Allgemeine Bedingungen für eine Datenverarbeitung im Auftrag

Version 1.0
25. Januar 2024

Inhaltsverzeichnis

1 Präambel

1.1 Diese allgemeinen Bedingungen für eine Datenverarbeitung im Auftrag **(„AVV“)** ist Teil des Vertrags zwischen NTT DATA und dem Kunden („**Kundenvertrag**“), in dessen Rahmen NTT DATA dem Kunden bestimmte Produkte und/oder Dienstleistungen („**Leistungen**“) bereitstellt.

1.2 Soweit NTT DATA unter dem Kundenvertrag personenbezogene Daten im Auftrag des Kunden zu verarbeiten hat, erfolgt dies zu den in diesem AVV dargelegten Bedingungen.

2 Begriffsbestimmungen

2.1 **„Zusätzliche Sicherheitsmaßnahmen“** sind die in Abschnitt 6 von Attachment D dargelegten Bestimmungen.

2.2 **„Verbundenes Unternehmen“** ist eine juristische Person, die entweder den Kunden oder NTT DATA kontrolliert, von diesen kontrolliert wird oder unter gemeinsamer Kontrolle mit diesen steht. Für die Zwecke dieser Definition bedeutet "Kontrolle" den Besitz von mehr als 50 % der stimmberechtigten Wertpapiere eines Unternehmens oder die Befugnis, das Management und die Politik eines Unternehmens zu lenken.

2.3 **„CCPA“** ist der California Consumer Privacy Act von 2018 in seiner jeweils aktuellen Fassung (Cal. Civ. Code §§ 1798.100 bis 1798.199).

2.4 **„China oder VR China“** i.S. dieser AVV bezeichnet die Volksrepublik China, mit Ausnahme der Sonderverwaltungsregion Hongkong, der Sonderverwaltungsregion Macau und Taiwan.

2.5 **„Chinesische Datenschutzgesetze“** sind das Cybersicherheitsgesetz der VR China, das Datensicherheitsgesetz der VR China, das Gesetz zum Schutz persönlicher Informationen der VR China und andere Gesetze, Verordnungen, Verwaltungsvorschriften und verbindliche nationale Normen der VR China.

2.6 **„Kunde“** bezeichnet das Unternehmen, für das NTT DATA Leistungen erbringt, wie im Kundenvertrag angegeben.

2.7 **„Datenexporteur“** bezeichnet eine Partei, die personenbezogene Daten direkt oder durch Weiterleitung in ein Land überträgt, aufgrund dessen zusätzliche Anforderungen an den Schutz personenbezogener Daten, die unter geltendem Datenschutzrecht übertragen werden, erforderlich werden.

2.8 **„Datenimporteur“** bezeichnet eine Partei, die personenbezogene Daten direkt von einem Datenexporteur oder durch Weiterleitung erhält und die sich in einem Land befindet, aufgrund dessen zusätzliche Anforderungen an den Schutz personenbezogener Daten, die unter geltendem Datenschutzrecht übertragen werden, erforderlich werden.

2.9 „**Datenschutzrecht**“ bedeutet alle Gesetze, die sich auf Datenschutz und Datensicherheit beziehen, die für eine Partei in Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen des Kundenvertrags zwingend gelten, einschließlich, nicht jedoch beschränkt auf – jeweils in der aktuellen Fassung – (a) EU-Datenschutzgesetze, (b) die Datenschutzgesetze des Vereinigten Königreichs, (c) den CCPA, (d) das schweizerische Bundesgesetz vom 19. Juni 1992 über den Datenschutz („**DSG**“), (e) chinesische Datenschutzgesetze und (f) aller weltweit geltenden Gesetze, die für NTT DATA oder Kunden (gegebenenfalls und als Empfänger der von NTT DATA erbrachten Leistungen) in Bezug auf den Datenschutz maßgeblich sind.

2.10 **„EU“** ist die Europäische Union.

2.11 **„EU-Datenschutzgesetze“** sind die Datenschutz-Grundverordnung (DSGVO), deren Nachfolgegesetze sowie alle anderen, im Europäischen Wirtschaftsraum geltenden Gesetze zum Schutz personenbezogener Daten.

2.12 **„EU-SCC“** sind die (jeweils maßgeblichen) Abschnitte I, II, III und IV – soweit sie sich auf Modul Zwei (Datenverantwortlicher an Auftragsverarbeiter), Modul Drei (Auftragsverarbeiter an Auftragsverarbeiter) und Modul Vier (Auftragsverarbeiter an Datenverantwortlichen) beziehen – der Standardvertragsklauseln für die Übertragung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, die durch den Beschluss der Europäischen Kommission vom 4. Juni 2021 gebilligt wurde, wie in **Anlage D** dargelegt.

2.13 **„DSGVO“** ist die Datenschutz-Grundverordnung (VO (EU) 2016/679).

2.14 **„NTT DATA“** bezeichnet das Mitglied der NTT Ltd-Gruppe, das dem Kunden die im Kundenvertrag genannten Leistungen erbringt.

2.15 **„NTT Ltd-Gruppe“** bezeichnet NTT Ltd und ihre jeweiligen verbundenen Unternehmen.

2.16 „**Personenbezogene Daten**“ sind alle personenbezogenen Daten, die NTT DATA von oder im Auftrag des Kunden durch die Inanspruchnahme der Leistungen durch den Kunden zur Verfügung gestellt werden.

2.17 **„Datenschutzerklärung“** bezeichnet die jeweils aktuelle Datenschutzerklärung, in der der Umgang von NTT DATA mit personenbezogenen Daten im Rahmen der allgemeinen Geschäftsführung, des Managements und Betriebs erklärt wird, die abrufbar ist unter services.global.ntt (oder einer entsprechenden Nachfolgeseite) und die von NTT DATA gegebenenfalls bei Bedarf aktualisiert wird (gültig ab Veröffentlichung).

2.18 **„Beschränkte Übertragung“** bedeutet eine Übertragung personenbezogener Daten von einem Datenexporteur an einen Datenimporteur.

2.19 **„Standardvertragsklauseln“** oder **„SCC“** sind alle vorab genehmigten Standardvertragsklauseln für die internationale Übertragung personenbezogener Daten gemäß den geltenden Datenschutzgesetzen, einschließlich

der europäischen Standardvertragsklauseln, des Schweizer Nachtrags und des UK-Nachtrags in ihrer jeweils gemäß des geltenden Datenschutzrechts aktualisierten, ergänzten oder ersetzten Form und Fassung als anerkannte Übertragungs- oder Verarbeitungsregelung (je nach Fall).

2.20 **„Standardvertrag“** oder **„China-SCC“** bezeichnet den Standardvertrag für den Export personenbezogener Daten für die Übertragung personenbezogener Daten von einem Datenexporteur in China an einen Datenimporteur außerhalb Chinas, der von der Cyberspace Administration of China **(„CAC“)** herausgegeben wird, oder alternative Standardvertragsklauseln, die von der CAC von Zeit zu Zeit genehmigt werden. Eine englische Übersetzung des Standardvertrags kann.hier abgerufen werden.

2.21 **„Unterauftragsverarbeiter“** bezeichnet jeden von NTT DATA oder einem verbundenen Unternehmen beauftragten Auftragsverarbeiter, der personenbezogene Daten gemäß dem Kundenvertrag verarbeitet. Zu den Unterauftragsverarbeitern können Dritte (externe Auftragsverarbeiter) oder mit NTT DATA verbundene Unternehmen gehören.

2.22 **„Schweizer Nachtrag“** bezeichnet die EU-SCC in der gemäß **Attachment E** geänderten Fassung.

2.23 **„UK“** bedeutet das Vereinigte Königreich von Großbritannien und Nordirland.

2.24 **„UK-Nachtrag“** bezeichnet das Muster für den Nachtrag B.1.0, das vom britischen Information Commissioner's Office herausgegeben und dem Parlament gemäß s119A des Data Protection Act von 2018 am 2. Februar 2022 vorgelegt wurde, wie es gemäß Abschnitt 18 der zwingenden Bestimmungen des Nachtrags überarbeitet wurde. Der UK-Nachtrag ist in **Anlage E** dargelegt.

2.25 **„Datenschutzgesetze des Vereinigten Königreichs“** bezeichnet alle Gesetze in Bezug auf Datenschutz, die Verarbeitung personenbezogener Daten, den Schutz der Vertraulichkeit und/oder elektronische Kommunikation (einschließlich der UK-DSGVO und des Data Protection Act von 2018), die jeweils im Vereinigten Königreich in Kraft sind.

2.26 **„UK-DSGVO“** bezeichnet die DSGVO in der im Vereinigten Königreich geltenden Fassung.

2.27 **Sonstige Begriffe**. Begriffe wie „**Datenverantwortlicher**“, „**betroffene Person**“ bzw. „**Betroffene**“, „**personenbezogene Daten**“, „**Datenschutzverstöße**“, „**Verletzung des Schutzes personenbezogener Daten**“, „**Auftragsverarbeiter**“ und „**(Daten-)Verarbeitung**“, die ohne Begriffsbestimmung in diesem AVV verwendet werden, haben dieselbe Bedeutung wie in Artikel 4 der DSGVO bzw. (wenn sie in den Datenschutzgesetzen nicht ausdrücklich definiert werden) wie die ihnen entsprechenden Begriffe im jeweiligen Datenschutzgesetz.

3 Anwendbares Recht

3.1 NTT DATA muss möglicherweise im Auftrag des Kunden personenbezogene Daten gemäß geltendem Datenschutzrecht verarbeiten.

3.2 Sofern nicht ausdrücklich anders dargelegt, ist im Falle eines Widerspruchs zwischen dem Hauptteil dieses AVV und dem Datenschutzrecht das anwendbare Datenschutzrecht maßgeblich.

3.3 Soweit NTT DATA ein Auftragsverarbeiter personenbezogener Daten ist, die den EU-Datenschutzgesetzen oder dem britischen Datenschutzrecht unterliegen, sind die in Artikel 28 Abs. 3 der DSGVO (bzw. gegebenenfalls der UK-DSGVO) vorgeschriebenen Abschnitte für Verträge zwischen Datenverantwortlichen und Auftragsverarbeitern, welche die Verarbeitung personenbezogener Daten regeln, in den Artikeln 5.1,5.2, 6.1,6.3, 6.4, 6.2, 8.1, 8.2, 9.1, 9.2, 10 bis 13 (einschließlich) aufgeführt.

3.4 Falls NTT DATA personenbezogene Daten im Rahmen des CCPA verarbeitet, gelten die CCPA-Bestimmungen in **Attachment F** für die Verarbeitung personenbezogener Daten. Die Bestimmungen des CCPA schränken die Datenschutzverpflichtungen, die NTT DATA gegenüber dem Kunden laut dem AVV, dem Kundenvertrag oder einer anderen Vereinbarung zwischen dem Kunden und NTT DATA eingegangen ist, weder ein noch begrenzen sie diese.

4 Laufzeit und Beendigung

4.1 Dieser AVV bleibt so lange bestehen, wie auch der Kundenvertrag in Kraft bleibt oder NTT DATA personenbezogene Daten in Zusammenhang mit demselben besitzt oder darüber verfügt.

4.2 Sofern NTT DATA nicht vom Kunden anderslautende schriftliche Anweisungen erhält, verarbeitet NTT DATA personenbezogene Daten bis zum Ablauf oder der Beendigung des Kundenvertrags, bis entsprechende personenbezogenen Daten auf schriftliche Anweisung des Kunden zurückgegeben oder vernichtet werden oder so lange NTT DATA verpflichtet ist, diese personenbezogenen Daten aufzubewahren, um die geltenden Gesetze einzuhalten.

5 Arten von personenbezogenen Daten und Verarbeitungszwecke

5.1 Der Kunde und NTT DATA bestätigen, dass der Kunde der Datenverantwortliche und NTT DATA der Auftragsverarbeiter oder Unterauftragsverarbeiter der personenbezogenen Daten ist.

5.2 Die Einzelheiten der Verarbeitung, insbesondere die Kategorien personenbezogener Daten und die Zwecke der Verarbeitung, für die die personenbezogenen Daten im Auftrag des Datenverantwortlichen in Bezug auf die im Kundenvertrag näher beschriebenen Leistungen verarbeitet werden **(„Geschäftszwecke“)**, sind in **0** dargelegt.

5.3 Der Kunde bleibt für die Erfüllung der eigenen Verpflichtungen gemäß geltendem Datenschutzrecht verantwortlich. Dies beinhaltet die Bereitstellung aller erforderlichen Mitteilungen, die Einholung aller benötigten Zustimmungen und die NTT DATA gegenüber erteilten Anweisungen zur Verarbeitung.

6 Pflichten von NTT DATA

6.1 **Anweisungen des Kunden**. Wenn NTT DATA als Verarbeiter personenbezogener Daten auftritt, verarbeitet NTT DATA die personenbezogenen Daten nur auf belegte Anweisungen des Kunden durch jene Personengruppe, die der Kunde zum Erteilen entsprechender Anweisungen zur Verarbeitung personenbezogener Daten ermächtigt hat, wie in 0 („**ermächtigte Personen**“) dargelegt, und dies nur in dem Umfang, wie es zur Erfüllung der Geschäftszwecke erforderlich ist. NTT DATA verarbeitet die personenbezogenen Daten nicht für andere Zwecke oder in einer Weise, die nicht mit diesem AVV oder geltendem Datenschutzrecht vereinbar ist. Sollte NTT DATA vernünftigerweise annehmen, dass eine bestimmte Verarbeitungstätigkeit, die über den Umfang der Anweisungen des Kunden hinausgeht, erforderlich ist, um einer gesetzlichen Verpflichtung nachzukommen, der NTT DATA unterliegt, hat NTT DATA den Kunden über diese gesetzliche Verpflichtung zu informieren und seine ausdrückliche Genehmigung einzuholen, ehe eine derartige Verarbeitung stattfindet. NTT DATA wird die personenbezogenen Daten nicht in einer Weise verarbeiten, die den belegten Anweisungen des Kunden widerspricht.

