Auftragsverarbeitungsvertrag

Name der 1. Partei		**NTT**
Physische Adresse		
Postanschrift		
Rufnummer		
E-Mailadresse	de.info@global.ntt	
Unterschriften (die versichern, dass sie ordnungsgemäß zur Unterzeichnung bevollmächtigt sind)	_____ _____ Für und im Namen von NTT	
Name des Unterzeichners		
Titel des Unterzeichners		
Datum der Unterschrift		

Name der 2. Partei		**Kunde**
Physische Adresse		
Postanschrift		
Rufnummer		
E-Mailadresse		
Unterschrift (die versichern, dass sie ordnungsgemäß zur Unterzeichnung bevollmächtigt sind)	_____ Für und im Namen des Kunden	
Name des Unterzeichners		
Titel des Unterzeichners		
Datum der Unterschrift		

Aufsichtsbehörde	${Name der Aufsichtsbehörde} Falls oben nicht angegeben, ist die Standardaufsichtsbehörde die Aufsichtsbehörde des Landes, in dem der Kunde seinen Sitz hat, und wird unter Bezugnahme auf die Liste der Aufsichtsbehörden der EFTA-EWR-Staaten bestimmt, die Sie hier finden: https://edpb.europa.eu/about-edpb/about-edpb/members_en.

Mit der obigen Unterschrift bestätigt jede Partei, dass sie diesen Auftragsverarbeitungsvertrag sorgfältig gelesen und vollständig verstanden hat, und stimmt zu, an die Bedingungen dieses Auftragsverarbeitungsvertrags gebunden zu sein. Wenn eine elektronische Signatur zur Unterzeichnung dieses Auftragsverarbeitungsvertrags verwendet wurde (unabhängig von der Form der elektronischen Signatur), erklärt sich jede Partei damit einverstanden, dass diese Art der Unterzeichnung ihre Absicht, durch diesen

Auftragsverarbeitungsvertrag gebunden zu sein, ebenso schlüssig bestätigt, wie die handschriftliche Unterzeichnung durch jede Partei.

Inhalt

1 Einführung

1.1 NTT Ltd. ist ein weltweit führendes Unternehmen für Technologiedienstleistungen. NTT Germany AG & Co. KG („**NTT**“) ist eine Tochtergesellschaft der NTT Ltd. und erbringt IKT-Dienstleistungen („**Dienstleistungen**“) für den Kunden gemäß [Name des betreffenden Vertrags ODER des bestehenden Servicevertrages einfügen] Vertrag („**Kundenvertrag**“).

1.2 Soweit NTT im Rahmen des Kundenvertrags verpflichtet ist, personenbezogene Daten im Namen des Kunden zu verarbeiten, wird NTT dies in Übereinstimmung mit den in diesem Auftragsverarbeitungsvertrag („**AVV**“) festgelegten Bedingungen tun.

2 Definierte Begriffe

2.1 Der Begriff „**Durchführungsbeschluss 2021**“ bezeichnet den DURCHFÜHRUNGSBESCHLUSS (EU) 2021/914 DER KOMMISSION.

2.2 **„EU-Standardvertragsklauseln“** sind die Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten aus der Europäischen Union in Drittländer, wie sie im Anhang des Durchführungsbeschlusses 2021 aufgeführt sind, das zweite Modul, wie es in Teil 1, **Anlage F** und das vierte Modul, wie es in Teil 2, **Anlage F** ausgeführt sind.

2.3 **„DS-GVO**“ bezeichnet die Datenschutz-Grundverordnung (VO (EU) 2016/679).

2.4 **„Eingeschränkte Übermittlung“** bedeutet eine Übermittlung von personenbezogenen Daten aus einem Mitgliedstaat des Europäischen Wirtschaftsraums („**EWR**“), dem Vereinigten Königreich oder der Schweiz in ein Land außerhalb der Europäischen Union, des EWR, des Vereinigten Königreichs oder der Schweiz.

2.5 **„Standardvertragsklauseln**“ oder „**SCC**“ sind die SCC der EU und die SCC des Vereinigten Königreichs, die von Zeit zu Zeit gemäß den geltenden Datenschutzgesetzen aktualisiert, ergänzt oder ersetzt werden können, als anerkannter Übermittlungs- oder Verarbeitungsmechanismus (je nach Fall).

2.6 **„UK GDPR**“ bezeichnet die United Kingdom General Data Protection Regulation in der im Vereinigten Königreich geltenden Fassung.

2.7 **„UK GDPR-Bedingungen**“ sind die Bedingungen, die gemäß UK GDPR anderweitig erforderlich sind und die nicht in den SCC enthalten sind, wie in **Anlage E** dargelegt.

2.8 **„Britische SCC**“ sind die in Artikel 46 Absatz 2 Buchstabe c der Datenschutz-Grundverordnung beschriebenen und durch den Beschluss 2010/87/EU der EU-Kommission vom 5. Februar 2010 genehmigten SCC.

2.9 **Sonstige Begriffe**. Begriffe, die in diesem AVV verwendet, aber nicht definiert werden, wie z. B. „**Verantwortlicher**“, „**betroffene Person“**, „**personenbezogene Daten**“, „**Auftragsverarbeiter**“ und „**Verarbeitung**“, haben dieselbe Bedeutung wie in Artikel 4 der DS-GVO, unabhängig davon, ob die DS-GVO Anwendung findet.

3 Anwendbares Recht

3.1 NTT kann verpflichtet sein, personenbezogene Daten im Namen des Kunden gemäß (a) allen anwendbaren Gesetzen, einschließlich (b) untergeordneten Gesetzen und Verordnungen zur Umsetzung der DS-GVO und (c) der UK GDPR (zusammenfassend als „**anwendbare Datenschutzgesetze**“ bezeichnet) zu verarbeiten.

3.2 Sofern nicht ausdrücklich anders angegeben, gilt im Falle eines Widerspruchs zwischen (a) dem Hauptteil dieses AVV und entweder: (b) den SCC oder (c) den UK GDPR-Bedingungen (soweit die UK GDPR in Bezug auf diese Bedingungen gilt), hat das anwendbare lokale Recht in (b) Vorrang.

3.3 Soweit NTT eine Auftragsverarbeiterin von personenbezogenen Daten ist, die der DS-GVO oder der UK GDPR unterliegen, sind die in Artikel 28 Absatz 3 der DS-GVO (bzw. der UK GDPR) geforderten zwingenden vertraglichen Regelungen zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern, die die Verarbeitung personenbezogener Daten regeln, in den Ziff. 5.1, 6.1, 6.3, 6.4, 7, 8.1, 8.2, 9.1, 9.2, 10 bis 14 enthalten. Die UK GDPR-Bedingungen regeln die Verarbeitung in Bezug auf alle Bedingungen, die von der UK GDPR gefordert werden und die nicht an anderer Stelle in dieses AVV abgedeckt sind.

4 Dauer und Beendigung

4.1 Dieser AVV tritt an dem Tag in Kraft, an dem sie von der zuletzt unterzeichnenden Partei unterzeichnet wird, und bleibt so lange in Kraft, wie der Kundenvertrag in Kraft bleibt oder NTT personenbezogene Daten im Zusammenhang mit dem Kundenvertrag in seinem Besitz oder unter seiner Kontrolle hat.

