STANDARDVERTRAGSKLAUSELN
Modul Drei: Übermittlung von Verantwortlichen an Auftragsverarbeiter

ABSCHNITT I

Klausel 1 - Zweck und Anwendungsbereich

(a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

b) Die Parteien:

(i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und

(ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“), haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) einverstanden erklärt.

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

(d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2 - Wirkung und Unabänderbarkeit der Klauseln

(a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

(b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

Klausel 3 - Drittbegünstigte

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

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

ii) Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b

iii) Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e

iv) Klausel 12 — Modul eins: Klausel 12 Buchstaben a und d Module zwei und drei: Klausel 12 Buchstaben a, d und f

v) Klausel 13

vi) Klausel 15.1 Buchstaben c, d und e

vii) Klausel 16 Buchstabe e

viii) Klausel 18 — Module eins, zwei und drei Klausel 18 Buchstaben a und b Modul vier: Klausel 18

(b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt.

Klausel 4 – Auslegung

(a) Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.

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

(c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5 – Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

Klausel 6 – Beschreibung der Datenübermittlung(en)

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

Klausel 7 – Kopplungsklausel

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

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

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

ABSCHNITT II — PFLICHTEN DER PARTEIEN

Klausel 8 – Datenschutzgarantien

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

8.1 Weisungen

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

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

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

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

8.2 Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

8.3 Transparenz

Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anhang II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen. Diese Klausel gilt unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.4 Richtigkeit

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

8.5 Dauer der Verarbeitung und Löschung oder Rückgabe der Daten

Die Daten werden vom Datenimporteur nur für die in Anhang I.B angegebene Dauer verarbeitet. Nach Wahl des Datenexporteurs löscht der Datenimporteur nach Beendigung der Erbringung der Datenverarbeitungsdienste alle im Auftrag des Datenexporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenexporteur, dass dies erfolgt ist, oder gibt dem Datenexporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist. Dies gilt unbeschadet von Klausel 14, insbesondere der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe e, den Datenexporteur während der Vertragslaufzeit zu benachrichtigen, wenn er Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten oder gelten werden, die nicht mit den Anforderungen in Klausel 14 Buchstabe a im Einklang stehen.

8.6 Sicherheit der Verarbeitung

(a) Der Datenimporteur und, während der Datenübermittlung, auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu diesen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der

Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann. Im Falle einer Pseudonymisierung verbleiben die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, soweit möglich, unter der ausschließlichen Kontrolle des Datenexporteurs. Zur Erfüllung seinen Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

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

(c) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Datenimporteur dem Datenexporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde. Diese Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen. Wenn und soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

(d) Unter Berücksichtigung der Art der Verarbeitung und der dem Datenimporteur zur Verfügung stehenden Informationen arbeitet der Datenimporteur mit dem Datenexporteur zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen, insbesondere die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen.

8.7 Sensible Daten

Soweit die Übermittlung personenbezogene Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Datenimporteur die in Anhang I.B beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8 Weiterübermittlungen

Der Datenimporteur gibt die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs an Dritte weiter. Die Daten dürfen zudem nur an Dritte weitergegeben werden, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union ansässig sind (im Folgenden „Weiterübermittlung"), sofern der Dritte im Rahmen des betreffenden Moduls an diese Klauseln gebunden ist oder sich mit der Bindung daran einverstanden erklärt oder falls

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

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

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

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

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

a.9 Dokumentation und Einhaltung der Klauseln

(a) Der Datenimporteur bearbeitet Anfragen des Datenexporteurs oder des Verantwortlichen, die sich auf die Verarbeitung gemäß diesen Klauseln beziehen, umgehend und in angemessener Weise.

(b) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten.

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

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

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

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

(g) Die Parteien stellen der zuständigen Aufsichtsbehörde die unter den Buchstaben b und c genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

Klausel 9 – Einsatz von Unterauftragsverarbeitern

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

(b) Beauftragt der Datenimporteur einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Datenexporteurs), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die den Datenimporteur gemäß diesen Klauseln binden, einschließlich im Hinblick auf Rechte als Drittbegünstigte für betroffene Personen. Die Parteien erklären sich damit einverstanden, dass der Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 8.8 nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.

(c) Der Datenimporteur stellt dem Datenexporteur auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

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

(e) Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein — das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Klausel 10 – Rechte betroffener Personen

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

(b) Der Datenimporteur unterstützt den Datenexporteur bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung

(EU) 2016/679 zu beantworten. Zu diesem Zweck legen die Parteien in Anhang II unter Berücksichtigung der Art der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen, durch die Unterstützung geleistet wird, sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

(c) Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Datenimporteur die Weisungen des Datenexporteurs.