6.2 **Unabhängiger Datenverantwortlicher**. In dem Maße, in dem NTT DATA personenbezogene Daten in Verbindung mit eigenen rechtmäßigen Geschäftsabläufen verwendet oder anderweitig verarbeitet, ist NTT DATA ein unabhängiger Datenverantwortlicher in Bezug auf eine solche Verwendung, verarbeitet entsprechende Daten gemäß der eigenen Datenschutzrichtlinie und ist haftbar für die Einhaltung aller geltenden Gesetze und Verpflichtungen von Datenverantwortlichen.

6.3 **Einhaltung von Vorschriften**. NTT DATA wird den Kunden in angemessener Weise bei der Einhaltung seiner Verpflichtungen unter geltendem Datenschutzrecht unterstützen. Dabei werden die Art der Verarbeitung durch NTT DATA und die NTT DATA zur Verfügung gestellten Informationen auch in Bezug auf Betroffenenrechte, Datenschutzfolgenabschätzungen sowie die Berichterstattung an und Rücksprache mit den Datenschutzbehörden gemäß geltendem Datenschutzrecht berücksichtigt. NTT DATA informiert den Kunden unverzüglich, wenn nach Ansicht von NTT DATA eine Anweisung des Kunden gegen geltendes Datenschutzrecht verstößt. Diese Benachrichtigung stellt weder eine allgemeine Verpflichtung von NTT DATA dar, die auf den Kunden anwendbaren Gesetze zu überwachen oder zu deuten, noch ist sie eine für den Kunden erbrachte Rechtsberatung.

6.4 **Weitergabe**. NTT DATA gibt personenbezogene Daten ausschließlich unter folgenden Umständen weiter: (a) auf schriftliche Anweisung des Kunden, (b) wie in diesem AVV dargelegt oder (c) wie gesetzlich vorgeschrieben. Soweit NTT DATA gesetzlich dazu befugt ist, wird NTT DATA bei Erhalt eines behördlichen Ersuchens angemessene Anstrengungen unternehmen, den Kunden zu benachrichtigen und versuchen, die Behörde an ihn weiterzuleiten, damit sie die personenbezogenen Daten vom Kunden direkt und in Übereinstimmung mit dessen Richtlinie für Datenanfragen von Behörden anfordert.

7 Beschäftigung von Unterauftragsverarbeitern

7.1 **Einsatz von Unterauftragsverarbeitern.** NTT DATA setzt Unterauftragsverarbeiter ein, die sich außerhalb des Landes befinden können, in dem personenbezogene Daten erhoben werden, und die personenbezogene Daten als Unterauftragsverarbeiter verarbeiten. Einige Unterauftragsverarbeiter können personenbezogene Daten weiterübertragen.

7.2 **Liste der Unterauftragsverarbeiter**. Eine Liste der von NTT DATA direkt für die konkreten Leistungen als Auftragsverarbeiter eingesetzten Unterauftragsverarbeiter ist auf Anfrage bei dem in **Attachment A** genannten Ansprechpartner von NTT DATA erhältlich oder wird anderweitig auf einer Webseite von NTT DATA zur Verfügung gestellt.

7.3 **Allgemeine Zustimmung.** Der Kunde erteilt seine allgemeine Zustimmung zur Beauftragung von Unterauftragsverarbeitern durch NTT DATA, inklusive ihrer konzernverbundenen Unternehmen, damit diese einige oder alle Leistungen erbringen und personenbezogene Daten in seinem Auftrag verarbeiten können. Soweit dies nach geltendem Datenschutzrecht zulässig ist, stellt dieser AVV die allgemeine schriftliche Zustimmung des Kunden zur Untervergabe der Verarbeitung personenbezogener Daten durch NTT DATA an die laut der entsprechenden Liste vereinbarten Unterauftragsverarbeiter dar.

7.4 **Änderungen.** NTT DATA informiert den Kunden mindestens 30 Tage im Voraus schriftlich über beabsichtigte Änderungen an der vereinbarten Liste der Unterauftragsverarbeiter, sodass der Kunde die Möglichkeit hat, diesen Änderungen zu widersprechen. Der entsprechende Widerspruch muss innerhalb von 14 Tagen nach der Benachrichtigung schriftlich an den in **Attachment A** genannten Ansprechpartner von NTT DATA gerichtet werden. Legt der Kunde nicht innerhalb von 14 Tagen nach Mitteilung schriftlich Widerspruch gegen die vereinbarte Liste der Unterauftragsverarbeiter ein, so gilt dies als seine Zustimmung zu den Änderungen an der vereinbarten Liste der Unterauftragsverarbeiter.

7.5 **Erbringung von Leistungen**. NTT DATA ist dafür verantwortlich, dass eigene Unterauftragsverarbeiter die Pflichten von NTT DATA unter diesem AVV erfüllen.

8 Pflichten des Kunden

8.1 **Anfragen Betroffener**. Erhält NTT DATA eine Anfrage von Betroffenen des Kunden hinsichtlich der Ausübung eines oder mehrerer ihrer Rechte unter den geltenden Datenschutzgesetzen in Zusammenhang mit einer Leistung, bei der NTT DATA Auftragsverarbeiter oder Unterauftragsverarbeiter ist, leitet NTT DATA die betroffene Person weiter, damit die Anfrage direkt an den Kunden gerichtet werden kann. Der Kunde ist zuständig für die Beantwortung entsprechender Anfragen. NTT DATA kommt angemessenen Bitten des Kunden nach, ihn bei der Reaktion auf entsprechende Anfragen zu unterstützen. Der Kunde trägt die angemessenen Kosten, die NTT DATA bei der Bereitstellung dieser Unterstützung entstehen.

8.2 **Kundenanfragen**. NTT DATA kommt unverzüglich allen Aufforderungen des Kunden oder Anweisungen ermächtigter Personen nach, (a) die personenbezogenen Daten zu ändern, zu übertragen, zu löschen oder anderweitig zu verarbeiten oder ihre unzulässige Verarbeitung einzustellen, zu begrenzen oder zu korrigieren, (b) die sich auf die Verpflichtungen des Kunden in Bezug auf die Sicherheit der Verarbeitung zu beziehen und (c) die unter geltendem Datenschutz die vorherige Rücksprache mit dem Kunden erfordern, wobei die Art der Verarbeitung und die NTT DATA zur Verfügung stehenden Informationen berücksichtigt werden.

8.3 **Zusicherungen**. Der Kunde versichert, dass (a) er über alle erforderlichen Rechte verfügt, um NTT DATA die personenbezogenen Daten für die in Zusammenhang mit den Leistungen durchzuführende Verarbeitung zur Verfügung zu stellen und (b) die voraussichtliche Verwendung der personenbezogenen Daten durch NTT DATA für die vom Kunden ausdrücklich angewiesenen Geschäftszwecke allen geltenden Datenschutzgesetzen entspricht.

8.4 **Hinweise zum Datenschutz**. Soweit dies nach geltendem Datenschutzrecht erforderlich ist, ist der Kunde dafür verantwortlich, dass Betroffenen alle nötigen Datenschutzhinweise zur Verfügung gestellt werden und dass (sofern keine andere, in den geltenden Datenschutzgesetzen definierte Rechtsgrundlage die Rechtmäßigkeit der Verarbeitung stützt) alle erforderlichen Einwilligungen Betroffener in die Verarbeitung eingeholt und protokolliert werden. Sollte eine solche Einwilligung von einer betroffenen Person widerrufen werden, ist der Kunde dafür zuständig, NTT DATA darüber zu informieren. NTT DATA hingegen bleibt für die Umsetzung der Anweisungen des Kunden in Bezug auf die Verarbeitung entsprechender personenbezogenen Daten verantwortlich.

9 Sicherheit

9.1 **Technische und organisatorische Maßnahmen**. NTT DATA ergreift geeignete technische und organisatorische Maßnahmen („**TOM**“), um die Sicherheit der personenbezogenen Daten im Sinne der geltenden Datenschutzgesetze zu gewährleisten, wie in Attachment C niedergelegt. Dies beinhaltet den Schutz der personenbezogenen Daten vor Sicherheitsverstößen, die eine versehentliche oder unrechtmäßige Vernichtung, den Verlust, die Änderung, unbefugte Offenlegung von oder den unberechtigten Zugriff auf die personenbezogenen Daten nach sich ziehen könnten.

9.2 **Zugang zu personenbezogenen Daten**. NTT DATA gewährt eigenen Mitarbeitern nur insoweit Zugriff auf die verarbeiteten personenbezogenen Daten, wie dies zur Erfüllung, Bearbeitung und Überwachung des Kundenvertrags unbedingt erforderlich ist. NTT DATA stellt sicher, dass die Personen, die zur Verarbeitung der erhaltenen personenbezogenen Daten befugt sind, sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

9.3 **Kostenverhandlungen**. Die Parteien verhandeln nach Treu und Glauben über die Kosten, die gegebenenfalls für die Umsetzung wesentlicher Änderungen anfallen, sofern diese nicht durch spezifische aktualisierte Sicherheitsanforderungen im geltenden Datenschutzrecht oder durch die zuständigen Datenschutzbehörden vorgeschrieben sind. (In diesem Fall übernimmt der NTT DATA die Kosten).

10 Überprüfungen

10.1 **Zertifizierungen**. NTT DATA erhält alle Zertifizierungen aufrecht, zu deren Aufrechterhaltung und Einhaltung NTT DATA (wie im Kundenvertrag ausdrücklich festgelegt) vertraglich verpflichtet ist. Bei Bedarf erneuert der NTT DATA diese Zertifizierungen.

10.2 **Vorlage von Nachweisen**. Auf schriftliches Verlangen des Kunden stellt NTT DATA dem Kunden Nachweise dieser Zertifizierungen in Bezug auf die Verarbeitung personenbezogener Daten zur Verfügung, was entsprechende Zertifizierungen oder Prüfberichte hinsichtlich der Computerumgebung und physischen Datenzentren, die NTT DATA zur Verarbeitung personenbezogener Daten bei Erbringung der Leistungen einsetzt, beinhaltet, sodass der Kunde in angemessener Weise verifizieren kann, ob NTT DATA den eigenen hierunter begründeten Verpflichtungen nachkommt.

10.3 **Konformität mit technischen und organisatorischen Maßnahmen**. NTT DATA kann entsprechende Zertifikate und Bescheinigungen auch heranziehen, um die Erfüllung der in Ziff. 9.1 dargelegten Anforderungen nachzuweisen.

10.4 **Vertrauliche Informationen**. Alle von NTT DATA zur Verfügung gestellten Nachweise sind vertrauliche Informationen und unterliegen den Auflagen zu Geheimhaltung und Weitergabe von NTT DATA und/oder eines Unterauftragsverarbeiters von NTT DATA.

10.5 **Überprüfungen durch den Kunden**. Der Kunde ist dazu berechtigt, die Räumlichkeiten und den Betrieb von NTT DATA zu überprüfen, sofern dies mit seinen personenbezogenen Daten in Zusammenhang steht, wenn

(a) NTT DATA keine ausreichenden Nachweise für die gemäß Artikel 9 ergriffenen Maßnahmen vorgelegt hat,

(b) die Überprüfung offiziell von einer zuständigen Datenschutzbehörde gefordert wird oder

(c) das anwendbare Datenschutzrecht dem Kunden ein direktes Prüfrecht einräumt (solange der Kunde nur einmal innerhalb eines Zwölfmonatszeitraums eine solche Überprüfung durchführt, falls nicht zwingend anwendbare Datenschutzgesetze eine häufigere Überprüfung erfordern).

Konzernverbundene Unternehmen der NTT DATA sind beabsichtigte Drittbegünstigte dieses Abschnitts.

10.6 **Prüfverfahren des Kunden**. Der Kunde kann mit der Überprüfung von NTT DATA einen unabhängigen Dritten (der jedoch kein Mitbewerber von NTT DATA und auch nicht unzureichend qualifiziert sein darf und unabhängig sein muss) beauftragen, der zuvor eine Vertraulichkeitsvereinbarung mit NTT DATA abschließen muss. Der Kunde hat jede Überprüfung mindestens 60 Tage im Voraus anzukündigen, es sei denn, zwingend anwendbare Datenschutzgesetze oder eine zuständige Datenschutzbehörde verlangen eine kürzere Frist. NTT DATA wird bei solchen Überprüfungen kooperieren und den Prüfern des Kunden angemessenen Zugang zu allen Räumlichkeiten und Geräten gewähren, die in Zusammenhang mit der Verarbeitung der personenbezogenen Daten des Kunden stehen. Die Überprüfungen durch den Kunden sind zeitlich auf maximal drei (3) Werktage begrenzt. Abgesehen davon nutzen die Parteien aktuelle Bescheinigungen oder andere Prüfberichte, um wiederholte Prüfungen zu vermeiden oder zu minimieren. Der Kunde trägt die Kosten der von ihm durchgeführten Überprüfungen, sofern diese nicht einen wesentlichen Verstoß auf Seiten von NTT DATA gegen diesen AVV ergeben. In diesem Fall trägt NTT DATA die Kosten der Überprüfung. Wird bei der Überprüfung festgestellt, dass NTT DATA gegen eigene Pflichten unter dem AVV verstoßen hat, behebt NTT DATA entsprechende Verstöße unverzüglich auf eigene Kosten.

11 Umgang mit Zwischenfällen

11.1 **Sicherheitsvorfälle**. Erlangt NTT DATA Kenntnis von einer Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Vernichtung, zu Verlust, Änderung, unbefugter Offenlegung von oder zum Zugriff auf personenbezogene Daten führt, während diese von NTT DATA verarbeitet werden (jeweils ein „**Sicherheitsvorfall**"), so wird NTT DATA unverzüglich

(a) den Kunden über den Sicherheitsvorfall informieren.

