DATENVERARBEITUNGSVEREINBARUNG

Diese Datenverarbeitungsvereinbarung (die „**DPA**“) wird zum Datum des Inkrafttretens, wie unten in Abschnitt 2 dargelegt („**Datum des Inkrafttretens**“), von NinjaOne, LLC, einer Delaware Limited Liability Company mit Sitz in Suite 200, 3687 Tampa Road, Oldsmar, Florida, 34677, Vereinigte Staaten von Amerika („**NinjaOne**“) und dem im Unterschriftsfeld angegebenen Unternehmen („**Kunde**“; jeweils die „**Partei**“ und gemeinsam die „**Parteien**“) geschlossen.

Präambel

In der Erwägung, dass NinjaOne eine SaaS-basierte, mandantenfähige RMM-Plattform betreibt und den zugehörigen technischen Support dafür bereitstellt (zusammenfassend die „**Dienstleistung**“) und dem Kunden den Zugang dazu ermöglicht.

In der Erwägung, dass die Parteien eine oder mehrere Vereinbarung(en) und Zusätze dazu (die „**Vereinbarung**“) für die Erbringung der Dienstleistung durch NinjaOne an den Kunden, wie in der Vereinbarung beschrieben, geschlossen haben.

In der Erwägung, dass NinjaOne bei der Erbringung der Dienstleistung im Rahmen der Vereinbarung bestimmte personenbezogene Daten im Namen des Kunden verarbeiten kann, wobei diese Daten vom Kunden durch die Dienstleistung direkt oder indirekt im Rahmen der Vereinbarung zur Verfügung gestellt werden.

In Anbetracht der hierin dargelegten gegenseitigen Vereinbarungen und Bedingungen, vereinbaren die Parteien folgendes:

1. Definitionen

Sofern sich aus dem Zusammenhang nichts anderes ergibt, haben die folgenden Begriffe die in diesem Abschnitt 1 festgelegte Bedeutung:

„**Anhang**“ bezeichnet einen Anhang zu dieser DPA, der einen integralen Bestandteil dieser DPA bildet;

„**Anwendbares Datenschutzrecht**“ bezeichnet alle anwendbaren Gesetze, Verordnungen und sonstigen rechtlichen Anforderungen in Bezug auf Datenschutz, Datensicherheit, Privatsphäre oder die Verarbeitung personenbezogener Daten in ihrer jeweils gültigen Fassung. Dies kann beispielsweise die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, „**DSGVO**“) umfassen, zusammen mit etwaigen Ersatzgesetzen oder ähnlichen Gesetzen, die vom Vereinigten Königreich im Zuge seines Übergangs aus der Europäischen Union oder nach seinem Austritt aus der Europäischen Union erlassen wurden, oder einer gleichwertigen Gesetzgebung einer anderen anwendbaren Rechtsordnung, der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, dem California Consumer Privacy Act und den dazugehörigen Verordnungen („**CCPA**“), dem California Privacy Rights Act und den dazugehörigen Verordnungen („**CPRA**“, und zusammen mit dem

CCPA das „**California Privacy Law**“) und ähnlichen US-Bundesstaatsgesetzen;

„**Personenbezogene Daten**“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person im Sinne der DSGVO beziehen (unabhängig davon, ob die DSGVO Anwendung findet), sowie alle anderen Informationen, die personenbezogene Daten (*personal information*) im Sinne des California Privacy Law (unabhängig davon, ob das California Privacy Law Anwendung findet);

„**Verarbeitung**“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten oder Datensätzen wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; und

Die in dieser DPA verwendeten Begriffe, die hier nicht definiert sind, haben die Bedeutung, die ihnen im geltenden Datenschutzgesetz zukommt.

2. Inkrafttreten der DPA

Diese DPA tritt an dem Tag in Kraft, an dem diese DPA vom Kunden unterzeichnet wird (Datum des Inkrafttretens).

3. Geltungsbereich dieser DPA

Diese DPA gilt für die Personenbezogenen Daten, die der Kunde NinjaOne direkt oder indirekt durch die Dienstleistung in Verbindung mit der Vereinbarung, wie in Anlage 1 zu dieser DPA beschrieben, zur Verfügung stellt (die „**Kundendaten**“). Der Kunde kann sich dafür entscheiden, die Dienstleistung so zu konfigurieren oder zu nutzen, dass Kundendaten und andere Daten mit Dienstleistungen von Drittanbietern geteilt werden („**Verknüpfbare Dienstleistungen von Drittanbietern**“), von denen einige von NinjaOne als Wiederverkäufer oder Händler erworben werden können. NinjaOne ist nicht für die Verarbeitung von Daten durch Verknüpfbare Dienstleistungen von Drittanbietern verantwortlich, und diese Verarbeitung unterliegt nicht dieser DPA.

