing personal data outside the borders of the People's Republic of China, those provisions may be carried out by the Entrusted Person.

17.4 The Entrusted Person shall adopt necessary measures to ensure that foreign receiving parties' Personal Information Handling activities reach the standard of Personal Information protection provided in PIPL.

17.5 Where the Entrusted Person provide Personal Information outside of the borders of the People's Republic of China, the Entrusted Person shall notify the individual about the foreign receiving side's name or personal name, contact method, Handling purpose, Handling methods, and Personal Information categories, as well as ways or procedures for individuals to exercise the rights provided in PIPL with the foreign receiving side, and other such matters, and obtain individuals' separate consent.

17.6 If the Entrusted Person is a Critical information infrastructure operator that is Handling Personal Information and reaches the quantities provided by the State cybersecurity and informatization department the Entrusted Person shall store Personal Information collected and produced within the borders of the People's Republic of China domestically. Where the Entrusted Person need to provide it abroad, the Entrusted Person shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cybersecurity and informatization department provisions permit that security assessment not be conducted, those provisions are to be followed by the Entrusted Person.

17.7 Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to Handle foreign judicial or law enforcement authorities' requests regarding the provision of Personal Information stored domestically. Without the approval of the competent authorities of the People's Republic of China, the Entrusted Person may not provide Personal Information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies.

17.8 The Entrusted Person shall observe the lists of the State cybersecurity and informatization department that contain foreign organizations or individuals with limitations or prohibitions regarding the provision of personal information to them and shall under no circumstances transfer or provide Personal Information to any foreign organization or individual that is named or included on such lists.

17.9 Where the People's Republic of China has adopted reciprocal measures against any country or region on the basis of actual circumstances, based on Art. 43 PIPL, the Entrusted Person shall comply with any such decision, and where required, without undue delay cease and desist any transfer to the respective country or region.

18. Individuals' Rights in Personal Information Handling Activities (Art. 44, 45, 46, 47, 48, 49, and 50 PIPL)

18.1 The Entrusted Person shall comply with its own obligations under Art. 44, 45, 46, 47, 48, 49, and 50 PIPL and inform the Personal Information Handler, with undue delay, fully about any individual that has contacted the Entrusted Person regarding any Rights in Personal Information

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Handling Activities relating to any Personal Information Handled on behalf of the Personal Information Handler.

18.2 Where the Entrusted Person Handles Personal Information on behalf of the Personal Information Handler, the Entrusted Person shall, before Handling Personal Information, inform individuals about their Rights in Personal Information Handling Activities regarding the Personal Information Handler by means of the Transparency Document published on the website of the Personal Information Handler.

19. Other Duties of the Entrusted Person (Art. 51, 52, 53, 54, 55, 56, 57, 58 and 59 PIPL)

19.1 The Entrusted Person shall, on the basis of the Personal Information Handling purpose, Handling methods, Personal Information categories, as well as the influence on individuals' rights and interests, possibly existing security risks, etc., adopt at least the following measures to ensure Personal Information Handling conforms to the provisions of laws and administrative regulations, and prevent unauthorized access as well as Personal Information leaks, distortion, or loss: (1) formulate internal management structures and operating rules, and (2) implement categorized management of Personal Information, and (3) adopt corresponding technical security measures such as encryption, de-identification, etc., and (4) reasonably determine operational limits for Personal Information Handling, and regularly conducting security education and training for employees, and (5) formulate and organize the implementation of Personal Information security incident response plans, and (6) take other measures provided in laws or administrative regulations.

19.2 If the Entrusted Person has reached the quantities provided by the State cybersecurity and informatization department, it shall appoint a Personal Information Protection Officer, to be responsible for supervising Personal Information Handling activities as well as adopted protection measures, etc., and shall disclose the methods of contacting the Personal Information Protection Officer, and report the personal names of the Officer and contact methods to the departments fulfilling Personal Information protection duties and responsibilities.

19.3 If the Entrusted Person engages a Personal Information Handler outside the borders of the People's Republic of China, the Entrusted Person shall make sure that the foreign Personal Information Handler has dedicated an entity or appointed a representative within the borders of the People's Republic of China that is responsible for matters related to the Personal Information which it Handles, and that the name of the relevant entity or the personal name of the representative and contact method, etc., was reported to the departments fulfilling personal information protection duties and responsibilities.

19.4 The Entrusted Person shall regularly engage in audits of their Personal Information Handling and compliance with laws and administrative regulations.

19.5 When one of the following circumstances is present, the Entrusted Person shall conduct a Personal Information Protection Impact Assessment in advance, and record the Handling situation: (1) Handling Sensitive Personal Information, or (2) Using Personal Information to conduct automated decision-making, or (3) Entrusting Personal Information Handling, providing Personal Information to other Personal Information Handlers, or disclosing Personal Information, or (4) Providing Personal Information abroad, or (5) other Personal Information Handling activities with a major influence on individuals.

19.6 The Entrusted Person shall include the following content in the Personal Information Protection Impact Assessment: (1) whether or not the Personal Information Handling purpose, Handling

© All rights reserved by Heiko Maniero.

method, etc., are lawful, legitimate, and necessary, and (2) the influence on individuals' rights and interests, and the security risks, and (3) whether protective measures undertaken are legal, effective, and suitable to the degree of risk. The Entrusted Person shall preserve the Personal Information Protection Impact Assessment Reports and Handling status records for at least three years.

19.7 Where a Personal Information leak, distortion, or loss occurs or might have occurred, the Entrusted Person shall immediately adopt remedial measures, and notify the Personal Information Handler to allow him to notify the departments fulfilling Personal Information protection duties and responsibilities and the individuals. The notification shall include the following items (1) the information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred, and (2) the remedial measures taken by the Personal Information Handler and measures individuals can adopt to mitigate harm, and (3) the contact method of the Entrusted Person.

19.8 If the Entrusted Person is providing important Internet platform services, that have a large number of users, and its business models are complex, the Entrusted Person shall fulfill the obligations in Art. 58 PIPL.

19.9 The Entrusted Persons shall, according to the provisions of PIPL and relevant laws and administrative regulations, take necessary measures to safeguard the security of the Personal Information it Handles, and assist the Personal Information Handler in fulfilling its obligations provided in PIPL.

20. Legal Liability (Art. 66 PIPL)

20.1 Where the Entrusted Person has Handled Personal Information in violation of PIPL or Personal Information is Handled by the Entrusted Person without fulfilling Personal Information protection duties in accordance with the provisions of PIPL, and the Entrusted Person acted on behalf of the Personal Information Handler, the Personal Information Handler is entitled to order correction, and order the provisional suspension or termination of service provision of the application programs unlawfully Handling Personal Information.

21. Compensation for infringements (Art. 69 PIPL)

21.1 Where the Entrusted Person Handled Personal Information, and such operation is infringing Personal Information rights and interests and results in harm, and the Entrusted Person cannot prove they are not at fault, the Entrusted Person shall bear compensation and take responsibility for the infringement. Responsibility to compensate for infringement shall be determined according to the resulting loss to the individual or the Personal Information Handler's resulting benefits. Where the loss to the individual and the Personal Information Handler's benefits are difficult to determine, a court may determine compensation according to practical conditions.

Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.