Klausel 11 – Rechtsbehelf

(a) Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

(b) Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.

(c) Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Datenimporteur die Entscheidung der betroffenen Person an,

(i) eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 13 einzureichen,

(ii) den Streitfall an die zuständigen Gerichte im Sinne der Klausel 18 zu verweisen.

(d) Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80 Absatz 1 der Verordnung (EU) 2016/679 vertreten werden kann.

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

(f) Der Datenimporteur erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

Klausel 12 – Haftung

(a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

(b) Der Datenimporteur haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenimporteur oder sein Unterauftragsverarbeiter der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt.

(c) Ungeachtet von Buchstabe b haftet der Datenimporteur gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenexporteur oder der Datenimporteur (oder dessen

Unterauftragsverarbeiter) der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs und, sofern der Datenexporteur ein im Auftrag eines Verantwortlichen handelnder Auftragsverarbeiter ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.

(d) Die Parteien erklären sich damit einverstanden, dass der Datenexporteur, der nach Buchstabe c für durch den Datenimporteur (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Datenimporteur den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Datenimporteurs für den Schaden entspricht.

(e) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

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

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

Klausel 13 – Aufsicht

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

(b) Der Datenimporteur erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

ABSCHNITT III – LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 14 –Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

(a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen

Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

(b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:

(i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

(ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien,

(iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

(c) Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe b nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.

(d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe b zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

(e) Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe a im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe a im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht

(f) Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn von der dafür zuständigen

Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben d und e Anwendung.

Klausel 15 – Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

15.1 Benachrichtigung

(a) Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen,

(i) wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder

(ii) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.

(b) Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.

(c) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).

(d) Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben a bis c während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

(e) Die Buchstaben a bis c gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe e und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

15.2 Überprüfung der Rechtmäßigkeit und Datenminimierung

(a) Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 14 Buchstabe e.

(b) Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.

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

ABSCHNITT IV – SCHLUSSBESTIMMUNGEN

Klausel 16 – Verstöße gegen die Klauseln und Beendigung des Vertrags

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

(b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14 Buchstabe f.

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

(i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe b ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,

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

(iii) der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der

Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

(d) Personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

(e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 17 – Anwendbares Recht

Diese Klauseln unterliegen dem Recht des EU-Mitgliedstaats, in dem der Datenexporteur niedergelassen ist. Wenn dieses Recht keine Rechte als Drittbegünstigte zulässt, unterliegen diese Klauseln dem Recht eines anderen EU-Mitgliedstaats, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von Deutschland ist.

Klausel 18 – Gerichtsstand und Zuständigkeit

(a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.

(b) Die Parteien vereinbaren, dass dies die Gerichte von Deutschland sind.

(c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.

(d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

ANLAGE

ANHANG I

A. LISTE DER PARTEIEN

Datenexporteur (e)	
Name	
Anschrift	
Name, Funktion und Kontaktdaten der Kontaktperson:	
Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind:	
Datenschutzbeauftragter	
Rolle	Verantwortlicher

_____ _____

Datum Unterschrift

Datenimporteur (e)	
Name	NinjaRMM, LLC
Anschrift	500 N. Brand, Glendale CA 91203
Name, Funktion und Kontaktdaten der Kontaktperson:	Lewis Huynh privacy@ninjarmm.com
Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind:	CSO
Datenschutzbeauftragten	Lewis Huynh
Rolle	Auftragsverarbeiter

20.10.2021

DocuSigned by:
Lewis Huynh
1F5B9694FB02487...

Datum Unterschrift

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden	Betroffene Personen sind die Personen, deren Daten vom Verantwortlichen verarbeitet werden, und können Endnutzer oder Mitarbeiter und Angestellte des für die Verarbeitung Verantwortlichen sein.
Kategorien der übermittelten personenbezogenen Daten	Bei den verarbeiteten Daten handelt es sich um die personenbezogenen Daten, die der für die Verarbeitung Verantwortliche dem Auftragsverarbeiter im Zusammenhang mit den vom Auftragsverarbeiter erbrachten Diensten zur Verfügung stellt, einschließlich, aber nicht beschränkt auf Vorname, Nachname, Adresse, E-Mail-Adresse, Telefonnummer, Standortdaten, Kontaktinformationen und Geräteinformationen.
Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen	n/a
Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden)	Kontinuierlich
Art der Verarbeitung	Bei der Art der Verarbeitung handelt es sich um eine Verarbeitung zum Zwecke der Erfüllung seiner Dienstleistung für den Verantwortlichen.
Zweck(e) der Datenübermittlung und Weiterverarbeitung	Der Auftragsverarbeiter kann Daten gemäß den in der Vereinbarung festgelegten Zwecken verarbeiten, und zwar im Allgemeinen: zur Erbringung seiner Dienstleistungen für den für die Verarbeitung Verantwortlichen; zur Aufdeckung,