4.2 NTT verarbeitet personenbezogene Daten bis zum Ablauf oder zur Beendigung des Kundenvertrags, es sei denn, der Kunde hat schriftlich eine andere Weisung erteilt, oder bis diese personenbezogenen Daten auf

schriftliche Anweisung des Kunden zurückgegeben oder vernichtet werden, oder bis zu dem Umfang, in dem NTT verpflichtet ist, diese personenbezogenen Daten aufzubewahren, um die geltenden Gesetze einzuhalten.

5 Arten von personenbezogenen Daten und Verarbeitungszwecke

5.1 Wenn das anwendbare Datenschutzgesetz die DS-GVO oder die UK GDPR ist:

(a) Der Kunde und NTT bestätigen, dass der Kunde der Verantwortliche und NTT die Auftragsverarbeiterin oder die Unterauftragsverarbeiterin ist.

(b) Die Einzelheiten der Verarbeitungen, insbesondere die Kategorien personenbezogener Daten und die Zwecke der Verarbeitung, für die die personenbezogenen Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet werden, sind in **Anlage B** aufgeführt.

5.2 Der Kunde behält die Kontrolle über die personenbezogenen Daten und bleibt für die Einhaltung seiner Verpflichtungen gemäß den geltenden Datenschutzgesetzen verantwortlich, einschließlich der Bereitstellung aller erforderlichen Mitteilungen, der Einholung aller erforderlichen Zustimmungen und der Verarbeitungsweisungen, die er NTT erteilt.

5.3 **Anlage B** beschreibt den Zweck der Verarbeitung und die Kategorien von betroffenen Personen und personenbezogene Daten, die NTT im Zusammenhang mit den in der Kundenvereinbarung beschriebenen Dienstleistungen verarbeiten darf ("**Geschäftszwecke**").

6 Pflichten der NTT

6.1 **Weisungen des Kunden**. Wenn NTT als Auftragsverarbeiterin hinsichtlich personenbezogener Daten auftritt, wird sie die vom Kunden zur Verarbeitung freigegebenen Kategorien personenbezogener Daten nur auf dokumentierte Weisung des Kunden verarbeiten, wie in **Anlage B** angegeben, und zwar nur in dem Umfang, der zur Erfüllung der Geschäftszwecke erforderlich ist. NTT wird die personenbezogenen Daten nicht für andere Zwecke oder in einer Weise verarbeiten, die nicht im Einklang mit diesem AVV oder den geltenden Datenschutzgesetzen steht. Sollte NTT vernünftigerweise davon ausgehen, dass eine bestimmte Verarbeitungstätigkeit, die über den Umfang der Weisungen des Kunden hinausgeht, erforderlich ist, um einer gesetzlichen Verpflichtung nachzukommen, der NTT unterliegt, muss NTT den Kunden über diese gesetzliche Verpflichtung informieren und die ausdrückliche Einwilligung des Kunden einholen, bevor eine solche Verarbeitung vorgenommen wird. NTT wird die personenbezogenen Daten nicht in einer Weise verarbeiten, die mit den dokumentierten Weisungen des Kunden unvereinbar ist.

6.2 **Unabhängige Verantwortliche**. Soweit NTT personenbezogene Daten in Verbindung mit dem ordnungsgemäßen Geschäftsbetrieb von NTT verwendet oder anderweitig verarbeitet, ist NTT eine unabhängige für die Verarbeitung Verantwortliche und für die Einhaltung aller geltenden Gesetze und Verpflichtungen als für die Verarbeitung Verantwortliche zuständig.

6.3 **Einhaltung**. NTT wird den Kunden in angemessener Weise bei der Einhaltung seiner Verpflichtungen gemäß den anwendbaren Datenschutzgesetzen unterstützen, insbesondere hinsichtlich der Rechte der betroffenen Personen, der Datenschutz-Folgenabschätzungen und Meldungen oder Abstimmungen mit Datenschutzbehörden, wobei die Art der Verarbeitung durch die NTT und die der NTT zur Verfügung gestellten Informationen berücksichtigt werden. NTT wird den Kunden unverzüglich benachrichtigen, wenn ihrer Meinung nach eine Weisung gegen geltende Datenschutzgesetze verstößt. Diese Benachrichtigung stellt keine rechtliche Verpflichtung der NTT dar, die auf den Kunden anwendbaren Gesetze zu überwachen oder auszulegen. Diese Benachrichtigung ist keine Rechtsberatung gegenüber dem Kunden.

6.4 **Offenlegung**. NTT wird personenbezogene Daten nicht weitergeben, außer: (a) auf schriftliche Weisung des Kunden, (b) wie in diesem AVV beschrieben oder (c) wie gesetzlich vorgeschrieben. Wenn NTT gesetzlich dazu befugt ist, wird NTT bei Erhalt einer Anfrage von einer Behörde angemessene Anstrengungen unternehmen, um den Kunden zu benachrichtigen und versuchen, die Behörde dazu zu veranlassen, die personenbezogenen Daten direkt vom Kunden anzufordern.

7 Auftragsvergabe an Unterauftragsverarbeiter

7.1 **Liste der Unterauftragsverarbeiter**. Eine Liste der Unterauftragsverarbeiter der NTT, die die NTT unmittelbar für die jeweiligen Dienstleistungen als Auftragsverarbeiter einsetzt, wird dem Kunden auf Anfrage an den in **Anlage A** genannten Kontak zur Verfügung gestellt, gemäß **Anlage B** definiert oder anderweitig auf einer NTT-Website aufgeführt.

7.2 **Allgemeine Genehmigung.** Der Kunde erteilt seine allgemeine Genehmigung für die Beauftragung von Unterauftragsverarbeitern durch die NTT, einschließlich gegenwärtiger und zukünftiger Tochterunternehmen der NTT Ltd., um Dienstleistungen ganz oder teilweise zu erbringen und um personenbezogene Daten in seinem Auftrag zu verarbeiten. Soweit dies nach den geltenden Datenschutzgesetzen zulässig ist, stellt dieser AVV die

allgemeine schriftliche Genehmigung des Kunden für die Untervergabe der Verarbeitung von personenbezogenen Daten durch NTT an die vereinbarte Liste von Unterauftragsverarbeitern dar.

7.3 **Änderungen.** NTT wird den Kunden mindestens 14 Tage im Voraus schriftlich über beabsichtigte Änderungen der vereinbarten Liste der Unterauftragsverarbeiter informieren und dem Auftraggeber die Möglichkeit geben, gegen diese Änderungen Einspruch zu erheben. Ein solcher Einspruch muss innerhalb von zehn Tagen nach der Benachrichtigung schriftlich an die in **Anlage A** genannte Kontaktperson von NTT gerichtet werden.

7.4 **Erfüllung der Anforderungen**. NTT ist dafür verantwortlich, dass ihre Unterauftragsverarbeiter die Verpflichtungen der NTT aus diesem AVV einhalten.

8 Verpflichtungen der Kunden

8.1 **Ersuchen einer betroffenen Person**. Erhält NTT eine Anfrage einer betroffenen Person des Kunden zur Ausübung eines oder mehrerer ihrer Rechte gemäß den geltenden Datenschutzgesetzen in Verbindung mit einer Dienstleistung, für die NTT eine Auftragsverarbeiterin oder eine Unterauftragsverarbeiterin ist, verweist NTT die betroffene Person weiter an den Kunden, damit sie ihre Anfrage direkt an den Kunden richtet. Der Kunde ist für die Beantwortung einer solchen Anfrage verantwortlich. NTT unterstützt den Kunden auf Anfrage angemessen bei der Beantwortung solcher Ersuchen. Der Kunde wird der NTT die Kosten, die für diese Unterstützungshandlung entstehen, angemessen entschädigen.