(b) den Sicherheitsvorfall untersuchen und dem Kunden hinlängliche Informationen über den Sicherheitsvorfall zur Verfügung stellen, was die Angabe beinhaltet, ob der Sicherheitsvorfall personenbezogene Daten des Kunden betrifft.

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

11.2 **Meldung von Sicherheitsvorfällen**. Die Meldung von Sicherheitsvorfällen erfolgt gemäß Ziff. 11.4. Betrifft ein Sicherheitsvorfall personenbezogene Daten des Kunden, unternimmt NTT DATA angemessene Anstrengungen, um den Kunden in die Lage zu versetzen, eine gründliche Untersuchung des Sicherheitsvorfalls durchzuführen, eine korrekte Reaktion auszuarbeiten und geeignete weitere Schritte im Hinblick auf den Sicherheitsvorfall zu unternehmen. NTT DATA bemüht sich in angemessener Weise, den Kunden bei der Erfüllung seiner unter geltendem Datenschutzrecht bestehenden Verpflichtungen zur Benachrichtigung der zuständigen Datenschutzbehörde und der betroffenen Personen über entsprechende Sicherheitsvorfälle zu unterstützen. Die Meldung eines Sicherheitsvorfalls durch NTT DATA oder die Reaktion darauf gemäß diesem Artikel ist kein Anerkenntnis eines Verschuldens oder einer Haftung von NTT DATA für den Sicherheitsvorfall.

11.3 **Sonstige Vorfälle**. NTT DATA informiert den Kunden unverzüglich, wenn NTT DATA Kenntnis erhält von

(a) Beschwerden oder Ersuchen in Bezug auf die Ausübung von Betroffenenrechten unter geltendem Datenschutzrecht in Bezug auf personenbezogene Daten, die NTT DATA im Auftrag des Kunden und seinen Betroffenen verarbeitet

(b) Untersuchungen oder Beschlagnahmen der personenbezogenen Daten des Kunden durch Regierungsbeamte oder konkreten Hinweisen, dass eine solche Untersuchung oder Beschlagnahme unmittelbar bevorsteht, oder

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

11.4 **Benachrichtigung des Kunden.** Alle Mitteilungen an den Kunden unter dieser Ziff. 11 sind an dessen in **Attachment A** aufgeführten Ansprechpartner zu richten, wobei eine der in **Attachment A** genannten Methoden zur Kontaktierung desselben zu nutzen ist.

12 Grenzüberschreitende Übertragung von personenbezogenen Daten

12.1 **Allgemeines.** Sofern nicht an anderer Stelle dieses AVV ausgeführt, können personenbezogene Daten, die NTT DATA im Auftrag des Kunden verarbeitet, in jedes Land, in dem NTT DATA oder Unterauftragsverarbeiter von NTT DATA tätig sind, übertragen und dort gespeichert und verarbeitet werden.

12.2 **Beschränkte Übertragungen**. Bei einer beschränkten Übertragung personenbezogener Daten haben der Datenexporteur und der Datenimporteur die personenbezogenen Daten in Übereinstimmung mit allen geltenden Datenschutzgesetzen zu übermitteln und zu verarbeiten. Insbesondere gilt

(a) **Anhang D**, wenn personenbezogene Daten, die den EU-Datenschutzgesetzen unterliegen, von einem Datenexporteur an einen Datenimporteur übertragen werden, der als Auftragsverarbeiter agiert.

(b) **Anhang E**, wenn personenbezogene Daten, die dem geltenden Datenschutzrecht der in **Anhang E** aufgeführten spezifischen Bestimmungen zur Zuständigkeit unterliegen, in Gebiete außerhalb der entsprechenden Gerichtsbarkeiten übertragen werden.

12.3 **Umsetzung der Standardvertragsklauseln**. Falls eine grenzüberschreitende Übertragung personenbezogener Daten zwischen NTT DATA und dem Kunden die Unterzeichnung von Standardvertragsklauseln erfordert, um das geltende Datenschutzrecht einzuhalten, gilt die Unterzeichnung dieses AVV, des Kundenvertrags oder eines anderen verbindlichen Dokuments durch die Parteien als ihre jeweilige Unterzeichnung der SCC.

12.4 **Änderung der gesetzlichen Übertragungsregelung**. Soweit sich NTT DATA auf die europäischen Standardvertragsklauseln, den UK-Nachtrag oder andere spezifische gesetzliche Regelungen zur Vereinheitlichung zwischenstaatlicher Datenübertragungen stützt und diese Regelungen zu einem späteren Zeitpunkt geändert, aufgehoben oder von einem zuständigen Gericht für ungültig befunden werden, verpflichten sich der Kunde und NTT DATA, nach Treu und Glauben zusammenzuarbeiten, um die Übertragung unverzüglich auszusetzen oder eine geeignete alternative Regelung anzuwenden, unter der die Übertragung rechtmäßig erfolgen kann.

13 Rückgabe oder Vernichtung von personenbezogenen Daten

13.1 **Löschung durch den Kunden.** Bei bestimmten Leistungen ist der Kunde für das Aufspielen und Hosting, die Verarbeitung und Nutzung personenbezogener Daten verantwortlich. Hier kann nur der Kunde auf die im entsprechenden Dienst gespeicherten personenbezogenen Daten zugreifen, sie extrahieren und löschen. Wenn der jeweilige Dienst den Zugriff, die Speicherung oder die Extraktion der vom Kunden bereitgestellten Software nicht unterstützt, übernimmt NTT DATA keine Haftung für die Löschung personenbezogener Daten wie in diesem Artikel 13.1 dargelegt.

13.2 **Löschung oder Rückgabe**. Wenn der Kundenvertrag die Aufbewahrung personenbezogener Daten durch NTT DATA vorschreibt, löscht NTT DATA diese personenbezogenen Daten innerhalb des im Kundenvertrag vereinbarten Zeitraums, es sei denn, NTT DATA ist nach geltendem Recht zur Aufbewahrung entsprechender personenbezogener Daten berechtigt oder verpflichtet. Wurde die Aufbewahrung personenbezogener Daten nicht im Kundenvertrag geregelt, so wird NTT DATA auf eigene Kosten alle personenbezogenen Daten entweder löschen, vernichten oder an den Kunden zurückgeben und alle vorhandenen Kopien vernichten oder zurückgeben, wenn NTT DATA die Erbringung von Leistungen wie folgt einstellt:

(a) bei Beendigung der Tätigkeiten, die in Zusammenhang mit der Verarbeitung stehen

(b) bei Außerkrafttreten dieses AVV

(c) wenn der Kunde NTT DATA schriftlich dazu auffordert oder

(d) wenn NTT DATA ansonsten alle in Zusammenhang mit den Leistungen vereinbarten Zwecke in Bezug auf die Verarbeitungstätigkeiten erfüllt hat und der Kunde von NTT DATA keine weitere Verarbeitung wünscht.

13.3 **Bestätigung der Vernichtung**. Auf Anfrage des Kunden bestätigt NTT DATA die Vernichtung besagter Daten schriftlich. Ist die Löschung oder Rückgabe der personenbezogenen Daten aus einem beliebigen Grund nicht möglich oder wurden Sicherungskopien und/oder archivierte Kopien der personenbezogenen Daten erstellt, bewahrt NTT DATA die entsprechenden personenbezogenen Daten unter Wahrung des anwendbaren Datenschutzrechts auf.

13.4 **Dritte**. Bei Beendigung dieses AVV wird NTT DATA alle Unterauftragsverarbeiter, die seine Verarbeitungstätigkeiten unterstützen, benachrichtigen und sicherstellen, dass diese nach Ermessen des Kunden die personenbezogenen Daten entweder vernichten oder sie an den Kunden zurückgeben.

14 Haftung und Gewährleistung

Jedwede Haftungsbeschränkung im Kundenvertrag **gilt** für diesen AVV. Ausnahmen bestehen lediglich in dem Umfang, in dem eine solche Beschränkung (a) die Haftung der Parteien gegenüber Betroffenen einschränkt oder (b) nach geltendem Recht nicht zulässig sind.

15 Mitteilungen und Benachrichtigungen

15.1 Jedwede Mitteilung oder sonstige Korrespondenz an die und zwischen den Parteien im Rahmen oder in Verbindung mit diesem AVV hat in schriftlicher Form zu erfolgen und ist der jeweils anderen Partei per E-Mail zuzustellen.

15.2 Ziff. 15.1 gilt nicht für die Zustellung von Verfahrensunterlagen oder sonstigen Schriftstücken im Rahmen von Rechtsverfahren bzw. Schiedsverfahren oder einer anderen Methode der Streitbeilegung.

15.3 Jedwede Mitteilung oder sonstige Korrespondenz gilt als getätigt, wenn sie

(a) persönlich übergeben wurde.

(b) auf dem Postweg (frankiert, per Einschreiben oder Einschreiben mit Rückschein) erhalten wurde oder

(c) durch einen international anerkannten Kurierdienst (der Nachweis der Zustellung ist durch den Absender zu erbringen) an die (oben angegebene) Hausanschrift zugestellt wurde (wobei eine elektronische Kopie an die in der Tabelle oben genannte E-Mail-Adresse zu senden ist).

16 Sonstige Bestimmungen

16.1 **In Widerspruch zueinanderstehende Bestimmungen.** Die Bestimmungen des Kundenvertrags bleiben in vollem Umfang in Kraft, sofern sie nicht in diesem AVV geändert werden. Soweit NTT DATA bei Erfüllung des Kundenvertrags im Auftrag des Kunden personenbezogene Daten verarbeitet, die dem anwendbaren Datenschutzrecht unterliegen, gelten die Bestimmungen dieses AVV. Sollten die Bestimmungen dieses AVV im Widerspruch zu den Bestimmungen des Kundenvertrags stehen, so haben die Bestimmungen dieses AVV Vorrang vor jenen des Kundenvertrags.

16.2 **Anwendbares Recht.** Dieser AVV unterliegt den Gesetzen jenes Landes, das in den entsprechenden Bestimmungen des Kundenvertrags angegeben ist. Die europäischen Standardvertragsklauseln und der UK-Nachtrag unterliegen den Gesetzen, die in den EU-SCC bzw. im UK-Nachtrag vorgesehen sind.

16.3 **Beilegung von Streitigkeiten.** Alle Streitigkeiten, die sich aus oder in Zusammenhang mit diesem AVV ergeben, werden ausschließlich dem zuständigen Gericht der in den entsprechenden Bestimmungen des Kundenvertrags angegebenen Rechtsordnung vorgelegt.

16.4 **Exemplare.** Dieser AVV kann in einer beliebigen Anzahl von Exemplaren ausgefertigt werden, von denen jedes für sich ein Original darstellt, die aber gemeinsam eine Vereinbarung bilden. Entscheiden sich eine oder beide Parteien für die elektronische Unterzeichnung dieses AVV, so hat jede elektronische Unterschrift dieselbe Gültigkeit und Rechtswirkung wie eine eigenhändige Unterschrift und wird in der Absicht geleistet, diesen AVV zu legalisieren und den Willen der betreffenden Partei zu bekunden, durch diesen AVV gebunden zu sein.

16.5 **Änderungen.** NTT DATA wird beabsichtigte Änderungen an diesem AVV auf einer NTT DATA Website veröffentlichen oder dem Kunden mindestens 14 Tage im Voraus eine schriftliche Benachrichtigung zukommen lassen, die es dem Kunden ermöglicht, solchen Änderungen zu widersprechen. Ein solcher Widerspruch muss innerhalb von zehn Tagen nach der Benachrichtigung schriftlich an die in Anhang A genannte Kontaktperson von NTT DATA gerichtet werden. Erhebt der Kunde nicht innerhalb von zehn Tagen nach der Benachrichtigung schriftlich Einspruch gegen die beabsichtigten Änderungen, so gilt dies als Zustimmung zu den Änderungen an diesem AVV.

Attachment A Ansprechpartner

Kontaktdaten des Datenschutzbeauftragten/Compliance-Beauftragten des Kunden:

Gegebenenfalls wie in der Kundenvereinbarung oder in den Informationen über den Vertreter des Kunden gemäß Art. 4 Abs. 17 i.V.m. Art. 27 der DS-GVO in der EU und im Vereinigten Königreich angegeben oder wie auf der Website des Kunden vorgesehen oder vom Kunden schriftlich übermittelt.

Kontaktdaten des Datenschutzbeauftragten von NTT DATA:

Kontaktdaten: NTT Germany AG & Co. KG, Der Datenschutzbeauftragte, Rheinstr. 10b, 14513 Teltow, Germany, +49 3328 3863137, EU.DE.Datenschutzbeauftragter@global.ntt

Attachment B Einzelheiten der Verarbeitung

Kategorien von betroffenen Personen, deren personenbezogene Daten übermittelt werden

NTT DATA bestätigt, dass der Datenimporteur – je nach Inanspruchnahme der Leistungen durch den Kunden – möglicherweise die personenbezogenen Daten einer der folgenden Arten von Betroffenen verarbeitet:

- Mitarbeiter, Auftragnehmer, Zeitarbeiter, Vertreter und Handlungsbevollmächtigte des Datenexporteurs
- Nutzer (z. B. Endnutzer von Kunden) und andere Betroffene, die Leistungen in Anspruch nehmen
- (gegebenenfalls) juristische oder Rechtspersonen

Kategorien der übermittelten personenbezogenen Daten
NTT DATA bestätigt, dass NTT DATA – je nach Inanspruchnahme der Leistungen durch den Kunden – möglicherweise unter anderem die folgenden Arten von personenbezogenen Daten verarbeitet, ohne jedoch darauf beschränkt zu sein:

- Grunddaten zur Person (z. B. Vorname, Nachname, E-Mail-Adresse und Anschrift des Arbeitsplatzes)
- Bankkontodaten
- Authentifizierungsdaten (z. B. Benutzername und Passwort)
- Kontaktdaten (z. B. berufliche E-Mail-Adresse und Telefonnummer)
- Berufliche oder beschäftigungsbezogene Informationen (z. B. Name des Arbeitgebers und Berufsbezeichnung)
- eindeutige Identifikationsnummern und Signaturen (z. B. IP-Adressen)
- Standortdaten (z. B. Standortnetzdaten)
- Gerätekennung (z. B. IMEI-Nummer und MAC-Adresse)

Übertragung sensibler Daten (falls zutreffend) und angewandte Beschränkungen oder Sicherheitsmaßnahmen, 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 Datenzugriffs, Beschränkungen der Weiterübertragung oder zusätzliche Sicherheitsmaßnahmen

- sofern zutreffend, biometrische Informationen (z. B. Fingerabdrücke in Rechenzentren von NTT DATA)

NTT DATA wird den Kunden schriftlich darüber informieren, wenn NTT DATA zur Erbringung der Dienste über die oben genannten Daten hinaus weitere sensible Daten erheben muss. **Anhang C** enthält Angaben zu den anzuwendenden Beschränkungen.