	Verhinderung und Eindämmung von Betrug; zum Anbieten, Aufrechterhalten und Verbessern der von ihm oder seinen verbundenen Unternehmen angebotenen Dienstleistungen sowie zum Verbessern oder Weiterentwickeln seines Dienstleistungsangebots oder des Angebots seiner verbundenen Unternehmen im Auftrag anderer Kunden, wobei die Daten nur in aggregierter Form verarbeitet werden.
Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer	Die Dauer der Verarbeitung ist auf die Dauer begrenzt, die für die Erfüllung seiner Verpflichtungen aus dem Vertrag erforderlich ist, es sei denn, es besteht eine gesetzliche Verpflichtung zur Speicherung. Die Verpflichtungen des Auftragsverarbeiters in Bezug auf die Datenverarbeitung bestehen in jedem Fall fort, bis die Daten ordnungsgemäß gelöscht oder auf Ersuchen des für die Verarbeitung Verantwortlichen zurückgegeben worden sind.
Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.	Kontinuierlich

ANHANG II

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

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

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • Für alle Daten, die zwischen dem NinjaRMM Agent und der NinjaRMM Plattform übertragen werden, werden FIPS 140-2 konforme kryptographische Module mittels TLS Verschlüsselung eingesetzt. o Im Einzelnen handelt es sich bei allen Chiffren um Perfect-Forward Secrecy (PFS) mit der folgenden Kryptographie: ▪ ECDHE RSA with AES128-GCM and SHA256 ▪ ECDHE RSA with AES128-CBC and SHA256 ▪ ECDHE RSA with AES128-CBC and SHA ▪ ECDHE RSA with AES256-GCM and SHA384 ▪ ECDHE RSA with AES256-CBC and SHA384 ▪ ECDHE RSA with AES256-CBC and SHA Für alle Daten im Ruhezustand, die im NinjaRMM Plattform Backend gespeichert sind, werden FIPS 140-2 konforme kryptographische Module für die

	Verschlüsselung im Ruhezustand verwendet. Die Daten werden mit einer Mindeststufe von AES256 verschlüsselt, wobei je nach Bedarf auch eine stärkere Kryptographie verwendet werden kann.
Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response • Using Amazon Web Services for Disaster

	Recovery, AWS October 2011 • Disaster Recovery with Amazon Web Services: A Technical Guide, Accenture June 2016 • Architecting for the Cloud: AWS Best Practices, AWS October 2018 • AWS Well-Architected Framework, AWS July 2019 • Affordable Enterprise-Grade Disaster Recovery Using AWS, CloudEndure/AWS 2019 • Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldekanäle, Notfallpläne
Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	• Using Amazon Web Services for Disaster Recovery, AWS October 2011 • Disaster Recovery with Amazon Web Services: A Technical Guide, Accenture June 2016 • Architecting for the Cloud: AWS Best Practices, AWS October 2018 • AWS Well-Architected Framework, AWS July 2019 • Affordable Enterprise-Grade Disaster Recovery Using AWS, CloudEndure/AWS 2019 • Backup (online/offline; on-site/off-site), Rapid recoverability
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	• NIST SP # 800-55, Performance Measurement Guide for Information Security • NIST SP # 800-115, Technical Guide to Information Security Testing and Assessment • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities • NIST SP # 800-192, Verification and Test Methods for Access Control Policies/Models • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • Data protection management, Incident

	response management, data protection-friendly default settings, order control (clear contract design, formalized order management, strict selection of service providers, duty of prior conviction, follow-up checks)
Maßnahmen zur Identifizierung und Autorisierung der Nutzer	• NIST SP # 800-178, A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications • NIST SP # 800-192, Verification and Test Methods for Access Control Policies/Models • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-92, Guide to Computer Security Log Management • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, Einsatz von Verschlüsselungsmethoden, Datenträgerverwaltung, Begrenzung der Anzahl von Administratoren, sichere Aufbewahrung von Datenträgern
Maßnahmen zum Schutz der Daten während der Übermittlung	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • Für alle Daten, die zwischen dem NinjaRMM Agent und der NinjaRMM Plattform übertragen werden, werden FIPS 140-2 konforme kryptographische Module mittels TLS Verschlüsselung eingesetzt. ○ Im Einzelnen handelt es sich bei allen Chiffren um Perfect-Forward Secrecy