8.2 **Kundenanfragen**. NTT muss unverzüglich jedem Ersuchen des Kunden oder jeder Anweisung von autorisierten Personen nachkommen, die (a) NTT auffordern, die personenbezogenen Daten zu berichtigen, zu übertragen, zu löschen oder anderweitig zu verarbeiten oder eine unberechtigte Verarbeitung zu beenden, einzuschränken oder anderweitig abzuhelfen, (b) die Verpflichtungen des Kunden hinsichtlich der Sicherheit der Verarbeitung betreffen und (c) die Verpflichtungen des Kunden zur vorherigen Konsultation im Sinne der geltenden Datenschutzgesetze unter Berücksichtigung der Art der Verarbeitung und der NTT zur Verfügung stehenden Informationen zum Gegenstand haben.

8.3 **Garantie**. Der Kunde garantiert, dass: (a) er über alle erforderlichen Rechte verfügt, um NTT die personenbezogenen Daten für die im Zusammenhang mit den Dienstleistungen durchzuführende Verarbeitung zur Verfügung zu stellen; und (b) er hinsichtlich der vorgesehenen Verwendung der personenbezogenen Daten durch die NTT für die Geschäftszwecke und hinsichtlich der einzelnen Weisungen alle geltenden Datenschutzgesetze einhält.

8.4 **Datenschutzhinweise**. Soweit dies nach den geltenden Datenschutzgesetzen erforderlich ist, ist der Kunde dafür verantwortlich, dass den betroffenen Personen alle erforderlichen Datenschutzhinweise zur Verfügung gestellt werden und dass, sofern die Rechtmäßigkeit der Verarbeitung nicht durch eine andere in den geltenden Datenschutzgesetzen festgelegte Rechtsgrundlage gestützt wird, alle erforderlichen Einwilligungen der betroffenen Personen in die Verarbeitung eingeholt werden und ein Protokoll über diese Einwilligungen geführt wird. Sollte eine solche Einwilligung von einer betroffenen Person widerrufen werden, so ist der Kunde dafür verantwortlich, NTT die Tatsache dieses Widerrufs mitzuteilen, und NTT bleibt für die Umsetzung der Anweisungen des Kunden in Bezug auf die Verarbeitung dieser personenbezogenen Daten verantwortlich.

9 Sicherheit

9.1 **TOM**. NTT wird geeignete technische und organisatorische Maßnahmen („**TOM**“) ergreifen, um die Sicherheit der personenbezogenen Daten im Sinne der geltenden Datenschutzgesetze zu gewährleisten, einschließlich der in **Anlage C** aufgeführten Sicherheitsmaßnahmen. Dies beinhaltet den Schutz der personenbezogenen Daten vor einer Sicherheitsverletzung, die zu einer versehentlichen oder unrechtmäßigen Zerstörung, einem Verlust, einer Änderung, einer unbefugten Offenlegung oder einem unberechtigten Zugriff auf die personenbezogenen Daten führt.

9.2 **Zugang zu personenbezogenen Daten.** NTT gewährt ihren Mitarbeitern nur in dem Umfang Zugang zu den personenbezogenen Daten, der für die Durchführung, Verwaltung und Überwachung des Kundenvertrags unbedingt erforderlich ist. NTT stellt sicher, dass die Personen, die zur Verarbeitung der erhaltenen personenbezogene Daten befugt sind, sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verpflichtung zur Vertraulichkeit unterliegen.

9.3 **Kostenverhandlungen**. Die Parteien werden redlich über die Kosten verhandeln, die gegebenenfalls für die Umsetzung wesentlicher Änderungen anfallen, soweit diese nicht durch spezifische aktualisierte Sicherheitsanforderungen in den geltenden Datenschutzgesetzen oder durch die zuständigen Datenschutzbehörden vorgeschrieben sind (in diesem Fall trägt NTT die Kosten in dem durch die geltenden Datenschutzgesetze oder durch die Datenschutzbehörde vorgeschriebenen Umfang).

10 Prüfungen

10.1 **Zertifizierungen**. NTT wird alle Zertifizierungen aufrechterhalten, zu deren Aufrechterhaltung und Einhaltung sie vertraglich verpflichtet ist, wie in der Kundenvereinbarung ausdrücklich vereinbart. NTT wird diese Zertifizierungen in angemessenem Umfang erneut zertifizieren.

10.2 **Bereitstellung von Nachweisen**. Auf schriftliches Verlangen des Kunden stellt NTT dem Kunden Nachweise über die Zertifizierungen in Bezug auf die Verarbeitung der personenbezogenen Daten zur Verfügung, einschließlich anwendbarer Zertifizierungen oder Auditberichte über die EDV-Umgebung und die physischen Datenzentren, die NTT bei der Verarbeitung von personenbezogenen Daten zur Erbringung der Dienste verwendet, so dass der Kunde in angemessener Weise die Einhaltung der Verpflichtungen der NTT gemäß diesem AVV überprüfen kann.

10.3 **Einhaltung der TOM**. NTT kann sich auch auf diese Zertifizierungen stützen, um die Einhaltung der in Ziff. 9.1 genannten Anforderungen nachzuweisen.

10.4 **Vertrauliche Informationen**. Alle von NTT zur Verfügung gestellten Nachweise sind vertrauliche Informationen und unterliegen den Geheimhaltungs- und Verbreitungsbeschränkungen der NTT oder des NTT-Unterverarbeiters.

10.5 **Kundenaudits**. Der Kunde kann Audits hinsichtlich der Räumlichkeiten und Abläufe der NTT durchführen, wenn diese sich auf die personenbezogenen Daten beziehen und:

(a) NTT keine ausreichenden Nachweise für die gemäß Ziff. 9 ergriffenen Maßnahmen vorgelegt hat; oder

(b) ein Audit von einer zuständigen Datenschutzbehörde förmlich verlangt wird; oder

(c) die anwendbaren Datenschutzgesetze dem Kunden ein direktes Auditrecht einräumen (und solange der Kunde nur einmal innerhalb eines Zwölfmonatszeitraums ein Audit durchführt, es sei denn, zwingende anwendbare Datenschutzgesetze verlangen häufigere Audits).

NTT Ltd. und ihre Tochtergesellschaften sind beabsichtigte Drittbegünstigte dieses Abschnitts.

10.6 **Ablauf des Kundenaudits**. Das Kundenaudit kann von einem Dritten durchgeführt werden (der jedoch kein Konkurrent von NTT sein darf und ausreichend qualifiziert und unabhängig sein muss), der zuvor eine Vertraulichkeitsvereinbarung mit NTT abschließen muss. Der Kunde muss jedes Audit mindestens 60 Tage im Voraus ankündigen, es sei denn, zwingend anwendbare Datenschutzgesetze oder eine zuständige Datenschutzbehörde verlangen eine kürzere Ankündigungsfrist. NTT wird bei solchen Audits kooperieren und den Auditoren des Kunden angemessenen Zugang zu allen Räumlichkeiten und Geräten gewähren, die mit der Verarbeitung der personenbezogenen Daten zu tun haben. Die Audits des Kunden sind zeitlich auf maximal drei Geschäftstage begrenzt. Über diese Beschränkungen hinaus werden die Parteien aktuelle Zertifizierungen oder andere Auditberichte verwenden, um wiederholte Audits zu vermeiden oder zu minimieren. Der Kunde hat die Kosten eines Kundenaudits zu tragen, es sei denn, die Prüfung ergibt einen wesentlichen Verstoß von NTT gegen diesen AVV; in diesem Fall trägt NTT die Kosten der Prüfung. Wird bei der Prüfung festgestellt, dass NTT gegen seine Verpflichtungen aus dem AVV verstoßen hat, wird NTT den Verstoß unverzüglich und auf eigene Kosten beheben.