Häufigkeit der Übertragung (beispielsweise, ob die Daten einmalig oder kontinuierlich übermittelt werden)
Personenbezogene Daten können kontinuierlich übermittelt werden, um die Leistungen unter dem bestehenden Kundenvertrag zu erbringen.

Art der Verarbeitung
Die übertragenen personenbezogenen Daten können den folgenden grundlegenden Verarbeitungstätigkeiten unterzogen werden:

- Erhalt von Daten, einschließlich Erfassung, Zugriff, Abruf, Aufzeichnung und Dateneingabe
- Datenhaltung, einschließlich Speicherung, Organisation und Strukturierung
- Datennutzung, einschließlich Analyse, Konsultation, Prüfung, automatisierte Entscheidungsfindung und Erstellung von Persönlichkeitsprofilen
- Aktualisierung von Daten, einschließlich Korrektur, Anpassung, Änderung, Angleichung und Verknüpfung
- Schutz von Daten, einschließlich Einschränkung, Verschlüsselung und Sicherheitsprüfung
- Datenweitergabe, einschließlich Offenlegung, Verbreitung, Gewährung des Zugriffs oder sonstige Bereitstellung
- Rückgabe von Daten an den Datenexporteur oder die Betroffenen
- Löschen von Daten, einschließlich Vernichtung und Löschung

Zweck(e) der Datenübertragung und Weiterverarbeitung
Der Zweck der Verarbeitung personenbezogener Daten besteht darin, dass NTT DATA die Leistungen im Rahmen des bestehenden Kundenvertrags erbringt. Dies kann folgendes beinhalten:

- Erbringung von Leistungen: Bereitstellung von Produkten und Dienstleistungen im Einklang mit dem Kundenvertrag;
- Lösung von Anfragen: Kommunikation und Koordinierung der Lösung von Supportanfragen in einer zeitnahen Weise;

- Geschäftsprozessverbesserungen: Verbesserung der Art und Weise, wie die Dienstleistungen für den 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 von Systemen: Gewährleistung der Verfügbarkeit und Sicherheit der Systeme

Zeitraum, für den die personenbezogenen Daten aufbewahrt werden, oder – falls diese Angabe nicht möglich ist – die Kriterien, nach denen dieser Zeitraum festgelegt wird
Siehe Artikel 13 des AVV
Bei Übertragungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Siehe Ziff. 7 des AVV. Eine Liste der Unterauftragsverarbeiter von NTT DATA, die NTT DATA als Auftragsverarbeiter direkt mit der Erbringung bestimmter Dienste beauftragt, ist auf Anfrage bei der in Attachment A genannten Kontaktperson von NTT DATA erhältlich oder kann auf der NTT DATA Website eingesehen werden. Derartige Unterauftragsverarbeiter dürfen personenbezogene Daten nur zur Erbringung einiger oder aller von NTT DATA beauftragten Dienste erhalten und dürfen personenbezogene Daten nicht für andere Zwecke verwenden.

Ermächtigte Personen: NTT DATA verarbeitet die personenbezogenen Daten nur auf belegte Anweisung des Kunden durch die folgenden Kategorien von Personen, die dieser dazu ermächtigt hat, NTT DATA Anweisungen zur Verarbeitung personenbezogener Daten zu erteilen:
Wie vom Kunden von Zeit zu Zeit schriftlich mitgeteilt.

Attachment C Technische und organisatorische Maßnahmen

1 Präambel

1.1 NTT DATA ist bestrebt, durch Technologie und Innovation eine sichere und vernetzte Zukunft zu ermöglichen. Wir haben technische und organisatorische Maßnahmen („TOM“) definiert, die erklären, wie wir den Schutz personenbezogener Daten auf transparente, faire, moralisch korrekte und rechtmäßige Weise sicherstellen.

1.2 Unsere TOM basieren auf den bewährtesten Verfahren der Branche und den geltenden rechtlichen Anforderungen in den Ländern, in denen wir tätig sind, wobei die Art der von uns verarbeiteten Daten und die Kosten der Umsetzung berücksichtigt werden.

1.3 Wenn Sie Fragen zu unseren TOM haben oder wissen möchten, wie sie sich auf unsere Produkte, Dienstleistungen und Lösungen beziehen, kontaktieren Sie uns bitte unter privacyoffice@global.ntt

(A) Datenschutzmaßnahmen

2 Verwaltung und Betriebsmodell

2.1 NTT DATA verpflichtet sich, personenbezogene Daten auf verantwortungsvolle Weise zu verarbeiten und hat eine Organisationsstruktur sowie Rollen und Zuständigkeiten für die Verwaltung und Überwachung der Verarbeitung personenbezogener Daten eingeführt.

2.2 Es wurden verschiedene Verwaltungs- und Kontrollstrukturen eingeführt, um sicherzustellen, dass Datenschutzangelegenheiten von der entsprechenden Führungsebene von NTT DATA überprüft werden. Die letztendliche Verantwortung für den Datenschutz liegt beim Vorstand der NTT DATA Ltd. und wird durch bestimmte Funktionen im gesamten Unternehmen (unter anderem Datenschutzbeauftragte bzw. entsprechende Rollen) unterstützt.

2.3 NTT DATA unterrichtet das Audit and Risk Committee (den Prüf- und Risikoausschuss) der NTT DATA Ltd. regelmäßig über die Konzeption und die operative Effektivität der Datenschutzmaßnahmen.

3 Richtlinien, Verfahren und Vorgaben

3.1 NTT DATA hat eigene Richtlinien, Verfahren, Standards und Vorgaben eingeführt und kommuniziert, die detailliert beschreiben, wie die Mitarbeiter von NTT DATA personenbezogene Daten verarbeiten sollen. Dazu gehören die folgenden:

(a) Datenschutz- und IT-Sicherheitsrichtlinie

(b) Richtlinie zu Betroffenenrechten

(c) Richtlinie zur Meldung von Datenschutzverletzungen

3.2 NTT DATA hat Datenschutzhinweise definiert und kommuniziert, die Mitarbeiter, Kunden und andere Interessengruppen über die Verarbeitung personenbezogener Daten informieren.

3.3 NTT DATA verfügt über ein Verfahren zur Datenschutzfolgenabschätzung („**DSFA**“) und führt bei Bedarf und in Übereinstimmung mit den geltenden Datenschutzgesetzen entsprechende Datenschutzfolgenabschätzungen durch.

4 Datenschutz durch Technikgestaltung

NTT DATA verpflichtet sich, angemessene Maßnahmen zu ergreifen, um eigene Kunden bei der Einhaltung des Datenschutzrechts zu unterstützen. Bei der Entwicklung der Produkte, Leistungen und Lösungen von NTT DATA werden möglichst die Grundsätze des Datenschutzes durch Technik und durch Voreinstellungen („Privacy by Design“ bzw. „Privacy by Default“) angewandt.

5 Datenlandschaft

5.1 NTT DATA hat Prozesse implementiert, um die verarbeiteten personenbezogenen Daten zu identifizieren, zu erfassen, zu bewerten und zu verstehen.

5.2 NTT DATA unterhält in Übereinstimmung mit geltendem Datenschutzrecht Aufzeichnungen der verarbeiteten personenbezogenen Daten.

6 Information Lifecycle Management

6.1 NTT DATA hat Richtlinien und Verfahren implementiert, die sicherstellen, dass personenbezogene Daten während ihres gesamten Lebenszyklus (von der Erhebung über die Verwendung, Aufbewahrung, Weitergabe und Vernichtung) angemessen verarbeitet werden.

6.2 NTT DATA verfügt über eine Richtlinie und einen Zeitplan für die Datenspeicherung, die mit geltendem Recht in Einklang stehen. NTT DATA speichert personenbezogene Daten nur, wenn ein legitimer geschäftlicher Grund dafür vorliegt und tut dies gemäß den eigenen Pflichten unter geltendem Recht. NTT DATA vernichtet, löscht oder anonymisiert personenbezogene Daten, wenn die Aufbewahrungsfrist abgelaufen ist und kein legitimer geschäftlicher Grund mehr vorliegt, die personenbezogenen Daten länger aufzubewahren.

6.3 NTT DATA bewahrt die im Auftrag von Kunden verarbeiteten personenbezogenen Daten in Übereinstimmung mit den Vorgaben dieser Kunden auf und vernichtet, löscht, anonymisiert oder gibt die personenbezogenen Daten zurück, wenn nach geltendem Recht keine weiteren Verpflichtungen zur Aufbewahrung der personenbezogenen Daten bestehen.

6.4 NTT DATA hat alle zumutbaren Anstrengungen unternommen, um sicherzustellen, dass die personenbezogenen Daten richtig, vollständig und auf dem neuesten Stand sind.

7 Betroffenenrechte

7.1 Die Datenschutzgesetze einiger Länder gewähren Betroffenen besondere Rechte in Bezug auf ihre personenbezogenen Daten. NTT DATA verpflichtet sich, diese Rechte zu wahren und sicherzustellen, dass NTT DATA auf Anfragen Betroffener auf transparente, billige, anständige und rechtmäßige Weise reagiert.

7.2 NTT DATA hat eine Richtlinie zu Betroffenenrechten und ein Verfahren für die Reaktion auf Anfragen von Betroffenen eingeführt, um deren Rechte in Übereinstimmung mit den geltenden Datenschutzgesetzen zu wahren.

7.3 NTT DATA unterstützt die folgenden Betroffenenrechte:

(a) das Recht auf Information

(b) das Recht auf Zugang

(c) das Recht auf Berichtigung

(d) das Recht auf Vergessenwerden

(e) das Recht auf Datenübertragbarkeit

(f) das Recht auf Nutzungsbeschränkung

(g) das Widerspruchsrecht (einschließlich des Rechts, Direktmarketing und den Verkauf personenbezogener Daten abzulehnen)

(h) das Recht auf Anfechtung automatisierter Entscheidungen sowie

(i) das Beschwerderecht

7.4 NTT DATA führt Aufzeichnungen über alle eingegangenen Anfragen Betroffener und die zur Reaktion darauf getroffenen Maßnahmen.

7.5 NTT DATA unterstützt Kunden auf Wunsch angemessen bei der Reaktion auf Anfragen Betroffener in Übereinstimmung mit entsprechenden getroffenen Vereinbarungen.

7.6 NTT DATA verpflichtet sich, auf alle Anfragen von Behörden auf Zugriff zu personenbezogenen Daten in Übereinstimmung mit geltendem Recht zu reagieren und, soweit zulässig, die Rechte und Freiheiten des Einzelnen zu wahren und durchzusetzen. Wird NTT DATA dazu aufgefordert, personenbezogene Daten offenzulegen, so geschieht dies in Übereinstimmung mit der internen Richtlinie für behördliche Datenauskunftsersuchen. Über entsprechende Anfragen werden Aufzeichnungen geführt und diese in einem jährlichen Transparenzbericht veröffentlicht.

8 Grenzüberschreitende Übertragungen

8.1 NTT DATA stützt sich bei der rechtmäßigen Übertragung personenbezogener Daten aus der Europäischen Union oder dem Vereinigten Königreich in Drittländer auf Standardvertragsklauseln und hat entsprechende Vereinbarungen mit Tochtergesellschaften, verbundenen Unternehmen, Auftragsverarbeitern, Unterauftragsverarbeitern und Kunden von NTT DATA getroffen, um grenzüberschreitende Übertragungen zu unterstützen. Falls erforderlich, holt NTT DATA möglicherweise auch die Zustimmung der jeweiligen Betroffenen zur grenzüberschreitenden Übertragung ihrer personenbezogenen Daten ein.

8.2 Bei der grenzüberschreitenden Übertragung personenbezogener Daten führt NTT DATA eine Folgenabschätzung durch, um festzustellen, ob in jenem Land, in das personenbezogene Daten übertragen werden, die Rechte und Freiheiten Betroffener in gleichem Umfang geschützt werden, wie im jeweiligen Herkunftsland. Werden Abweichungen erkannt, hat NTT DATA zusätzliche Maßnahmen ergriffen, um die Betroffenenrechten in Übereinstimmung mit eigenen Richtlinien zu unterstützen und sicherzustellen, dass personenbezogene Daten auf transparente, faire und anständige Weise verarbeitet werden.

9 Gesetzliche Bestimmungen

NTT DATA verpflichtet sich, sich über Änderungen der Datenschutzgesetze in jenen Ländern, in denen NTT DATA tätig ist, auf dem Laufenden zu halten, und hat Verfahren zur Unterstützung der Einhaltung derselben implementiert.