4. Verarbeitung von Personenbezogenen Daten

4.1 NinjaOne verarbeitet die Kundendaten im Namen des Kunden und agiert als Auftragsverarbeiter und der Kunde handelt als oder im Namen eines für die Verarbeitung Verantwortlichen. Handelt der Kunde im Namen eines für die Verarbeitung Verantwortlichen (oder im Namen von Vermittlern wie anderen Auftragsverarbeitern des für die Verarbeitung Verantwortlichen), so gilt, soweit gesetzlich zulässig, Folgendes:

(a) Der Kunde ist der einzige Ansprechpartner für NinjaOne in Bezug auf diese Dritten;

(b) NinjaOne muss in Angelegenheiten, die diese DPA betreffen, nicht direkt mit solchen Dritten interagieren; und

(c) Wenn NinjaOne andernfalls verpflichtet wäre, einem solchen Dritten

Informationen, Unterstützung oder Zusammenarbeit zu gewähren, kann NinjaOne diese nur dem Kunden zur Verfügung stellen; aber

(d) Ausschließlich hinsichtlich Personenbezogener Daten eines Dritten darf NinjaOne, wenn NinjaOne vernünftigerweise annehmen darf, unter den gegebenen Umständen rechtlich dazu verpflichtet zu sein, (i) die Anweisungen eines solchen Dritten anstelle der Anweisungen des Kunden befolgen und (ii) einem solchen Dritten Informationen, Unterstützung oder Zusammenarbeit anbieten.

4.2 Jede Partei kommt den Verpflichtungen, die für sie nach dem anwendbaren Datenschutzrecht gelten, in vollem Umfang nach. Zwischen den Parteien wird ausdrücklich vereinbart, dass die Kundendaten zu jeder Zeit Eigentum des Kunden bleiben.

4.3 In seiner Eigenschaft als Auftragsverarbeiter:

(a) NinjaOne behandelt die Kundendaten als vertrauliche Informationen und verarbeitet die Kundendaten einzig und allein zum Zweck der Erbringung der Dienstleistung für den Kunden und im Namen des Kunden.

(b) NinjaOne bietet zu jeder Zeit während der Durchführung dieser DPA ausreichende Garantien für die Einhaltung der Anforderungen des anwendbaren Datenschutzrechts. NinjaOne darf Kundendaten nur für Zwecke verwenden, offenlegen, aufbewahren oder anderweitig verarbeiten, die für die Erfüllung unbedingt erforderlich sind (i) um den gewünschten Betrieb der Dienste für den Kunden bereitzustellen und zu unterstützen, (ii) um in dem nach dem geltenden Datenschutzrecht zulässigen Umfang aggregierte oder anonymisierte[1] Daten für NinjaOne‘s rechtmäßige Nutzung zu erstellen und (iii) um seine Verpflichtungen aus der Vereinbarung, dieser DPA oder dem geltenden Datenschutzrecht zu erfüllen, und verarbeitet die Kundendaten nur in Übereinstimmung mit den angemessenen dokumentierten Anweisungen des Kunden, die in dieser DPA, der Vereinbarung oder auf andere Weise während der Erfüllung dieser DPA erteilt werden (der "zulässige Zweck"). Sollte NinjaOne nach geltendem Recht verpflichtet sein, Kundendaten auf eine andere als die hierin erlaubte Weise zu verarbeiten, informiert NinjaOne den Kunden vor der Verarbeitung über dieses gesetzliche Erfordernis, es sei denn, das Gesetz verbietet eine solche Information aus Gründen des öffentlichen Interesses. Ohne Einschränkung der vorgenannten Verpflichtungen:

i. wird NinjaOne die Personenbezogenen Daten nicht „verkaufen“ (*sell*), wie im CPRA und ähnlichen Gesetzen in den USA definiert ist;
ii. wird NinjaOne die Personenbezogenen Daten nicht „weitergeben“ (*share*), wie im CPRA und den damit verbundenen Vorschriften definiert ist;
iii. wird NinjaOne nicht versuchen, vom Kunden erhaltene pseudonymisierte oder anderweitig anonymisierte Personenbezogene Daten ohne die ausdrückliche schriftliche Zustimmung des Kunden zu identifizieren;
iv. darf NinjaOne die Personenbezogenen Daten nicht außerhalb der direkten Geschäftsbeziehung zwischen dem Kunden und NinjaOne aufbewahren, nutzen oder weitergeben;
v. beachtet NinjaOne alle geltenden Beschränkungen des anwendbaren Datenschutzrechts hinsichtlich der Kombination Personenbezogener Daten, die NinjaOne vom Kunden oder in dessen Namen erhält, mit

[1] Aus Klarstellungsgründen: Aggregierte und anonymisierte Daten dürfen keine persönlich identifizierbaren Informationen oder Informationen, die eine Person identifizieren können, enthalten.