11 Management von Zwischenfällen

11.1 **Sicherheitsvorfälle**. Erhält NTT Kenntnis von einer Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum Zugriff auf personenbezogene Daten führt, während diese von NTT verarbeitet werden (jeweils ein „**Sicherheitsvorfall“**), wird NTT unverzüglich und ohne unangemessene Verzögerung:

(a) den Kunden über den Sicherheitsvorfall informieren;

(b) den Sicherheitsvorfall untersuchen und den Kunden mit ausreichenden Informationen über den Sicherheitsvorfall versorgen, einschließlich der Information, ob der Sicherheitsvorfall personenbezogene Daten betrifft;

(c) angemessene Maßnahmen ergreifen, um die Auswirkungen des Sicherheitsvorfalls zu mildern und den Schaden zu minimieren.

11.2 **Meldung von Sicherheitsvorfällen**. Die Meldung von Sicherheitsvorfällen erfolgt in Übereinstimmung mit Ziff. 11.4. Wenn der Sicherheitsvorfall personenbezogene Daten betrifft, wird NTT angemessene Anstrengungen unternehmen, um den Kunden in die Lage zu versetzen, eine gründliche Untersuchung des Sicherheitsvorfalls durchzuführen, eine korrekte Reaktion zu formulieren und geeignete weitere Schritte in Bezug auf den Sicherheitsvorfall zu unternehmen. NTT wird sich in angemessener Weise bemühen, den Kunden bei der Erfüllung seiner Verpflichtung nach den geltenden Datenschutzgesetzen zu unterstützen, die zuständige Datenschutzbehörde und die betroffenen Personen über einen solchen Sicherheitsvorfall zu informieren. Die Benachrichtigung von NTT über einen Sicherheitsvorfall oder die Reaktion auf einen Sicherheitsvorfall gemäß

dieser Klausel ist kein Anerkenntnis eines Fehlers oder einer Haftung von NTT in Bezug auf den Sicherheitsvorfall.

11.3 **Andere Vorfälle**. NTT wird den Kunden unverzüglich benachrichtigen, wenn NTT davon Kenntnis erhält, dass

(a) eine Beschwerde oder ein Ersuchen in Bezug auf die Ausübung der Rechte einer betroffenen Person gemäß den geltenden Datenschutzgesetzen in Bezug auf personenbezogene Daten, die NTT im Namen des Kunden und seiner betroffenen Personen verarbeitet eingeht; oder

(b) eine Untersuchung oder Beschlagnahme der personenbezogenen Daten durch Regierungsbeamte erfolgt ist oder ein konkreter Hinweis vorliegt, dass eine solche Untersuchung oder Beschlagnahme unmittelbar bevorsteht; oder

(c) nach Ansicht von NTT die Umsetzung einer vom Kunden erhaltenen Weisung in Bezug auf die Verarbeitung der personenbezogenen Daten gegen geltende Gesetze verstoßen würde, denen der Kunde oder NTT unterliegt.

11.4 **Benachrichtigungen an den Kunden.** Alle Mitteilungen, die dem Kunden gemäß dieser Ziff. 11 gemacht werden, sind an die in **Anlage A** genannte Kontaktperson des Kunden zu richten, wobei eine der in **Anlage A** genannten Kontaktmethoden zu verwenden ist.

12 Allgemeine grenzüberschreitende Übermittlung von personenbezogenen Daten

12.1 Vorbehaltlich der sonstigen Bestimmungen dieser Ziffer 12 und Ziffer 13 können personenbezogene Daten, die NTT im Auftrag des Kunden verarbeitet, in jedes Land, in dem NTT oder seine Unterauftragsverarbeiter tätig sind, übermittelt und dort gespeichert und verarbeitet werden.

12.2 **Übermittlungsbeschränkungen**. Wenn ein anwendbares Datenschutzgesetz die grenzüberschreitende Übermittlung von personenbezogenen Daten einschränkt, wird der Kunde diese personenbezogenen Daten nur dann an NTT übermitteln, wenn NTT entweder durch seinen Standort oder durch die Teilnahme an einem gültigen grenzüberschreitenden Übermittlungsmechanismus gemäß den anwendbaren Datenschutzgesetzen diese personenbezogenen Daten rechtmäßig empfangen kann.

12.3 **Änderung des gesetzlichen Übermittlungsmechanismus**. Für den Fall, dass NTT sich auf die SCC oder andere spezifische gesetzliche Mechanismen zur Vereinfachung internationaler Datenübermittlungen stützt und diese Mechanismen später geändert, widerrufen oder von einem zuständigen Gericht für ungültig erklärt werden, verpflichten sich der Kunde und NTT, nach Kräften zusammenzuarbeiten, um die Übermittlung unverzüglich auszusetzen oder einen geeigneten alternativen Mechanismus zu verfolgen, der die Übermittlung rechtmäßig unterstützen kann.

13 Grenzüberschreitende Übermittlung von personenbezogenen Daten gem. der DS-GVO und der UK GDPR

13.1 Wenn die DS-GVO oder UK GDPR das anwendbare Datenschutzgesetz ist, darf NTT die Verarbeitung von personenbezogenen Daten bei der Erbringung der Dienstleistungen im Zusammenhang mit einer eingeschränkten Übermittlung nur unter den folgenden Bedingungen verarbeiten oder ermöglichen:

(a) **Angemessenheitsbeschluss**. Wenn die Europäische Kommission oder das Vereinigte Königreich (je nach Fall) festgestellt hat, dass das betreffende Land einen angemessenen Schutz für die Rechte der betroffenen Personen bietet;

(b) **Geeignete Garantie**. In Ermangelung eines Angemessenheitsbeschlusses, wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, der in einem Drittland ansässig ist, das kein angemessenes Datenschutzniveau gewährleistet, und der die personenbezogenen Daten im Rahmen eines gültigen Übermittlungsverfahrens gemäß Art. 46 Abs. 2 DS-GVO, der UK GDPR oder eines anderen anwendbaren Datenschutzgesetzes erhält, angemessene Garantien geboten hat.

13.1.2 **Standardvertragsklauseln**. SCC können wie folgt verwendet werden:

(i) Die britischen SCC für personenbezogene Daten, die der UK GDPR oder deren Nachfolgeverordnungen unterliegen, einschließlich der Fälle, in denen das Vereinigte Königreich ein Addendum zu den EU-Standardvertragsklauseln annimmt;

(ii) Das/die anwendbare(n) Modul(e) der EU-Standardvertragsklauseln für personenbezogene Daten, die der DS-GVO unterliegen, oder das Schweizer Bundesgesetz vom 19. Juni 1992 über den Datenschutz (**DSG**).