	(PFS) mit der folgenden Kryptographie: ▪ ECDHE RSA with AES128-GCM and SHA256 ▪ ECDHE RSA with AES128-CBC and SHA256 ▪ ECDHE RSA with AES128-CBC and SHA ▪ ECDHE RSA with AES256-GCM and SHA384 ▪ ECDHE RSA with AES256-CBC and SHA384 ▪ ECDHE RSA with AES256-CBC and SHA
Maßnahmen zum Schutz der Daten während der Speicherung	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • Für alle Daten im Ruhezustand, die im NinjaRMM-Plattform-Backend gespeichert sind, werden FIPS 140-2-konforme kryptographische Module für die Verschlüsselung im Ruhezustand verwendet. Die Daten werden mit einer Mindeststufe von AES256 verschlüsselt, wobei je nach Bedarf auch eine höhere Verschlüsselungsstärke verwendet werden kann. • Mehrmandantenfähigkeit, Sandboxing, Physikalisch getrennte Speicherung auf separaten Ordnerstrukturen, Mandantentrennung, Autorisierungskonzepte, Datenbankrechte
Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten	• NIST SP # 800-30, Guide for Conducting Risk Assessments • NIST SP # 800-39, Managing Information

verarbeitet werden	Security Risk • NIST SP # 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations Darüber hinaus kontrolliert NinjaRMM den physischen Zugriff durch: - Bereitstellung von Anwendungen und Backend-Systemen bei sicheren, geprüften und angesehenen Cloud-Service-Anbietern. - keine physischen Server, Speicher oder Netzwerke in Verbindung mit der NinjaRMM-Anwendung und den Diensten besitzt und einsetzt. - Beibehaltung physischer Büros für die Mitarbeiter der Geschäftsleitung, der Finanzabteilung, des Marketings, des Vertriebs, der Kundenbetreuung und des Supports. - Beschränkung des Zugangs zu den NinjaRMM-Büros auf Angestellte, Auftragnehmer und eingeladene Gäste (ungebetene Gäste werden gebeten, das Gebäude zu verlassen oder einen späteren Besuch zu vereinbaren, falls ein solcher erforderlich ist). - Professionelle Verwaltung der NinjaRMM-Büros durch geprüfte Vermieter und Hausverwaltungsfirmen. - Die Verwendung von Schlüsseln, Schlüsselkarten, elektronischen Schlüsselanhängern oder Token für mobile Geräte für den Zugang zu einem NinjaRMM-Büro zu verlangen - Festlegung eines Büroleiters für jedes NinjaRMM-Büro, wobei der jeweilige NinjaRMM-Büroleiter alle Schlüssel, Schlüsselkarten und Anhänger inventarisiert, ausgibt und verwaltet und alle Zuweisungen von Schlüsseln und Anhängern in einem offiziellen Protokoll festhält. - Anforderung, dass verlorene oder gestohlene Schlüssel, Schlüsselkarten oder Anhänger

	unverzüglich dem NinjaRMM-Büroleiter gemeldet werden müssen, woraufhin die Schlüssel, Schlüsselkarten oder Anhänger gesperrt werden. - Es wird verlangt, dass eingeladene Besucher von NinjaRMM sich beim NinjaRMM-Büroleiter anmelden müssen, der ein offizielles Besucherprotokoll führt, in dem der Name des Besuchers, seine Identifikationsnummer, seine Vereinigung, der Zweck des Besuchs sowie Datum und Uhrzeit des Besuchs festgehalten werden. - Es wird verlangt, dass alle eingeladenen Besucher durch das Büro begleitet werden müssen. - Es wird verlangt, dass alle Besucherausweise am Ende des Tages, am Tag der Ausstellung, ablaufen. - Es wird verlangt, dass alle NinjaRMM-Mitarbeiter alle Anstrengungen unternehmen, um ein geordnetes Arbeitsumfeld zu schaffen, das frei von Unordnung und der Preisgabe geschützter oder sensibler Informationen ist. - Vorschrift, dass nicht benutzte Akten in den Gemeinschaftsbereichen am Ende des Tages geschreddert oder in einem Aktenschrank eingeschlossen werden. - Aufzeichnung des Ein- und Ausgangs aller Besucher und Mitarbeiter durch eine der vorhandenen Türen und Aufbewahrung dieser Aufzeichnungen für mindestens 30 Tage. - Unverzüglicher Entzug aller Schlüsselkarten, Token und des physischen Zugangs von Mitarbeitern, die freiwillig gegangen sind oder denen gekündigt wurde.
Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen	• NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-92, Guide to Computer Security Log Management • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)