10 Schulung und Sensibilisierung

NTT DATA verlangt von allen Mitarbeitern, dass sie in regelmäßigen Abständen Schulungen zum Thema Datenschutz absolvieren. Alle Richtlinien, Verfahren, Standards und Vorgaben zum Datenschutz stehen den Mitarbeitern zur Verfügung und werden regelmäßig kommuniziert. Bei Bedarf finden lokale, regionale oder funktionale Schulungen statt, um die Mitarbeiter von NTT DATA dabei zu unterstützen, in Übereinstimmung mit den Anforderungen in bestimmten Ländern, Regionen oder Geschäftsbereichen zu handeln.

11 Sicherheit in Bezug auf Datenschutz

11.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, des Kontextes und des Zwecks der Verarbeitung personenbezogener Daten und der Risiken für die Rechte und Freiheiten der Betroffenen hat NTT DATA angemessene technische und organisatorische Maßnahmen ergriffen, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sicherzustellen.

11.2 Die Sicherheitsverfahren von NTT DATA orientieren sich an ISO 27001 und dem NIST Cybersecurity Framework („CSF“).

12 Reaktion und Benachrichtigung bei Verstößen

12.1 NTT DATA verfügt über Richtlinien, Prozesse und Verfahren zur Identifizierung, Erkennung, Reaktion, Wiederherstellung und Benachrichtigung der entsprechenden Beteiligten im Falle einer Verletzung des Schutzes personenbezogener Daten. Dazu gehören Regelungen für die Durchführung einer Ursachenanalyse und das Umsetzen von Abhilfemaßnahmen.

12.2 NTT DATA verpflichtet sich, sicherzustellen, dass die zuständigen Datenschutzbehörden, die betroffenen Kunden und die jeweiligen Betroffenen im Falle einer Datenschutzverletzung in Übereinstimmung mit geltendem Datenschutzrecht und vertraglichen Verpflichtungen benachrichtigt werden.

12.3 NTT DATA führt Aufzeichnungen über alle Verletzungen des Schutzes personenbezogener Daten und die als Reaktion auf entsprechende Ereignisse ergriffenen Maßnahmen.

12.4 Die Maßnahmen des Zwischenfallmanagements von NTT DATA zur Identifizierung, Erkennung, Reaktion und Behebung von Informationssicherheitsvorfällen sind unten in Abschnitt B dieser TOM dargelegt.

13 Umgang mit Dritten

13.1 NTT DATA haftet für die Handlungen eigener Auftragsverarbeiter und Unterauftragsverarbeiter, die personenbezogene Daten im Auftrag von NTT DATA verarbeiten. NTT DATA bewertet die Fähigkeit eigener Auftragsverarbeiter, personenbezogene Daten in Übereinstimmung mit den Vorgaben von NTT DATA zu schützen, zum Zeitpunkt ihrer Beauftragung und auch danach in regelmäßigen Abständen.

13.2 Die Auftragsverarbeiter und Unterauftragsverarbeiter von NTT DATA sind verpflichtet, entsprechende Vereinbarungen zu unterzeichnen, welche die Verarbeitung und den Schutz personenbezogener Daten regeln. Diese enthalten Anforderungen, um sicherzustellen, dass dieselben Verpflichtungen auf alle weiteren Auftragsverarbeiter, die personenbezogene Daten verarbeiten, übertragen werden.

(B) Maßnahmen zur Informationssicherheit

NTT DATA verpflichtet sich, dafür zu sorgen, dass Informationssicherheitskontrollen eingeführt und ordnungsgemäß unterhalten werden, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten zu schützen.

NTT DATA unterhält ein konzernweites Informationssicherheitsmanagementsystem („**ISMS**“), das nach ISO 27001 zertifiziert ist.

14 Funktionen und Zuständigkeiten im Bereich der Informationssicherheit

14.1 Die Funktionen und Zuständigkeiten im Bereich der Informationssicherheit wurden offiziell zugewiesen. Dies beinhaltet Berichtswege, die die Unabhängigkeit der Funktion gewährleisten, einschließlich eines Chief Information Security Officers und eines Information Security Officers, also eines (Leitenden) Informationssicherheitsbeauftragten, in allen Geschäftsbereichen.

14.2 Die Mitarbeiter von NTT DATA sind dafür verantwortlich, dass sie im täglichen Geschäftsbetrieb entsprechend den Richtlinien, Verfahren, Standards und Vorgaben zur Informationssicherheit handeln.

15 Richtlinien zur Informationssicherheit

NTT DATA hat eine Reihe von Informationssicherheitsrichtlinien dokumentiert und veröffentlicht, welche die im ISMS dargelegten Anforderungen und Vorgaben unterstützen. Die Richtlinien und zugehörigen Unterlagen werden in regelmäßigen Abständen überprüft.

16 Umgang mit Mobilgeräten

NTT DATA verfügt über eine Richtlinie für Mobilgeräte und Telearbeit. NTT DATA hat Maßnahmen ergriffen, um sicherzustellen, dass mobile Geräte (wie Laptops, Mobiltelefone, Tablets, Geräte mit Fernzugriff und solche im Rahmen von „Bring Your Own Device“-Programmen) sowie deren Inhalte geschützt sind. NTT DATA hat angemessene Anstrengungen unternommen, um sicherzustellen, dass auf allen mobilen Geräten, die Zugang zu Unternehmensnetzwerken bzw. Zugriff auf Informationen, Systeme, Netzwerke und Infrastrukturen von Kunden haben, „Mobile Device Management“-Software („**MDM**“) installiert ist.

17 Personal

17.1 NTT DATA verfügt über eine Personalrichtlinie. Im gesetzlich zulässigen Rahmen untersucht NTT DATA den Hintergrund und die Eignung eigener Mitarbeiter für die Einstellung und den Umgang mit Informationen des

Unternehmens und von Kunden (einschließlich personenbezogener Daten), um ihre entsprechende Tauglichkeit zu gewährleisten. Der Umfang solcher Überprüfungen steht im Verhältnis zu den geschäftlichen Erfordernissen und der Klassifizierung der Informationen, zu denen der jeweilige Mitarbeiter Zugang haben wird.

17.2 NTT DATA verlangt von eigenen Mitarbeitern (einschließlich Auftragnehmern und Zeitarbeitskräften), dass sie sich verpflichten, die Vertraulichkeit der Informationen und personenbezogenen Daten von NTT DATA und Kunden zu wahren.

17.3 Die Mitarbeiter von NTT DATA sind verpflichtet, jährlich eine Schulung zur Informationssicherheit zu absolvieren. Informationssicherheitsrichtlinien und unterstützende Verfahren, Prozesse und Vorgaben werden den Mitarbeitern zur Verfügung gestellt und regelmäßig kommuniziert.

17.4 Außerdem erhalten die Mitarbeiter von NTT DATA relevante Informationen über Entwicklungen, Bedrohungen und bewährte Verfahren über die von NTT DATA betriebenen Kommunikationsplattformen.

18 Die Arbeitsplatzüberwachung

18.1 NTT DATA verfügt über eine Richtlinie zur Arbeitsplatzüberwachung, um Prozesse und Systeme zum Schutz und zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit („VIV“) aller kritischen Informationen (einschließlich personenbezogener Daten) und Informationsverarbeitungsanlagen zu implementieren.

18.2 Zweck der Richtlinie zur Arbeitsplatzüberwachung ist es, zu NTT DATA gehörende Nutzer und andere Personen darüber in Kenntnis zu setzen, wenn eine Überwachung am Arbeitsplatz stattfinden kann.

18.3 NTT DATA kann Nutzer dort, wo sie arbeiten, elektronisch überwachen – sei es an einem von NTT DATA bereitgestellten Arbeitsplatz, bei einem Kunden oder auch zu Hause („Arbeitsplatz“), um Fehlverhalten von Nutzern zu verhindern, die Produktivität zu steuern und die Sicherheit am Arbeitsplatz zu erhöhen („Arbeitsplatzüberwachung“).

19 Zulässige Nutzung

NTT DATA verfügt über eine Angemessenheitsrichtlinie zur ordnungsgemäßen und effektiven Nutzung und zum Schutz von Informationsbeständen, was Computer- und Telekommunikationsanlagen, Produkte, Dienstleistungen, Lösungen und IT-Infrastruktur beinhaltet.

20 Umgang mit und Klassifizierung von Ressourcen

NTT DATA verfügt über eine Richtlinie zum Umgang mit und Klassifizierung von Ressourcen, in der die geeigneten Kontrollmechanismen für den Umgang mit Informationen, basierend auf deren Klassifizierung, beschrieben sind. Informationen und Ressourcen werden entsprechend ihrer Klassifizierung geschützt.

21 Zugangskontrollen

21.1 NTT DATA verfügt über eine Zugangskontrollrichtlinie, unterstützende Verfahren sowie logische und materielle Zugangskontrollmaßnahmen, um sicherzustellen, dass ausschließlich entsprechend befugte Personen (dies basierend auf dem Prinzip der minimalen Rechte bzw. des „Least-Privilege-Prinzips“) Zugang zu Informationen haben.

21.2 Wo es sinnvoll ist, wendet NTT DATA eine dem Branchenstandard entsprechende Verschlüsselung für gespeicherte Daten und Daten während der Übertragung an, um sicherzustellen, dass personenbezogene Daten vor unbefugtem Zugriff oder Offenlegung geschützt sind. Der Zugang zu IT-Anlagen, Anwendungen, Systemen und Datenbanken wird regelmäßig überprüft, um sicherzustellen, dass dieser ausschließlich befugten Personen möglich ist.

21.3 NTT DATA hat angemessene Anstrengungen unternommen, um die Anzahl der privilegierten Nutzer („Administrator“) im Hinblick auf alle Anwendungen, Systeme und Datenbanken streng zu begrenzen. Allgemeine Konten oder die gemeinsame Nutzung von Anmeldeinformationen sind nur dann zulässig, wenn dies ausdrücklich von der Geschäftsleitung oder von Kunden von NTT DATA genehmigt wurde.

22 Richtlinie für Verschlüsselung und Umgang mit Schlüsseln

NTT DATA verfügt über eine Richtlinie für die Verschlüsselung und den Umgang mit Schlüsseln, welche Effizienz bei der Verschlüsselung und dem Umgang mit Schlüsseln innerhalb von NTT DATA unterstützt, um zu verhindern, dass unbefugte Dritte oder in böswilliger Absicht handelnde Parteien ursprüngliche Informationen (während der Übertragung oder Speicherung) wiederherstellen können. Die zugehörigen Standards bieten Anleitungen für den Einsatz kryptografischer Kontrollen zum Schutz von Informationen.

23 Netzwerksicherheit

NTT DATA verfügt über eine Netzwerksicherheitsrichtlinie mit für eigene Netzwerke geltenden Maßnahmen zur Verwaltung, Kontrolle und für den Schutz von in Besitz von NTT DATA befindlichen Informationen.

24 Anwendungssicherheit

NTT DATA verfügt über eine Richtlinie zur Anwendungssicherheit, die vorschreibt, dass alle von NTT DATA eigenentwickelten oder gekauften Softwareanwendungen verwaltet werden und der Zugriff auf diese Anwendungen kontrolliert wird, um im Besitz von NTT DATA befindliche Informationen zu schützen und

sicherzustellen, dass bei der internen Entwicklung von Anwendungen von der ersten Entwurfsphase an bewährte Sicherheitsverfahren angewandt werden.

25 Backups

NTT DATA verfügt über eine Backup-Richtlinie, welche die Anforderungen für die Aufbewahrung und Wiederherstellung von Sicherungskopien solcher sensiblen Informationen von NTT DATA darlegt, die auf Computern und Kommunikationssystemen von NTT DATA erstellt, verarbeitet oder gespeichert werden.

26 Richtlinie für Systemsicherheit

NTT DATA verfügt über eine Richtlinie für Systemsicherheit, die vorsieht, dass im Besitz von NTT DATA befindliche Systeme verwaltet und kontrolliert werden, um Informationen von NTT DATA zu schützen. „Systeme von NTT DATA“ sind alle physischen und virtuellen Systemen (einschließlich Servern, Arbeitsplätzen und Geräten) in Unternehmensniederlassungen und der Cloud von NTT DATA.

27 Physische und ökologische Sicherheit

NTT DATA verfügt über eine Richtlinie für physische Sicherheit. NTT DATA hat im Rahmen dieser Richtlinie für physischr Sicherheit angemessene und geeignete Maßnahmen ergriffen, um unbefugten physischen Zugriff auf unsere Informationen, Anwendungen, Systeme, Datenbanken und die Infrastruktur von NTT DATA sowie deren Beschädigung oder Beeinträchtigung wie folgt zu verhindern:

(a) durch physische Zugangskontrollen

(b) durch Überwachung und Überprüfung des physischen Zugangs

(c) durch Schutz vor Umweltrisiken

(d) durch Sicherung materieller Anlagen

(e) durch sichere Verkabelung

(f) durch entsprechenden Umgang mit materiellen Ressourcen

(g) durch Instandhaltung und Entsorgung von materiellen Ressourcen

(h) durch das „Clean Desk & Screen“-Prinzip

(i) durch Überwachung von Besuchern und

(j) durch Arbeitssicherheitsverfahren

28 Operative Sicherheit

28.1 Die Abteilung Digital & Global Business Services („DGBS“) von NTT DATA ist dafür zuständig, die Anwendungen, Systeme, Datenbanken und Infrastrukturen von NTT DATA in Übereinstimmung mit den Grundsätzen, Standards und Richtlinien für die Informationssicherheit von NTT DATA zu verwalten. DGBS dokumentiert, pflegt und implementiert alle betrieblichen IT-Richtlinien, -Prozesse und -Verfahren, die sich an COBIT- und ITIL-Standards orientieren.