13.2 **Ausfertigung von SCC**. Wenn eine grenzüberschreitende Übermittlung personenbezogener Daten zwischen NTT und dem Kunden die Unterzeichnung von SCC oder die Unterzeichnung von Nachfolgeregelungen oder Ergänzungen zu den in Ziffer 13.1.2 erwähnten SCC erforderlich macht, um das geltende Datenschutzrecht einzuhalten, werden die Parteien alle relevanten Details in den anwendbaren SCC oder Ergänzungen ausfüllen und diese unterzeichnen sowie alle anderen Maßnahmen ergreifen, die zur Legitimierung der Übermittlung erforderlich sind.

13.3 **Unterauftragsverarbeiter**. Der Kunde ermächtigt NTT, die anwendbare Form der anwendbaren SCC mit Unterauftragsverarbeitern im Namen des Kunden und in seinem Auftrag abzuschließen (in diesem Fall muss der Kunde selbst keine direkten Vereinbarungen mehr mit solchen Unterauftragsverarbeitern treffen). NTT wird dem Kunden auf Anfrage die ausgefertigten SCC zur Verfügung stellen.

14 Rückgabe oder Vernichtung von personenbezogenen Daten

14.1 **Löschung durch den Kunden.** Bei bestimmten Diensten ist der Kunde für die Installation, das Hosting, die Verarbeitung und die Nutzung der personenbezogenen Daten verantwortlich. Hier hat nur der Kunde die Möglichkeit, auf die in diesem Dienst gespeicherten personenbezogene Daten zuzugreifen, sie zu extrahieren und zu löschen. Wenn der betreffende Dienst den Zugriff, die Speicherung oder die Extraktion der vom Kunden bereitgestellten Software nicht unterstützt, übernimmt NTT keine Haftung für die Löschung der personenbezogenen Daten, wie in dieser Ziff. 14.1 beschrieben.

14.2 **Löschen oder Rückgabe**. Wenn der Kundenvertrag vorschreibt, dass NTT personenbezogene Daten aufbewahren muss, wird NTT diese personenbezogenen Daten innerhalb des im Kundenvertrag vereinbarten Zeitraums löschen, es sei denn, NTT ist nach geltendem Recht berechtigt oder verpflichtet, diese personenbezogenen Daten aufzubewahren. Wenn die Aufbewahrung von personenbezogenen Daten nicht in der Kundenvereinbarung geregelt ist, wird NTT alle personenbezogene Daten entweder löschen, vernichten oder an den Kunden zurückgeben und alle vorhandenen Kopien vernichten oder zurückgeben, wenn

(a) NTT die Erbringung der Dienstleistungen beendet hat, die im Zusammenhang mit der Verarbeitung stehen;

(b) dieser AVV endet;

(c) der Kunde NTT schriftlich dazu auffordert; oder

(d) NTT auf andere Weise alle im Rahmen der Dienstleistungen vereinbarten Zwecke im Zusammenhang mit den Verarbeitungstätigkeiten erfüllt hat, sofern der Kunde keine weitere Verarbeitung durch NTT verlangt.

14.3 **Bescheinigung über die Vernichtung**. NTT stellt dem Kunden auf dessen Wunsch ein Bescheinigung über die Vernichtung zur Verfügung. Wenn die Löschung oder Rückgabe der personenbezogenen Daten aus irgendeinem Grund nicht möglich ist oder wenn Sicherungskopien oder archivierte Kopien der personenbezogenen Daten erstellt wurden, bewahrt NTT diese personenbezogenen Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen auf.

14.4 **Dritte**. Bei Beendigung dieses AVV wird NTT alle Unterauftragsverarbeiter, die ihre eigene Verarbeitung unterstützen, benachrichtigen und sicherstellen, dass diese die personenbezogenen Daten entweder vernichten oder die personenbezogenen Daten an den Kunden zurückgeben, je nach Ermessen des Kunden.

15 Haftung und Gewährleistung

Jegliche Haftungsbeschränkung in der Kundenvereinbarung **gilt** für diesen AVV, es sei denn, eine solche Beschränkung (a) schränkt die Haftung der Parteien gegenüber den betroffenen Personen ein oder (b) ist nach geltendem Recht nicht zulässig.

16 Hinweis

16.1 Jede Mitteilung oder sonstige Mitteilung an eine Partei im Rahmen oder im Zusammenhang mit diesem AVV muss in schriftlicher Form erfolgen und der anderen Partei per E-Mail zugestellt werden.

16.2 Ziff. 16.1 gilt nicht für die Zustellung von Verfahren oder anderen Dokumenten im Rahmen eines Gerichtsverfahrens oder gegebenenfalls eines Schiedsverfahrens oder einer anderen Methode der Streitbeilegung.

16.3 Jede Benachrichtigung oder sonstige Mitteilung gilt als erfolgt, wenn

(a) sie persönlich zugestellt wurde;

(b) sie per Post (frankiert, per Einschreiben oder Einschreiben mit Rückschein) zugegangen ist; oder

(c) durch einen international anerkannten Kurierdienst (Nachweis der Zustellung durch den Anzeigenden) an die physische Adresse (wie oben angegeben) und eine elektronische Kopie an die elektronische Adresse (wie oben in der Tabelle angegeben) zugestellt wurde.

17 Sonstiges

17.1 **Widersprüche zwischen den Bedingungen**. Die Bedingungen des Kundenvertrags bleiben in vollem Umfang in Kraft und wirksam, sofern sie nicht in diesem AVV geändert werden. Soweit NTT im Rahmen der Erfüllung des Kundenvertrags personenbezogene Daten, die den geltenden Datenschutzgesetzen unterliegen, im Namen des Kunden verarbeitet, gelten die Bestimmungen dieses AVV. Sollten die Bestimmungen dieses AVV im

Widerspruch zu den Bestimmungen des Kundenvertrags stehen, haben die Bestimmungen dieses AVV Vorrang vor den Bestimmungen des Kundenvertrags.

17.2 **Geltendes Recht**. Dieser AVV unterliegt den Gesetzen des Landes, das in den entsprechenden Bestimmungen der Kundenvereinbarung angegeben ist.

17.3 **Beilegung von Streitigkeiten**. Alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem AVV ergeben, werden ausschließlich vor dem zuständigen Gericht des in den einschlägigen Bestimmungen der Kundenvereinbarung angegebenen Gerichtsstands verhandelt.

17.4 **Gegenstücke**: Dieser AVV und alle SCC können in einer beliebigen Anzahl von Ausfertigungen ausgefertigt werden, von denen jede ein Original darstellt, die aber zusammen eine Vereinbarung bilden. Entscheiden sich eine oder beide Parteien für die elektronische Unterzeichnung dieses AVV und der SCC, so hat jede elektronische Unterschrift dieselbe Gültigkeit und Rechtswirkung wie eine handschriftliche Unterschrift und wird in der Absicht geleistet, diesen AVV und SCC zu bestätigen und die Absicht dieser Partei, durch diesen AVV und SCC gebunden zu sein, zu belegen.