	Außerdem nutzt Ninja: 1) Nutzung eines 24x7 Security Operations Center durch einen branchenweit vertrauenswürdigen externen Sicherheitsdienstleister. 2) Einsatz von Echtzeit-Überwachung, Auditing und Alarmierung von: o Netzwerkeingang o Netzwerk-Ausgang o Dateiveränderungen o Konfigurationsänderungen o erfolgreiche und fehlgeschlagene Anmeldungen o Befehlsausführung o Ausführung von Anwendungen o privilegierte Ausführung o Schwachstellen im Betriebssystem o Software-Schwachstellen o Richtlinienänderungen o völlig neue Aktivität o atypische Aktivitäten 3) Aufrechterhaltung der Protokolle und der erfassten Ereignisse für mindestens ein Jahr und, falls erforderlich, bis zu einem unbestimmten Zeitraum.
Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-36, Guide to Selecting Information Technology Security Products • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-40, Guide to Enterprise Patch

	Management Technologies
Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response
Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten	Jährliche Prüfungen und Tests der Konformitäts- und Sicherheitskontrollen im Rahmen des AICPA Service Organization Control (SOC 2)-Prozesses zur Prüfung der Grundsätze des Vertrauensdienstes. Die

	AICPA SOC 2-Prüfung umfasst 144 [von 150] Einzelkontrollen, die sich mit der ISO27001-Norm überschneiden.
Maßnahmen zur Gewährleistung der Datenminimierung	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response
Maßnahmen zur Gewährleistung der	• NIST SP # 800-35, Guide to Information

Datenqualität	Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response
Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung	• NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • Using Amazon Web Services for Disaster Recovery, AWS October 2011

	• Disaster Recovery with Amazon Web Services: A Technical Guide, Accenture June 2016 • Architecting for the Cloud: AWS Best Practices, AWS October 2018 • AWS Well-Architected Framework, AWS July 2019 • Affordable Enterprise-Grade Disaster Recovery Using AWS, CloudEndure/AWS 2019
Maßnahmen zur Gewährleistung der Rechenschaftspflicht	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-92, Guide to Computer Security Log Management • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering

	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • Für alle Daten, die zwischen dem NinjaRMM Agent und der NinjaRMM Plattform übertragen werden, werden FIPS 140-2 konforme kryptographische Module mittels TLS Verschlüsselung eingesetzt. o Insbesondere sind alle Chiffren Perfect-Forward Secrecy (PFS), mit der folgenden Verschlüsselung: ▪ ECDHE RSA with AES128-GCM and SHA256 ▪ ECDHE RSA with AES128-CBC and SHA256 ▪ ECDHE RSA with AES128-CBC and SHA ▪ ECDHE RSA with AES256-GCM and SHA384 ▪ ECDHE RSA with AES256-CBC and SHA384 ▪ ECDHE RSA with AES256-CBC and SHA • Für alle Daten im Ruhezustand, die im NinjaRMM-Plattform-Backend gespeichert sind, werden FIPS 140-2-konforme kryptographische Module für die Verschlüsselung im Ruhezustand verwendet. Die Daten werden mit einer Mindeststufe von AES256 verschlüsselt, wobei bei Bedarf auch eine stärkere Verschlüsselung eingesetzt werden kann. • NIST SP # 800-111, Guide to Storage Encryption Technologies for End User Devices • NIST SP # 800-124, Guidelines for

	Managing the Security of Mobile Devices in the Enterprise
Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-) Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.	• NIST SP # 800-35, Guide to Information Technology Security Services • NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems • NIST SP # 800-95, Guide to Secure Web Services • NIST SP # 800-123, Guide to General Server Security • NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing • NIST SP # 800-160, Systems Security Engineering • NIST SP # 800-39, Managing Information Security Risk • NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy • NIST SP # 800-154, Guide to Data-Centric System Threat Modeling • NIST SP # 800-128, Guide for Security-Focused Configuration Management of Information Systems • NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs) • NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) • NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations • NIST SP # 800-34, Contingency Planning Guide for Federal Information Systems • NIST SP # 800-61, Computer Security Incident Handling Guide • NIST SP # 800-184, Guide for Cybersecurity Event Recovery • NIST SP # 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops • NIST SP # 800-86, Guide to Integrating Forensic Techniques into Incident Response

ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Amazon Web Services Inc. (AWS), mit AWS GDPR DPA:
********d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf*

Gemäß der AWS GDPR DPA behält sich AWS das Recht vor, weitere Subunternehmer zu behalten.