28.2 NTT DATA verfügt über eine Richtlinie und unterstützende Verfahren für sichere Architektur, Design, Betrieb und Wartung zum Umgang mit Änderungen an unseren Geschäftsprozessen, Anwendungen, Systemen, Datenbanken und unserer Infrastruktur. NTT DATA hat verschiedene Kontrollstrukturen eingerichtet, um alle Änderungen basierend auf ihrem Ausmaß und Umfang sowie den strategischen Zielen zu überprüfen und zu genehmigen. Alle Anfragen und deren Ergebnisse werden protokolliert und dokumentiert.

28.3 NTT DATA verfügt über eine Richtlinie zum Umgang mit Schwachstellen unterhält ein Programm zum Umgang mit Bedrohungen und Schwachstellen, das sich auf branchenübliche Tools stützt, um Risiken für Unternehmensinformationen, einschließlich personenbezogener Daten von Mitarbeitern und Kunden, zu erkennen, zu verwalten und zu mindern. Dies beinhaltet Endpoint Detection & Response („EDR“) der nächsten Generation für Antiviren- und Anti-Malware-Tools, das regelmäßige Durchsuchen von Umgebungen, Patching-Protokolle sowie Abhilfe- und Verbesserungsmaßnahmen.

28.4 Der Kapazitätsbedarf wird kontinuierlich überwacht und regelmäßig überprüft. Die Systeme und Netzwerke werden übereinstimmend mit diesen Überprüfungen verwaltet und skaliert.

28.5 Die Systemverfügbarkeit umfasst Architektur, Hochverfügbarkeitsdesign oder Backups auf Grundlage der Risiko- und Verfügbarkeitsanforderungen des jeweiligen Systems. Die Methode zur Aufrechterhaltung der Systemverfügbarkeit oder zur Systemwiederherstellung (einschließlich des Umfangs und der Häufigkeit von Backups) wird auf Grundlage der Geschäftsanforderungen von NTT DATA (einschließlich der Kundenanforderungen) und der Kritikalität der Informationen festgelegt. Backups werden überwacht, um ihre erfolgreiche Fertigstellung zu gewährleisten und auf Probleme, Ausnahmen oder Fehler bei der Sicherung reagieren zu können.

28.6 NTT DATA verfügt über eine Richtlinie zur Überwachung der Informationssicherheit und unternimmt angemessene Anstrengungen, um die Protokollierung der Überprüfung von Anwendungen und Systemen aufrechtzuerhalten. Die Protokolle werden in regelmäßigen Abständen überprüft und sind für Untersuchungen verfügbar. Der Zugang zu den Protokollen ist streng auf entsprechend befugtes Personal beschränkt.

29 Systembeschaffung, -entwicklung und -wartung

29.1 NTT DATA verfügt über eine Richtlinie für sichere Architektur und Entwicklung sowie für unterstützende Standards und Verfahren, um sicherzustellen, dass die Grundsätze des „Security by Design“ im Lebenszyklus der Softwareentwicklung angewandt werden.

29.2 NTT DATA hat angemessene Maßnahmen ergriffen, um zu verhindern, dass „Backdoor“-Programme oder ähnliche Programmierungen erstellt oder gepflegt werden, die den unbefugten Zugriff auf personenbezogene Daten oder Systeme von NTT DATA gestatten oder Behörden den Zugriff darauf ermöglichen.

30 Umgang mit Dritten

NTT DATA verfügt über eine Richtlinie zur Informationssicherheit von Drittanbietern und unterstützende Verfahren, um sicherzustellen, dass Informationsbestände geschützt werden, wenn NTT DATA unabhängige Dienstleister und/oder Auftragsverarbeiter einsetzt. Diese beinhaltet Anforderungen an den Datenschutz, die Sorgfaltspflicht im Bereich der Informationssicherheit und die Durchführung von Risikobewertungen in Zusammenhang mit der Informationssicherheit, um sicherzustellen, dass

(a) die Anforderungen an die Informationssicherheit in den Vereinbarungen mit den Auftragsverarbeitern von NTT DATA klar formuliert und dokumentiert sind.

(b) die Dienstleister und Auftragsverarbeiter von NTT DATA das gleiche Maß an Schutz und Kontrolle bieten wie NTT DATA selbst.

(c) die entsprechenden Dienstleister und Auftragsverarbeiter verpflichtet sind, NTT DATA alle mutmaßlichen oder tatsächlichen Vorfälle im Hinblick auf die Informationssicherheit unverzüglich zu melden.

31 Umgang mit Informationssicherheitsvorfällen

31.1 NTT DATA verfügt über Richtlinien, Prozesse und Verfahren zur Identifizierung, Erkennung, Reaktion, Wiederherstellung und Benachrichtigung der entsprechenden Interessengruppen im Falle eines Informationssicherheitsvorfalls, was Verletzung des Schutzes personenbezogener Daten beinhaltet. Dazu gehören Regelungen für die Durchführung einer Ursachenanalyse und das Umsetzen von Abhilfemaßnahmen.

31.2 NTT DATA hat eine konzernweite Sicherheitsinfrastruktur eingerichtet, der alle Netzwerk- und Computeranlagen proaktiv überwacht und verwaltet. Unterstützt wird dies durch technische Hilfsmittel für die Reaktion auf Informationssicherheitszwischenfälle und entsprechende Wiederherstellung.

32 Aufrechterhaltung des Geschäftsbetriebs

NTT DATA hat Pläne zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung im Notfall erstellt. NTT DATA hat sich für einen mehrstufigen Ansatz entschieden, um die Verfügbarkeit unserer Systeme und Daten zu gewährleisten.

33 Einhaltung von Vorschriften

NTT DATA hat Rollen und Zuständigkeiten für die Ermittlung von Gesetzen und Vorschriften, die sich auf die Geschäftstätigkeit von NTT DATA auswirken, definiert. Die Verantwortung für die Einhaltung von Gesetzen und Vorschriften wird auf Konzern- und Regionalebene festgelegt, um sicherzustellen, dass NTT DATA die weltweit und vor Ort geltenden Anforderungen erfüllt.

Attachment D EU-Standardvertragsklauseln

1 Begriffsbestimmungen

Für die Zwecke dieses **Anhangs D** gelten die folgenden Definitionen:

(a) „**Bestimmungen für die Übertragung vom Datenverantwortlichen an den Auftragsverarbeiter**“ sind die Abschnitte I, II, III und IV (je nach Anwendbarkeit), soweit sie sich auf Modul Zwei (Datenverantwortlicher an Auftragsverarbeiter) der Standardvertragsklauseln für die Übertragung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates beziehen, die durch den Beschluss der EU-Kommission vom 4. Juni 2021 genehmigt wurde.

(b) „**Bestimmungen für die Übertragung vom Auftragsverarbeiter an den Datenverantwortlichen**“ sind die Abschnitte I, II, III und IV (je nach Anwendbarkeit), soweit sie sich auf Modul Vier (Auftragsverarbeiter an Datenverantwortlichen) der Standardvertragsklauseln für die Übertragung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates beziehen, die durch den Beschluss der EU-Kommission vom 4. Juni 2021 genehmigt wurde.

(c) „**Bestimmungen für die Übertragung von Auftragsverarbeiter zu Auftragsverarbeiter**“ sind die Abschnitte I, II, III und IV (je nach Anwendbarkeit), soweit sie sich auf Modul Drei (Auftragsverarbeiter zu Auftragsverarbeiter) der Standardvertragsklauseln für die Übertragung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates beziehen, die durch den Beschluss der EU-Kommission vom 4. Juni 2021 genehmigt wurde.

2 Alle Module

Wenn bei der Erbringung der Leistungen personenbezogene Daten, die den EU-Datenschutzgesetzen unterliegen, von einem Datenexporteur an einen Datenimporteur übertragen werden, haben die Parteien die Bedingungen der europäischen Standardvertragsklauseln (wie in den Abschnitten 3 bis 5 unten näher beschrieben) einzuhalten und es gelten die folgenden Bestimmungen:

(a) Artikel 7 (Andockklausel) der EU-SCC findet keine Anwendung.

(b) Die unter Artikel 11 (Rechtsbehelf) der EU-SCC dargelegte Option findet keine Anwendung.

(c) Alle Streitigkeiten, die sich aus den EU-SCC ergeben, werden von Gerichten der Bundesrepublik Deutschland entschieden.

(d) Anlage I.A zu den EU-SCC (Liste der Parteien): Die Tätigkeiten, die für die Übertragung personenbezogener Daten gemäß den europäischen Standardvertragsklauseln relevant sind, beziehen sich auf die Erbringung der von NTT DATA unter dem Kundenvertrag für Kunden erbrachten Leistungen (siehe Einzelheiten auf der ersten Seite). **Anhang A** enthält den Namen, die Position und die Kontaktdaten des Ansprechpartners. Die Parteien vereinbaren, dass ihre Unterzeichnung des Kundenvertrags, des vorliegende AVV oder eines anderen verbindlichen Dokuments, das den AVV anderweitig einbezieht, als Unterzeichnung der Standardvertragsklauseln gemäß den darin dargelegten Bedingungen gilt.

(e) Der Inhalt von **Anhang B** bildet Anlage I.B zu den europäischen Standardvertragsklauseln (Beschreibung der Übertragung).

(f) Der Hessische Beauftragte für Datenschutz und Informationsfreiheit fungiert als zuständige Aufsichtsbehörde im Sinne von Anlage I.C der europäischen Standardvertragsklauseln (zuständige Aufsichtsbehörde).

3 Bestimmungen für die Übertragung vom Datenverantwortlichen an den Auftragsverarbeiter

Wenn der Kunde der Datenverantwortliche und Exporteur von personenbezogenen Daten und NTT DATA ein Auftragsverarbeiter und Importeur in Bezug auf diese personenbezogenen Daten ist, haben die Parteien die Bedingungen der Bestimmungen für die Übertragung vom Datenverantwortlichen an den Auftragsverarbeiter einzuhalten. Zudem gelten die folgenden Bestimmungen:

(a) Option 2 unter Artikel 9 (allgemeine schriftliche Genehmigung) findet Anwendung und „[Zeitraum angeben]“ wird durch „14 (vierzehn) Tage“ ersetzt.

(b) Für die Zwecke von Artikel 13(a) (Beaufsichtigung) gilt die in Artikel 13(a) dargelegte Option, je nachdem, ob der Datenexporteur (i) in einem EU-Mitgliedstaat niedergelassen ist, (ii) nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den territorialen Anwendungsbereich der Datenschutz-Grundverordnung gemäß Artikel 3(2) der Datenschutz-Grundverordnung fällt und einen Vertreter gemäß Artikel 27(1) der Datenschutz-Grundverordnung bestellt hat oder (iii) nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den territorialen Anwendungsbereich der Datenschutz-Grundverordnung gemäß Artikel 3(2) fällt, ohne jedoch einen Vertreter gemäß Artikel 27(2) der Datenschutz-Grundverordnung bestellen zu müssen.

(c) Es gilt die Option 1 unter Artikel 17 (Anwendbares Recht). Das anwendbare Recht ist das Recht der Bundesrepublik Deutschland.

(d) Der Inhalt von **Attachment C** zu diesem AVV (Technische und organisatorische Maßnahmen) bildet Anlage II der Bestimmungen für die Übertragung vom Datenverantwortlichen an den Auftragsverarbeiter (Technische und organisatorische Maßnahmen einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit).

(e) Die in **Attachment B** zu diesem AVV enthaltene Liste der Unterauftragsverarbeiter bildet Anlage III der Bestimmungen für die Übertragung vom Datenverantwortlichen an den Auftragsverarbeiter (Liste der Unterauftragsverarbeiter).

4 Bestimmungen für die Übertragung von Auftragsverarbeiter zu Auftragsverarbeiter

Wenn NTT DATA der Auftragsverarbeiter und Exporteur von personenbezogenen Daten und der Unterauftragsverarbeiter der Importeur in Bezug auf diese personenbezogenen Daten ist, haben die Parteien die Bedingungen der Bestimmungen für die Übertragung vom Auftragsverarbeiter zu Auftragsverarbeiter einzuhalten. Zudem gelten die folgenden Bestimmungen:

(a) Für die Zwecke von Artikel 8.6(c) und (d) (Sicherheit der Verarbeitung) hat der Unterauftragsverarbeiter Verletzungen des Schutzes personenbezogener Daten in Bezug auf von ihm verarbeitete personenbezogene Daten NTT DATA und nicht direkt dem Kunden zu melden. Gegebenenfalls leitet NTT DATA die Mitteilung an den jeweiligen Kunden weiter.

(b) Für die Zwecke von Artikel 8.9 (Dokumentation und Einhaltung) richtet der Kunde alle Anfragen an NTT DATA.

(c) Option 2 unter Artikel 9 (allgemeine schriftliche Genehmigung) findet Anwendung und „[Zeitraum angeben]“ wird durch „14 Tage“ ersetzt. Die Parteien sind sich ferner darüber einig, dass der Datenverantwortliche die Entscheidungs- und Genehmigungsbefugnis für die Unterverarbeitung für die Zwecke von Artikel 9 (Inanspruchnahme von Unterauftragsverarbeitern) an den Kunden übertragen hat. NTT DATA besitzt die allgemeine Genehmigung des Kunden (im Namen des Datenverantwortlichen) für die Bestellung der in Anhang B zu diesem AVV aufgeführten Unterauftragsverarbeiter. NTT DATA hat das in Artikel 7.3 dieses AVV dargelegte Verfahren zu befolgen, um (nur) den Kunden, nicht jedoch den Datenverantwortlichen über beabsichtigte Änderungen an der entsprechenden Liste zu informieren. Gegebenenfalls informiert der Kunde den Datenverantwortlichen über etwaige Änderungen.

(d) Für die Zwecke von Artikel 10 (Betroffenenrechte) hat der NTT DATA (nur) den Kunden und nicht den Datenverantwortlichen über etwaige, direkt von Betroffenen erhaltene Anfragen zu informieren. Gegebenenfalls leitet der Kunde die Mitteilung an den jeweiligen Datenverantwortlichen weiter. Die Befugnis zur Beantwortung von Anfragen muss NTT DATA vom Kunden im Namen des Datenverantwortlichen erteilt werden.