Anlage A Ansprechpartner

Kontaktinformationen des [Datenschutzbeauftragten/Compliance-Beauftragten] des Kunden:
Kontaktinformationen: Physische Adresse; Telefon; E-Mail

Kontaktinformationen des Datenschutzbeauftragten von NTT:
Kontaktinformationen: Datenschutzbeauftragter, EU.DE.Datenschutzbeauftragter@global.ntt

Anlage B Einzelheiten der Verarbeitung

1. Kategorien von betroffenen Personen, deren personenbezogene Daten übermittelt werden

Zu den betroffenen Personen gehören die Vertreter des Kunden, Mitarbeiter, Auftragnehmer und Abnehmer. NTT weist darauf, dass NTT je nach Nutzung der Dienste durch den Kunden die personenbezogenen Daten einer der folgenden Arten von betroffenen Personen verarbeiten kann:

- Beschäftigte, externe Mitarbeiter, Zeitarbeiter, Bevollmächtigte und Vertreter des Datenexporteurs;
- Nutzer (z. B. Kunden, Endnutzer) und andere betroffene Personen, die die Dienste des Kunden nutzen;
- Juristische Personen (falls zutreffend).

2. Kategorien der übermittelten personenbezogenen Daten

NTT nimmt zur Kenntnis, dass NTT je nach Nutzung der Dienste durch den Kunden die folgenden Arten von personenbezogenen Daten verarbeiten kann:

- Allgemeine persönliche Daten (z. B. Vorname, Nachname, E-Mail-Adresse);
- Authentifizierungsdaten (z. B. Benutzername und Passwort);
- Kontaktinformationen (z. B. berufliche E-Mail-Adresse und Telefonnummer);
- Eindeutige Identifikationsnummern und Signaturen (z. B. IP-Adressen);
- Standortdaten (z. B. Geostandortnetzdaten);
- Gerätekennung (z. B. IMEI-Nummer und MAC-Adresse);
- Alle anderen personenbezogenen Daten, die in Artikel 4 der Datenschutz-Grundverordnung genannt werden.

3. Übermittlung sensibler Daten (falls zutreffend) und Anwendung von Beschränkungen oder Garantien, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie z. B. strikte Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnung des Zugangs zu den Daten, Beschränkungen für die Weiterübermittlung oder zusätzliche Sicherheitsmaßnahmen.

Biometrische Informationen (z. B. Fingerabdrücke in NTT-Rechenzentren) [Löschen, wenn unzutreffend]

4. Häufigkeit der Übermittlung (z. B. einmalige oder kontinuierlich Datenübermittlung).

personenbezogene Daten können fortlaufend übermittelt werden, um die Dienstleistungen im Rahmen des bestehenden Kundenvertrags zu erbringen.

5. Art der Verarbeitung

Die Art der Verarbeitung personenbezogener Daten besteht darin, dass NTT die Dienstleistungen gemäß dem bestehenden Kundenvertrag erbringt. Dies beinhaltet:

- Erbringung von Dienstleistungen: Bereitstellung von Produkten und Dienstleistungen im Einklang mit dem geltenden Vertrag;
- Lösung von Anfragen: Kommunikation und Koordinierung der Lösung von Support-Anfragen in einer zeitnahen Weise;
- Verbesserungen der Geschäftsprozesse: Verbesserung der Art und Weise, wie die Dienstleistungen für unsere Kunden erbracht werden;
- Berichterstattung über die Vertragsleistung: Berichterstattung über die vertraglich vereinbarten Dienstleistungen und Lösungsaktivitäten;
- Rechnungsstellung und Vertragsmanagement: Verwaltung von Verträgen, Vertragsverlängerungen und der damit verbundenen Rechnungsstellung;
- Sicherheit und Authentifizierung: Identifizierung und Überprüfung der Identität von Personen, bevor sie Zugang zu Systemen und Daten erhalten; Koordinierung von Reaktionen auf potenzielle Informationssicherheitsvorfälle; und
- Verwaltung der Systeme: Gewährleistung der Verfügbarkeit und Sicherheit der Systeme.

6. Zweck(e) der Datenübermittlung und Weiterverarbeitung

Der Zweck der Verarbeitung personenbezogener Daten besteht darin, dass NTT die Dienstleistungen gemäß dem bestehenden Kundenvertrag erbringen kann.

7. Zeitraum, für den die personenbezogenen Daten aufbewahrt werden, oder, falls dies nicht möglich ist, die Kriterien, nach denen dieser Zeitraum festgelegt wird

Siehe Ziff. Anlage A14 des AVV

8. Bei Übermittlungen an (Unter-)Verarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben

In Übereinstimmung mit dem AVV kann NTT Unterauftragsverarbeiter damit beauftragen, einige oder alle Dienstleistungen im Namen der NTT zu erbringen oder gegenwärtige oder zukünftige Tochterunternehmen der NTT Ltd. für die Dauer des Kundenvertrags zu nutzen. Solche Unterauftragsverarbeiter dürfen personenbezogene Daten nur erhalten, um einige oder alle Dienste zu erbringen, mit deren Erbringung der Datenimporteur sie beauftragt hat, und es ist ihnen untersagt, personenbezogene Daten für einen anderen Zweck zu verwenden. Die Liste der gegenwärtig mit NTT Ltd konzernverbundenen Unternehmen ist beigefügt.

Anlage C Technische und organisatorische Maßnahmen

Anlage C beschreibt die technischen und organisatorischen Maßnahmen („**TOM“)**, die NTT ergreift, um sicherzustellen, dass die Verarbeitung und der Schutz von personenbezogenen Daten auf verantwortungsvolle Weise erfolgt, wobei die Arten der von NTT verarbeiteten personenbezogene Daten, die Branchenstandards, die Interessen und Rechte der Mitarbeiter, Kunden und Gemeinschaften von NTT sowie die angemessenen Kosten der Umsetzung gemäß Ziff. Anlage A10 des AVV oder gemäß Annex II der anwendbaren SCC oder der anwendbaren Datenschutzgesetze berücksichtigt werden.

Die TOM der NTT sind abrufbar unter der folgenden URL:

https://services.global.ntt/en-us/legal/data-privacy-and-protection

Anlage D UK Standard Contractual Clauses (processors) – Transfers from the UK

For the purposes of **UK GDPR** for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Please refer to Client details on front page

Tel.: Please refer to Client details on front page; fax: N/A; e-mail: Please refer to Client details on front page

(the data exporter)

And

Name of the data importing organisation: Please refer to NTT details on front page

Address: Please refer to NTT details on front page

Tel.: Please refer to NTT details on front page; fax:N/A ; e-mail: Please refer to NTT details on front page

Other information needed to identify the organisation:

……
(the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'Commissioner'* shall have the same meaning as in the UK GDPR;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

(f) *'technical and organisational* security *measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of Data Protection Act 2018;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;
   (b) to refer the dispute to the UK courts.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by English law.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 of Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by English law.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Clause 13

Counterparts and electronic signatures

1 These Clauses may be executed in any number of counterparts, each of which will constitute an original, but which will together constitute one agreement.

2 Where one or both of the parties choses to execute these Clauses by electronic signature, each electronic signature will have the same validity and legal effect as the use of a signature affixed by hand and is made with the intention of authenticating these Clauses and evidencing the intention of that party (for itself and for the other data exporters on whose behalf that party is executing these Clauses) to be bound by these Clauses.

Appendix 1 to the UK Standard Contractual Clauses

Data exporter: **Client** is the data exporter. The data exporter receives Services under the Client Agreement.

Data importer: The data importer is **NTT** and the sub-processors referred to in Attachment B who are involved in the processing of personal data for the Service.

Subject matter: The subject-matter of the processing is limited to personal data within the scope of the section 'Nature and purpose of data processing' (below) and the UK GDPR.

Duration and object of processing. The duration of processing will be for the duration of the Client Agreement between data exporter and NTT. The objective of the data processing is the performance of the Services.

Nature and Purpose of Data Processing. The nature and purpose of processing personal data is for data importer to provide the Services under the existing Client Agreement.

The data importer operates a global network of data centers and support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities.

Data Exporter's Instructions. For all Services, data importer will only act upon data exporter's instructions as conveyed to it.

personal data Deletion or Return. Upon expiration or termination of the Services, data exporter may extract personal data and data importer will delete personal data, each in accordance with the DPA.

Categories of data subjects: See Attachment B.

Categories of personal data: See Attachment B.

Sub-processors: See Attachment B.

Authorized persons: See Attachment B

Appendix 2 to the UK Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. **Personnel**. Data importer's personnel will not process personal data without authorization.
2. **Data Privacy Contact**. The data privacy officer of the data importer can be reached at the following address:

   NTT

   Attn: Data Protection Officer

   PrivacyOffice@global.ntt

3. **Technical and Organization Measures**. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect personal data, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

The technical and organizational measures, internal controls, and information security routines set forth in Anlage C are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2 on behalf of the data importer:

Data Exporter: Please refer to Client details on front page

Signature:

Name:

Designation:

Address:

Data Importer: Please refer to NTT details on front page

Signature:

Name:

Designation:

Address:

Anlage E UK GDPR-Bedingungen

In dem Maße, in dem der AVV nicht alle Punkte in dieser Anlage E anspricht oder im AVV geringere Datenschutzverpflichtungen gegenüber dem Kunden vorgesehen sind, wenn NTT im Auftrag des Kunden personenbezogenen Daten im Anwendungsbereich der UK GDPR verarbeitet, geht NTT die Verpflichtungen in dieser Anlage gegenüber dem Kunden ein (kurz „**UK GDPR-Bedingungen**“). Diese UK GDPR-Bedingungen schränken die Datenschutzverpflichtungen, die NTT gegenüber dem Kunden in der Kundenvereinbarung eingeht, weder ein noch verringern sie sie.

Für die Zwecke dieser UK GDPR-Bestimmungen vereinbaren der Kunde und NTT, dass der Kunde der für die Verarbeitung Verantwortliche und NTT die Verarbeiterin der personenbezogenen Daten ist, es sei denn, der Kunde handelt als Verarbeiter; in diesem Fall ist NTT eine Unterverarbeiterin. Diese UK GDPR-Bedingungen gelten nicht, wenn NTT die für die Verarbeitung Verantwortliche für personenbezogene Daten ist.

1. Ergänzende vertragliche Maßnahmen

1.1 Soweit die von NTT durchgeführte Verarbeitung von personenbezogenen Daten der UK GDPR unterliegt und NTT eine Übermittlung an ihre Unterauftragsverarbeiter als "Datenimporteur" vornimmt, gelten die Verpflichtungen gem. Ziff. 1.1 bis einschließlich 1.11.

1.2 Jede Partei garantiert, dass sie keinen Grund zu der Annahme hat, dass geltende Gesetze, denen sie unterliegt, einschließlich etwaiger Anforderungen zur Offenlegung von personenbezogenen Daten oder Maßnahmen zur Genehmigung des Zugriffs durch Behörden, sie daran hindern, ihren Verpflichtungen im Rahmen dieses AVV und der britischen SCC nachzukommen. Jede Partei erklärt, dass sie bei der Abgabe dieser Garantie insbesondere die folgenden Elemente gebührend berücksichtigt hat:

(a) Die besonderen Umstände der Verarbeitung, einschließlich des Umfangs und der Regelmäßigkeit der Verarbeitung, die den geltenden Gesetzen unterliegt; die verwendeten Übermittlungskanäle; die Art der betreffenden personenbezogenen Daten; einschlägige praktische Erfahrungen mit früheren Fällen oder das Fehlen von Auskunftsersuchen von Behörden für die Art von personenbezogenen Daten, die von ihr verarbeitet wurden;

(b) die geltenden Gesetze, denen sie unterliegt/unterliegen, einschließlich der Gesetze, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang solcher Behörden gestatten, sowie die geltenden Beschränkungen und Garantien; und

(c) Garantien, die über die in diesem AVV vorgesehenen hinausgehen, einschließlich der technischen und organisatorischen Maßnahmen, die bei der Verarbeitung von personenbezogenen Daten durch NTT und den jeweiligen Unterauftragsverarbeiter angewandt werden.

1.3 Jede Partei sichert zu, dass sie sich bei der Durchführung der Bewertung gemäß Ziff. 1.2 nach besten Kräften bemüht hat, dem Kunden einschlägige Informationen zur Verfügung zu stellen, und erklärt sich bereit, weiterhin mit dem Kunden zusammenzuarbeiten, um die Einhaltung dieses AVV sicherzustellen. NTT verpflichtet sich, diese Bewertung zu dokumentieren und sie dem Kunden auf Anfrage zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass diese Bewertung auch einer Datenschutzbehörde zur Verfügung gestellt werden kann.

1.4 NTT verpflichtet sich, den Kunden unverzüglich zu benachrichtigen, wenn sie nach der Zustimmung zu diesem AVV und während der Laufzeit dieses AVV Grund zu der Annahme hat, dass sie (oder ein relevanter Unterauftragsverarbeiter, an den eine Übermittlung erfolgt) anwendbaren Gesetzen unterliegt oder unterlegen hat, die nicht mit den Anforderungen unter Ziff. 1.2 übereinstimmt, einschließlich einer Änderung der anwendbaren Gesetze, denen sie (oder der relevante Unterauftragsverarbeiter) unterliegt, oder einer Maßnahme (z. B. einer Offenlegungsaufforderung), die auf eine Anwendung solcher anwendbaren Gesetze in der Praxis hinweist, die nicht mit den Anforderungen unter Ziff. 1.2 übereinstimmt. Nach einer solchen Benachrichtigung oder wenn der Kunde anderweitig Grund zu der Annahme hat, dass NTT seinen Verpflichtungen aus diesem AVV (auch in Bezug auf den betreffenden Unterauftragsverarbeiter) nicht mehr nachkommen kann, wird der Kunde (und die betreffenden Tochtergesellschaften, die für die Verarbeitung Verantwortliche sind) unverzüglich geeignete Maßnahmen (wie z. B. technische oder organisatorische Maßnahmen zur Gewährleistung von Sicherheit und Vertraulichkeit) festlegen, die von ihm selbst oder von NTT (oder dem betreffenden Unterauftragsverarbeiter) auf Kosten des Kunden zu ergreifen sind, um die Situation zu bereinigen, gegebenenfalls in Abstimmung mit der zuständigen Datenschutzbehörde.

1.5 NTT verpflichtet sich, den Kunden unverzüglich zu benachrichtigen, wenn sie (oder der jeweilige Unterauftragsverarbeiter, an den eine Übertragung erfolgt):

(a) eine rechtsverbindliche Aufforderung einer Behörde nach geltendem Recht, dem sie (oder der jeweilige Unterauftragsverarbeiter) unterliegt, zur Offenlegung von personenbezogenen Daten erhält; eine solche

Mitteilung enthält Informationen über die angeforderten personenbezogene Daten, die anfragende Behörde, die Rechtsgrundlage für die Anfrage und die erteilte Antwort;

(b) von einem direkten Zugriff öffentlicher Behörden auf personenbezogene Daten in Übereinstimmung mit den geltenden Gesetzen, denen sie (oder der jeweilige Unterauftragsverarbeiter) unterliegt, Kenntnis erlangt; eine solche Mitteilung enthält alle NTT (und dem jeweiligen Unterauftragsverarbeiter) vorliegenden Informationen.