(e) Für die Zwecke von Artikel 13(a) (Beaufsichtigung) gilt die in Artikel 13(a) dargelegte Option, je nachdem, ob der Datenexporteur (i) in einem EU-Mitgliedstaat niedergelassen ist, (ii) nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den territorialen Anwendungsbereich der Datenschutz-Grundverordnung gemäß Artikel 3(2) der Datenschutz-Grundverordnung fällt und einen Vertreter gemäß Artikel 27(1) der Datenschutz-Grundverordnung bestellt hat oder (iii) nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den territorialen Anwendungsbereich der Datenschutz-Grundverordnung gemäß Artikel 3(2) fällt, ohne jedoch einen Vertreter gemäß Artikel 27(2) der Datenschutz-Grundverordnung bestellen zu müssen.

(f) Für die Zwecke von Artikel 15 (Pflichten des Datenimporteurs im Falle des behördlichen Zugriffs) muss NTT DATA im Falle des Zugriffs durch Behörden (nur) den Kunden und nicht die Betroffenen informieren. NTT DATA verpflichtet sich, den Kunden über Zugriffsersuchen von Behörden gemäß Abschnitt 6 dieses Anhangs D zu informieren. Erhält NTT DATA von den zuständigen Datenschutzbehörden eine Anfrage zu den von ihm aufbewahrten Informationen gemäß den Artikeln 15.1 (a) bis (c) oder 15.2 (b) der Bestimmungen für Übertragungen von Auftragsverarbeiter zu Auftragsverarbeiter, muss NTT DATA den Kunden informieren und diesen an der Beantwortung der Anfrage der zuständigen Datenschutzbehörde beteiligen.

(g) Es gilt die Option 1 unter Artikel 17 (Anwendbares Recht). Das anwendbare Recht ist das Recht der Bundesrepublik Deutschland.

(h) Der Inhalt von **Attachment C** zu diesem AVV (Technische und organisatorische Maßnahmen) bildet Anlage II der Bestimmungen für die Übertragung von Auftragsverarbeiter zu Auftragsverarbeiter (Technische und organisatorische Maßnahmen einschließlich solcher zur Gewährleistung der Datensicherheit).

5 Bestimmungen für die Übertragung vom Auftragsverarbeiter an den Datenverantwortlichen

Ist der NTT DATA der Verarbeiter und Exporteur personenbezogener Daten und der Kunde der Datenverantwortliche und Importeur in Bezug auf diese personenbezogenen Daten, so halten sich die Parteien an die Bestimmungen für die Übertragung vom Auftragsverarbeiter an den Datenverantwortlichen und das anwendbare Recht in Artikel 17 (Anwendbares Recht) ist das Recht der Bundesrepublik Deutschland.

6 Zusätzliche Schutzmaßnahmen zu den europäischen Standardvertragsklauseln

6.1 Soweit die europäischen Standardvertragsklauseln Anwendung finden, sind die folgenden Schutzmaßnahmen zu den EU-SCC einzuhalten, die in diesem Abschnitt 6 von Attachment D dargelegt sind.

6.2 Erfordert die Datenübertragung nach angemessener Auffassung des Kunden Folgenabschätzungen oder Risikobewertungen, so wird NTT DATA ihn auf Wunsch unverzüglich und in zumutbarem Umfang (auf Kosten des Kunden) bei der Durchführung derselben unterstützen und mit ihm zusammenarbeiten, um die Vereinheitlichung der internationalen Datenübertragung zu ermöglichen.

6.3 Die Parteien versichern, dass sie keinen Grund zu der Annahme haben, dass geltende Gesetze, denen sie unterliegen (einschließlich etwaiger Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen zur Genehmigung des Zugriffs durch Behörden), sie daran hindern, ihren unter diesem AVV und dem Datenschutzrecht bestehenden Pflichten nachzukommen. Beide Parteien erklären, dass sie bei der Gewährung dieser Zusicherung insbesondere die folgenden Punkte berücksichtigt haben:

(a) die besonderen Umstände der Verarbeitung, einschließlich des Umfangs und der Regelmäßigkeit der Verarbeitung, die geltendem Recht unterliegt; die genutzten Übertragungskanäle; die Art der betreffenden personenbezogenen Daten; einschlägige praktische Erfahrungen mit früheren Fällen oder das Nichtvorliegen von behördlichen Auskunftsersuchen für die Art von personenbezogenen Daten, die von ihnen verarbeitet werden

(b) die geltenden Gesetze, denen sie unterliegen (einschließlich jener, welche die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugriff solcher Behörden gestatten) sowie die geltenden Beschränkungen und Schutzmaßnahmen sowie solche

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

6.4 Beide Parteien versichern, dass sie sich bei der Durchführung der Bewertung gemäß Abschnitt 6.3 oben nach besten Kräften bemüht haben, relevante Informationen zur Verfügung zu stellen, und erklären sich bereit, weiterhin zusammenzuarbeiten, um die Einhaltung dieses AVV sicherzustellen. Die Parteien vereinbaren, die entsprechende Bewertung zu dokumentieren und erklären sich zudem damit einverstanden, dass solche Bewertungen auch Datenschutzbehörden zur Verfügung gestellt werden können.

6.5 NTT DATA verpflichtet sich, den Kunden unverzüglich zu benachrichtigen, wenn nach Zustimmung zu diesem AVV und während dessen Laufzeit Grund zu der Annahme besteht, dass NTT DATA anwendbaren Gesetzen unterliegt oder unterlegen hat, die nicht mit den Anforderungen gemäß Abschnitt 6.3 übereinstimmen. Dies gilt auch nach einer Änderung der geltenden Rechtsvorschriften, denen NTT DATA unterliegt, oder im Falle von Maßnahmen (wie einer Aufforderung zur Offenlegung), die darauf hindeuten, dass die geltenden Rechtsvorschriften in der Praxis nicht im Einklang mit den Anforderungen gemäß Abschnitt 6.3 angewendet werden. Nach einer entsprechenden Benachrichtigung oder falls der Kunde anderweitig Grund zu der Annahme hat, dass NTT DATA den eigenen Pflichten unter diesem AVV (auch in Bezug auf den jeweiligen Unterauftragsverarbeiter) nicht mehr nachkommen kann, wird der Kunde unverzüglich zusätzliche Maßnahmen festlegen (wie technische oder organisatorische Maßnahmen zur Gewährleistung von Sicherheit und Vertraulichkeit), die er oder NTT DATA (und/oder der betreffende Unterauftragsverarbeiter) auf Kosten des Kunden zu ergreifen hat, um die personenbezogenen Daten vor Eingriffen zu schützen, die über das hinausgehen, was in einer demokratischen Gesellschaft zum Schutz der nationalen Sicherheit, der Verteidigung und der öffentlichen Sicherheit erforderlich ist. Dies hat gegebenenfalls in Absprache mit der zuständigen Datenschutzbehörde zu erfolgen.

6.6 Sofern dies nicht durch geltendes Recht untersagt ist, verpflichtet sich NTT DATA, den Kunden unverzüglich zu benachrichtigen, wenn NTT DATA (oder der jeweilige Unterauftragsverarbeiter, an den eine Übertragung erfolgt):

(a) unter geltendem Recht, dem NTT DATA (oder der jeweilige Unterauftragsverarbeiter) unterliegt, die rechtsverbindliche Aufforderung einer Behörde zur Offenlegung personenbezogener Daten erhält. NTT DATA verpflichtet sich, die Aufforderung und Rechtmäßigkeit des Offenlegungsersuchens unter Berücksichtigung der für NTT DATA (und den jeweiligen Unterauftragsverarbeiter) geltenden Gesetze zu prüfen (und dafür zu sorgen, dass der betreffende Unterauftragsverarbeiter, an den die Übertragung erfolgt, dies ebenfalls tut). Dies betrifft insbesondere die Frage, ob das Ersuchen im Rahmen der der ersuchenden Behörde eingeräumten Befugnisse bleibt. Die Mitteilung an den Kunden enthält Informationen über die angeforderten personenbezogenen Daten, zur anfragenden Behörde und zur Rechtsgrundlage für die Anfrage.

(b) vom direkten Zugriff einer Behörde auf personenbezogene Daten gemäß dem geltenden Recht, dem NTT DATA (oder der betreffende Unterauftragsverarbeiter) unterliegt, Kenntnis erlangt. Die entsprechende Mitteilung enthält alle NTT DATA (und dem betreffenden Unterauftragsverarbeiter) vorliegenden Informationen.

6.7 Ist es NTT DATA (oder dem jeweiligen Unterauftragsverarbeiter, an den die Übertragung erfolgt) untersagt, den Kunden gemäß Abschnitt 6.6 zu benachrichtigen, bemüht sich NTT DATA nach besten Kräften darum, eine Befreiung von dieser Untersagung zu erwirken, um dem Kunden möglichst viele Informationen schnellstmöglich zukommen lassen zu können. Kann NTT DATA keine Befreiung von dem Verbot erwirken und besteht eine zwingende rechtliche Verpflichtung zur Offenlegung eines rechtsverbindlichen Behördenersuchens, so stellt NTT DATA bei der Beantwortung nur so viele Informationen zur Verfügung, wie dies nach geltendem Recht zulässig ist. Sofern es NTT DATA nicht gesetzlich untersagt ist (wenn beispielsweise strafrechtlich vorgesehen ist, die Vertraulichkeit der behördlichen Untersuchung zu wahren), stellt NTT DATA dem Kunden alle Antworten zur Verfügung, die der Behörde übermittelt wurden.

6.8 NTT DATA verpflichtet sich, die eigene (und die des jeweiligen Unterauftragsverarbeiters) rechtliche Beurteilung sowie jedwede Anfechtung des Auskunftsersuchens zu dokumentieren und, soweit unter dem für NTT DATA (oder den jeweiligen Unterauftragsverarbeiter) geltenden Recht zulässig, dem Kunden die entsprechenden

Unterlagen zur Verfügung zu stellen. Auch stellt NTT DATA sie der zuständigen Datenschutzbehörde auf Anfrage zur Verfügung.

6.9 NTT DATA bemüht sich in angemessener Weise, bei der Beantwortung eines Auskunftsersuchens auf Grundlage einer angemessenen Auslegung des Ersuchens nur das zulässige Mindestmaß an Informationen bereitzustellen (bzw. dafür zu sorgen, dass der betreffende Unterauftragsverarbeiter, an den die Übertragung erfolgt, dies tut).

6.10 Soweit dies nach den geltenden Gesetzen, denen NTT DATA und der betreffende Unterauftragsverarbeiter unterliegen, zulässig ist, erklärt sich NTT DATA dazu bereit, Transparenzberichte oder Zusammenfassungen über an NTT DATA gerichtete Anträge von Behörden auf Datenzugriff und die Art der erteilten Antwort zu veröffentlichen, soweit eine solche Bekanntgabe nach geltendem Recht zulässig ist.

6.11 NTT DATA verpflichtet sich, die unter Abschnitt 6.10 aufgeführten Informationen für die Dauer der Verarbeitung aufzubewahren und der zuständigen Datenschutzbehörde auf Anfrage zur Verfügung zu stellen.

6.12 NTT DATA hält sich bei der Offenlegung personenbezogener Daten an die eigene Richtlinie für behördliche Datenauskunftsersuchen.

6.13 NTT DATA informiert die Betroffenen in einem transparenten und leicht zugänglichen Format auf der eigenen Webseite über einen Ansprechpartner, der für die Bearbeitung von Beschwerden oder Anträgen zuständig ist. Außerdem bearbeitet NTT DATA Beschwerden über Behördenersuchen unverzüglich (und sorgt dafür, dass Unterauftragsverarbeiter dies ebenfalls tun).

Attachment E Besondere Bestimmungen zur Zuständigkeit bei grenzüberschreitenden Übertragungen

1 Allgemeines

1.3 Im Interesse der Erfüllung ihrer datenschutzrechtlichen Verpflichtungen vereinbaren die Parteien, dass dieser Allgemeine Teil von Anhang E gilt, wenn

(a) personenbezogene Daten von einem Datenexporteur an einen Datenimporteur übertragen werden und

(b) die Rechtsordnung, aus der die personenbezogenen Daten stammen, die EU-SCC als Angemessenheitsregelung anerkennt, falls diese Rechtsordnung keine andere rechtlich hinlängliche Übertragungsregelung unter dem Datenschutzrecht festgelegt hat oder eine entsprechende beschränkte Übertragung nicht anderweitig durch länderspezifische Rechtsordnungen gemäß diesem Anhang E geregelt ist.

1.2 Für die Zwecke dieses Allgemeinen Teils von Anhang E werden die EU-SCC wie folgt geändert:

(a) Die EU-SCC gelten als in dem Umfang geändert, der erforderlich sind, um sie anzuwenden für:

(i) Übertragungen durch den Datenexporteur an den Datenimporteur, soweit das geltende Datenschutzrecht auf die Verarbeitung durch den Datenexporteur bei dieser beschränkten Übertragung Anwendung findet und um

(ii) für Übertragungen angemessene Sicherheitsmaßnahmen gemäß geltendem Datenschutzrecht zu bieten.

(b) Verweise in den EU-SCC auf die Verordnung (EU) 2016/679 oder „diese Verordnung“ sind als Verweise auf das geltende Datenschutzrecht zu verstehen.

(c) Verweise in den EU-SCC auf bestimmte Artikel der Verordnung (EU) 2016/679 werden gelöscht und gegebenenfalls durch die entsprechenden Artikel oder Abschnitte der geltenden Datenschutzgesetze ersetzt.

(d) Verweise auf die Verordnung (EU) 2018/1725 werden gestrichen.