1.6 Sollte es NTT (oder dem jeweiligen Unterauftragsverarbeiter, an den die Übermittlung erfolgt) untersagt sein, den Kunden gemäß Ziff. 1.4 zu benachrichtigen, verpflichtet sich NTT, sich nach besten Kräften zu bemühen, eine Befreiung von diesem Verbot zu erwirken (und dafür zu sorgen, dass der jeweilige Unterauftragsverarbeiter eine solche erwirkt), um so viele Informationen wie möglich und so schnell wie möglich zu übermitteln. NTT verpflichtet sich, ihre Bemühungen (und die des jeweiligen Unterauftragsverarbeiters) zu dokumentieren, um sie auf Anfrage des Auftraggebers nachweisen zu können.

1.7 Soweit dies nach den geltenden Gesetzen, denen NTT (und der betreffende Unterauftragsverarbeiter) unterliegt, zulässig ist, erklärt sich NTT bereit, dem Kunden für die Dauer der Verarbeitung die einschlägigen Informationen über die bei ihr und dem betreffenden Unterauftragsverarbeiter eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere die Anzahl der Ersuchen, die Art der angeforderten Daten, die ersuchende(n) Behörde(n), die Frage, ob Ersuchen angefochten wurden, und das Ergebnis solcher Anfechtungen usw.).

1.8 NTT verpflichtet sich, die in den Ziff. 1.1 bis 1.7 genannten Informationen für die Dauer der Verarbeitung aufzubewahren und sie der zuständigen Datenschutzbehörde auf Anfrage zur Verfügung zu stellen.

1.9 NTT erklärt sich bereit, die Rechtmäßigkeit des Offenlegungsersuchens unter Berücksichtigung der für sie (und den jeweiligen Unterauftragsverarbeiter) geltenden Gesetze zu überprüfen (und dafür zu sorgen, dass der jeweilige Unterauftragsverarbeiter dies tut), insbesondere, ob das Ersuchen im Rahmen der der ersuchenden Behörde eingeräumten Befugnisse bleibt, und alle zur Verfügung stehenden Rechtsmittel auszuschöpfen, um das Ersuchen anzufechten, wenn sie (oder der jeweilige Unterauftragsverarbeiter) nach sorgfältiger Prüfung zu dem Schluss kommt, dass nach den für sie (oder den jeweiligen Unterauftragsverarbeiter) geltenden Gesetzen ein Grund dafür besteht, dies zu tun. Bei der Anfechtung eines Ersuchens wird NTT einstweilige Maßnahmen beantragen (und dafür sorgen, dass der betreffende Unterauftragsverarbeiter dies tut), um die Auswirkungen des Ersuchens auszusetzen, bis das Gericht in der Sache entschieden hat. NTT wird die beantragten personenbezogene Daten erst dann offenlegen (und dafür sorgen, dass der betreffende Unterauftragsverarbeiter dies tut), wenn dies nach den geltenden Verfahrensvorschriften erforderlich ist. Diese Anforderungen gelten unbeschadet der Verpflichtungen von NTT gemäß Ziff. 1.4. NTT erklärt sich bereit, ihre rechtliche Bewertung (und die des jeweiligen Unterauftragsverarbeiters) sowie etwaige Einwände gegen das Offenlegungsersuchen zu dokumentieren und, soweit dies nach den geltenden Gesetzen, denen sie (oder der jeweilige Unterauftragsverarbeiter) unterliegt, zulässig ist, dem Kunden zur Verfügung zu stellen. Auf Anfrage wird sie bzw. er sie auch der zuständigen Datenschutzbehörde zur Verfügung stellen.

1.10 NTT wird sich in angemessener Weise bemühen, bei der Beantwortung eines Auskunftsersuchens auf der Grundlage einer angemessenen Auslegung des Ersuchens das zulässige Mindestmaß an Informationen bereitzustellen (und dafür zu sorgen, dass der betreffende Unterauftragsverarbeiter, an den die Übermittlung erfolgt, diese bereitstellt).

1.11 NTT informiert die betroffenen Personen in einem transparenten und leicht zugänglichen Format auf ihrer Website über eine Kontaktstelle, die für die Bearbeitung von Beschwerden oder Anfragen zuständig ist, und NTT wird alle Beschwerden unverzüglich bearbeiten (und dafür sorgen, dass die Unterauftragsverarbeiter dies tun).

Anlage F EU Standard Contractual Clauses (processors) – Transfers from EEA/EU

EU Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679

(Module 2 – EU Controller to Non-EU Processor transfers)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

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

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to

the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these clauses.

another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[3]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

[3] This requirement may be satisfied by the sub-processor acceding to these clauses under the appropriate Module, in accordance with Clause 7.

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

[4] As regards the impact of such laws and practices on compliance with these clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the governing law as set out in the applicable Client Agreement between the Parties unless otherwise specified.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Member State specified in the Client Agreement between the Parties.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Clause 19

Additional clause relevant to data exporters who are subject to data protection laws in Switzerland

This Clause 19 applies to personal data subject to Switzerland's Federal Act on Data Protection of 19 June 1992 itself and as revised on 25 September 2020 ("FADP"). The term EU Member State in these Clauses includes the EEA States and Switzerland. The data transfer is subject to the provisions of the GDPR. The provisions of the FADP are additionally applicable on a secondary basis. With regard to data transfers of personal data from Switzerland, the Federal Data Protection and Information Commissioner is the competent supervisory authority. Pursuant to the current Federal Act on Data Protection of 19 June 1992 (current as at the date on which these Clauses are entered into) and until the Federal Act on Data Protection of 19 June 1992 as revised on 25 September 2020 enters into force (on or after the date on which these Clauses are entered into), the term personal data with respect to Switzerland includes, in addition, the data of legal entities and not only of natural persons.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Client

Name: See Client details on front page.

Address: See Client details on front page.

Contact person's name, position and contact details: See Client details on front page.

Activities relevant to the data transferred under these Clauses: See details of Client Agreement and Description of Transfer.

Signature and date: See Client details on front page.

Role (controller/processor): Controller.

Data importer(s): NTT and the sub-processors referred to in Attachment B who are involved in the processing of Personal Data for the Service.

Name: See NTT details on front page, as well as the name and details of each of the NTT Group Companies involved in the processing of Personal Data for the Service referred to in Attachment B.
Address: See NTT details on front page, as well as the address of each of the NTT Group Companies involved in the processing of Personal Data for the Service referred to in Attachment B.
Contact person's name, position and contact details: See NTT details on front page.
Activities relevant to the data transferred under these Clauses: See details of Client Agreement and Description of Transfer.
Signature and date: See NTT details on front page.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Attachment B.

Categories of personal data transferred

See Attachment B.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Attachment B.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

See Attachment B.

Nature of the processing

See Attachment B.

Purpose(s) of the data transfer and further processing

See Attachment B.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Attachment B.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Attachment B.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority/ies will be as set out beneath the Client details on the front page of this document.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Attachment C.