(e) Verweise in den EU-SCC auf „einen Mitgliedstaat“ oder „EU-Mitgliedstaaten“ sind als Verweise auf das Land, in dem der Datenexporteur niedergelassen ist, zu verstehen. Eine Ausnahme davon begründet Artikel 11(c) Ziffer i, wo der Verweis auf „Mitgliedstaat“ durch „Land“ ersetzt wird und

(f) die Fußnoten zu den EU-SCC werden entfernt.

1.4 Um jedweden Zweifel auszuschließen: Die Parteien beabsichtigen nicht, Betroffenen unter den EU-SCC Rechte als Drittbegünstigte zu gewähren, wenn diese Betroffenen nicht anderweitig unter dem Datenschutzrecht in den Genuss solcher Rechte kämen. Der durch die EU-SCC gebotene höhere Sicherheitsgrad gilt nur in Ländern außerhalb Europas, in denen ein solcher höherer Sicherheitsgrad für den Schutz personenbezogener Daten, die gemäß dem Datenschutzrecht übertragen werden, erforderlich ist.

2 China

2.1 Wenn eine eingeschränkte Übermittlung personenbezogener Daten erforderlich ist, darf der Datenimporteur personenbezogene Daten in einer ausländischen Gerichtsbarkeit nur über einen der folgenden, nach dem chinesischen Datenschutzgesetz verfügbaren Mechanismen für die grenzüberschreitende Übermittlung rechtmäßig empfangen und verarbeiten:

(a) eine obligatorische Bewertung der Datensicherheit durch die chinesische Cyberspace-Verwaltung oder

(b) die Zertifizierung des Schutzes personenbezogener Daten durch eine professionelle Institution, oder

(c) die Unterzeichnung des Standardvertrags.

2.2 Die Parteien müssen den Mechanismus, der es dem Datenimporteur ermöglicht, die personenbezogenen Daten in einem anderen Land zu verarbeiten, diesem AVV beifügen.

2.3 Wenn eine Übermittlung personenbezogener Daten zwischen dem Datenimporteur und dem Datenexporteur den Abschluss des Standardvertrags erfordert, werden die Parteien den Standardvertrag abschließen und alle anderen Maßnahmen ergreifen, die für die Rechtmäßigkeit der Übermittlung erforderlich sind, einschließlich der Einreichung des Standardvertrags bei den zuständigen Behörden oder der Durchführung aller erforderlichen zusätzlichen Maßnahmen.

2.4 Der Datenimporteur wird keine personenbezogenen Daten in ein anderes Land übermitteln, es sei denn, die Übermittlung entspricht den gesetzlichen Bestimmungen zum Datenschutz.

2.5 Der Datenexporteur muss für die Übermittlung personenbezogener Daten, die von dem in China ansässigen Datenexporteur erfasst und generiert werden, alle erforderlichen behördlichen Anmeldungen, Genehmigungen, Zustimmungen und Bescheinigungen von den zuständigen Behörden der VR China einholen und aufrechterhalten.

3 Schweiz

3.1 Wenn eine beschränkte Übertragung personenbezogener Daten von einem Datenexporteur an einen Datenimporteur der DSGVO und dem DSG unterliegt, gelten die folgenden zusätzlichen Bestimmungen zu den EU-

SCC, damit diese geeignet sind, ein angemessenes Schutzniveau für diese Übertragung gemäß Artikel 6 Absatz 2 Ziffer (a) des DSG zu gewährleisten:

(a) „EDÖB“ bezeichnet den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten.

(b) „Überarbeitetes DSG“ bezeichnet die überarbeitete Fassung des DSG vom 25. September 2020, die am 1. September 2023 in Kraft getreten ist.

(c) Der Begriff „EU-Mitgliedstaat“ darf nicht so ausgelegt werden, dass Betroffene in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) gemäß Artikel 18(c) geltend zu machen.

(d) Die EU-SCC schützen bis zum Inkrafttreten des überarbeiteten DSG auch die Daten von juristischen Personen.

3.2 Der EDÖB fungiert als „zuständige Aufsichtsbehörde“, sofern die betreffende beschränkte Übertragung durch das DSG geregelt ist.

3.3 Die Parteien werden auch den in Abschnitt 6 von Anhang D aufgeführten zusätzlichen Sicherheitsbestimmungen der EU-SCC entsprechen.

4 Vereinigtes Königreich

4.1 Wenn eine beschränkte Übertragung personenbezogener Daten von einem Datenexporteur an einen Datenimporteur erfolgt, der dem Datenschutzrecht des Vereinigten Königreichs unterliegt, gilt dieser Abschnitt 3 von Anhang E. Die Parteien verpflichten sich zudem, den in **Abschnitt 6 von Anhang D** aufgeführten zusätzlichen Sicherheitsmaßnahmen der EU-SCC zu entsprechen.

TEIL 1 – TABELLEN

Tabelle 1: Parteien und Unterschriften

Startdatum	Datum des Inkrafttretens des AVV	
Die Parteien	Exporteur (derjenige, der die beschränkte Übertragung sendet)	Importeur (derjenige, der die beschränkte Übertragung erhält)
Angaben zu den Parteien	NTT DATA oder der Kunde, je nach Sachlage. Siehe Anhang B	NTT DATA oder der Kunde, je nach Sachlage. Siehe **Attachment B**
Erster Ansprechpartner	Siehe **Anhang A**	
Unterschriften (falls für die Zwecke von Abschnitt 2 erforderlich)	nicht zutreffend	nicht zutreffend

Tabelle 2: Ausgewählte Standardvertragsklauseln, Module und ausgewählte Bestimmungen

Nachtrag zu den EU SCCs	Die Fassung der genehmigten europäischen Standardvertragsklauseln, denen dieser Nachtrag beigefügt wird, ist in Anhang E aufgeführt, einschließlich der Informationen in der Anlage.

Tabelle 3: Informationen in der Anlage

„**Informationen in der Anlage“ bezeichnet jene Angaben, die für die ausgewählten Module gemäß der Anlage zu den europäischen Standardvertragsklauseln vorzulegen sind (**mit Ausnahme **der Parteien) und die für den vorliegenden AVV enthalten sind in:**

Anlage 1A: Liste der Parteien: Inhalt von Anlage I.A zu **Attachment D**
Anlage 1B: Beschreibung der Übertragung: siehe **Attachment B**
Anlage II: Technische und organisatorische Maßnahmen, einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Daten: siehe **Attachment C**
Anlage III: Liste der Unterauftragsverarbeiter (nur Module 2 und 3): siehe **Attachment B**

Tabelle 4: Beendigung dieses Nachtrags bei Änderungen des genehmigten Nachtrags

Beendigung dieses Nachtrags bei Änderungen des genehmigten Nachtrags	Folgende Parteien können diesen Nachtrag wie in Abschnitt 19 dargelegt beenden: ☒ Importeur ☒ Exporteur ☐ keine der Parteien

TEIL 2 – ZWINGENDE BESTIMMUNGEN

Zwingende Bestimmungen des genehmigten Nachtrags, also die vom ICO herausgegebene und dem Parlament gemäß s119A dem Data Protection Act 2018 am 2. Februar 2022 vorgelegte „Vorlage Nachtrag B.1.0“ in der gemäß Abschnitt 18 dieser Zwingenden Bestimmungen überarbeiteten Fassung.

Attachment F Bestimmungen des California Consumer Privacy Act

Diese Bestimmungen des CCPA gelten nur, wenn NTT DATA personenbezogene Daten von in Kalifornien ansässigen Personen verarbeitet.

1 Begriffsbestimmungen

1.1 Es gelten die folgenden Definitionen:

(a) „**CCPA**“ ist der California Consumer Privacy Act von 2018 in seiner jeweils aktuellen Fassung (Cal. Civ. Code §§ 1798.100 bis 1798.199) und alle damit zusammenhängenden Vorschriften oder Anweisungen des kalifornischen Generalstaatsanwalts.

(b) „**Vertraglich vereinbarte Geschäftszwecke**“ sind die Zwecke der Verarbeitung personenbezogener Daten, wie sie in **0** dargelegt sind.

(c) „**Personenbezogene Daten**“ sind Informationen, die einen bestimmten Verbraucher oder Haushalt kennzeichnen, sich auf ihn beziehen, ihn beschreiben und vernünftigerweise mit ihm in Verbindung oder Zusammenhang gebracht werden könnten.

1.2 Die folgenden Begriffe, die in diesem Attachment F verwendet, jedoch nicht erklärt werden (wie beispielsweise „Verbrauchersammeldaten“, „geschäftliche Zwecke“, „kommerzielle Zwecke“, „Verbraucher“, „anonymisieren“, „Verarbeitung“, „pseudonymisieren“, „Verkauf“ und „verifizierbarer Verbraucherantrag“), haben dieselbe Bedeutung, wie sie in den §§ 1798.14 des CCPA dargelegt ist.

2 Pflichten von NTT DATA unter dem CCPA

2.1 NTT DATA verarbeitet personenbezogene Daten nur für die vertraglich vereinbarten Geschäftszwecke, für die der Kunde den Zugriff auf personenbezogenen Daten ermöglicht oder gestattet, was auch eine Ausnahmeregelung für den „Verkauf“ beinhaltet.

2.2 NTT DATA wird personenbezogene Daten nicht für eigene kommerzielle Zwecke oder in einer Weise verarbeiten, verkaufen oder anderweitig zur Verfügung stellen, die nicht mit dem CCPA übereinstimmt. Falls ein Gesetz NTT DATA dazu verpflichtet, personenbezogene Daten für einen Zweck weiterzugeben, der nicht mit den vertraglich vereinbarten Geschäftszwecken zusammenhängt, hat NTT DATA zunächst den Kunden über die gesetzliche Auflage zu informieren und diesem die Möglichkeit zu geben, dagegen Einspruch zu erheben oder die Auflage anzufechten, falls eine solche Benachrichtigung nicht gesetzlich untersagt ist.

2.3 NTT DATA beschränkt die Verarbeitung personenbezogener Daten auf Tätigkeiten, die zum Erreichen der vertraglich vereinbarten Geschäftszwecke oder eines anderen passenden Geschäftszwecks notwendig und angemessen sind.

2.4 NTT DATA hat unverzüglich jeder Aufforderung oder Anweisung der vom Kunden ermächtigten Personen nachzukommen, laut der NTT DATA die personenbezogenen Daten bereitstellen, ändern, übertragen oder löschen oder ihre unbefugte Verarbeitung beenden, eindämmen oder korrigieren soll.

2.5 Falls die vertraglich vereinbarten Geschäftszwecke die Erhebung personenbezogener Daten von Verbrauchern im Auftrag des Kunden erfordern, hat der Kunde NTT DATA einen CCPA-konformen Hinweis zukommen zu lassen, in dem die vom Kunden ausdrücklich vorab schriftlich genehmigten Verwendungszwecke und Verfahren zur Erhebung dargelegt werden. NTT DATA darf den Hinweis ohne die vorherige schriftliche Zustimmung des Kunden keinesfalls verändern oder umformulieren.

2.6 Sofern der CCPA es zulässt, kann NTT DATA personenbezogene Daten zusammenfassen oder anonymisieren, sodass sie nicht mehr der Definition für personenbezogene Daten entsprechen. Derart zusammengefasste oder anonymisierte Daten kann NTT DATA für eigene Forschungs- und Entwicklungszwecke verwenden.

3 Unterstützung bei der Erfüllung der durch den CCPA begründeten Verpflichtungen des Kunden

3.1 NTT DATA kooperiert in angemessener Weise mit dem Kunden und unterstützt diesen bei der Erfüllung seiner Verpflichtungen zur Übereinstimmung mit dem CCPA und bei der Beantwortung von Anfragen, die mit dem CCPA in Zusammenhang stehen. Dies beinhaltet die Beantwortung verifizierbarer Verbraucheranfragen. Dabei sind die Art der Verarbeitung durch NTT DATA sowie die NTT DATA zur Verfügung stehenden Informationen zu berücksichtigen.

3.2 NTT DATA ist verpflichtet, den Kunden unverzüglich zu benachrichtigen, wenn NTT DATA Beschwerden, Hinweise oder Mitteilungen erhält, die sich direkt oder indirekt auf die Einhaltung des CCPA durch eine der Parteien beziehen. Insbesondere muss NTT DATA den Kunden innerhalb von fünf (5) Werktagen informieren, wenn NTT DATA eine verifizierbare Verbraucheranfrage gemäß dem CCPA erhält.

4 Vergabe von Unteraufträgen

4.1 NTT DATA kann zur Erfüllung der vertraglich vereinbarten Geschäftszwecke Unterauftragnehmer einsetzen. Jeder Unterauftragnehmer muss als Dienstleister im Sinne des CCPA gelten. NTT DATA darf dem Unterauftragnehmer gegenüber keine Angaben machen, die der CCPA als Verkauf behandeln würde.

4.2 NTT DATA übergibt dem Kunden für jeden eingesetzten Unterauftragnehmer eine aktuelle Liste, aus der Folgendes hervorgeht:

(a) Name, Anschrift und Kontaktdaten des Unterauftragnehmers

(b) die Art der vom Unterauftragnehmer erbrachten Dienstleistungen

(c) die Kategorien personenbezogener Daten, die in den vorangegangenen zwölf (12) Monaten an den Unterauftragnehmer weitergegeben wurden

4.3 NTT DATA haftet gegenüber dem Kunden in vollem Umfang für die Erfüllung der Vertragspflichten des Unterauftragnehmers. NTT DATA prüft in regelmäßigen Abständen, ob die Unterauftragnehmer ihren Verpflichtungen in Bezug auf personenbezogene Daten in Übereinstimmung mit unseren Richtlinien nachkommen und stellt dem Kunden auf Anfrage die Prüfungsergebnisse zur Verfügung.

5 Zusicherungen in Zusammenhang mit dem CCPA

Beide Parteien werden bei der Verarbeitung personenbezogener Daten alle unter dem CCPA geltenden Auflagen erfüllen.