Personenbezogenen Daten, die NinjaOne von einer oder mehreren anderen Person(en) oder in deren Namen erhält oder die NinjaOne im Rahmen einer gesonderten Interaktion zwischen NinjaOne und einer betroffenen Person erhebt; und

vi. wird NinjaOne für Personenbezogene Daten, die dem CPRA unterliegen, kein geringeres als das nach dem CPRA geforderte Schutzniveau bieten (zusätzlich zur Erfüllung seiner anderen Verpflichtungen aus dieser DPA).

(c) NinjaOne informiert den Kunden unverzüglich, wenn eine Anweisung seiner Ansicht nach gegen das anwendbare Datenschutzrecht verstößt, und teilt ihm die Einzelheiten des Verstoßes oder des möglichen Verstoßes mit. NinjaOne ist berechtigt, die Erbringung einer Dienstleistung auszusetzen, bei welcher der Verdacht besteht, dass sie gegen das anwendbare Datenschutzrecht verstößt, bis der Kunde seine Weisung schriftlich bestätigt oder abändert. NinjaOne ist berechtigt, Anweisungen des Kunden, die offensichtlich rechtswidrig sind und/oder gegen das anwendbare Datenschutzrecht verstoßen, zurückzuweisen.

(d) NinjaOne ergreift vor und während der Verarbeitung von Kundendaten angemessene technische und organisatorische Sicherheitsmaßnahmen, um die Sicherheit, Vertraulichkeit und Integrität der Kundendaten zu schützen und die Kundendaten vor versehentlicher, unrechtmäßiger oder unbefugter Verarbeitung zu schützen. Insbesondere schützt NinjaOne die Kundendaten gegen zufällige oder unrechtmäßige Zerstörung, Verlust, Veränderung, unberechtigte Offenlegung, Nutzung oder Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete Kundendaten sowie gegen unrechtmäßige Verarbeitung. NinjaOne gewährleistet ein Sicherheitsniveau, das den mit der Verarbeitung der Kundendaten verbundenen Risiken und der Art der Kundendaten angemessen ist. Zu diesen Maßnahmen gehören, soweit angemessen:

i. Verfahren zum Schutz der bestehenden Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten;
ii. Verfahren zur rechtzeitigen Wiederherstellung der Verfügbarkeit und des Zugriffs auf die Kundendaten im Falle eines physischen oder technischen Zwischenfalls;
iii. Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zum Schutz der Sicherheit der Verarbeitung; und
iv. Verfahren zum Löschen, Vergessen, Ändern, Korrigieren oder Portieren der Kundendaten nach Anweisung des Kunden.

Diese Maßnahmen umfassen mindestens die technischen und organisatorischen Maßnahmen („**TOM**“), die der einschlägigen Branchenpraxis entsprechen oder diese übertreffen. Diese Maßnahmen (oder Alternativen, die NinjaOne nach eigenem Ermessen einführen kann und die das Gesamtschutzniveau nicht senken) müssen während der gesamten Dauer der Erbringung der Dienstleistung durch NinjaOne für den Kunden oder bis zur Einstellung der Verarbeitung von Kundendaten durch NinjaOne (je nachdem, welcher Zeitpunkt später eintritt) in Kraft bleiben;

(e) NinjaOne behandelt die Kundendaten vertraulich und gestattet seinen Mitarbeitern, Beratern oder Beauftragten den Zugriff auf die Kundendaten nur dann, wenn sie diese Kundendaten zur Erfüllung der ihnen von NinjaOne zugewiesenen Aufgaben benötigen (die „**Autorisierten Personen**“). NinjaOne stellt sicher, dass die Autorisierten

Personen, die Kundendaten verarbeiten:

i. über die Bestimmungen dieser DPA informiert sind und sie einhalten;
ii. in Bezug auf die Kundendaten einer Geheimhaltungspflicht unterliegen, die nicht weniger restriktiv ist als die hierin festgelegten Pflichten, bevor sie Zugang zu den Kundendaten erhalten. NinjaOne stellt sicher, dass diese Geheimhaltungspflicht auch nach Beendigung des Beschäftigungs- oder Vertragsverhältnisses bestehen bleiben;
iii. eine angemessene Schulung in Bezug auf das geltende Datenschutzrecht erhalten haben;
iv. beim Zugriff auf die Kundendaten einer Benutzerauthentifizierung und einem Anmeldeverfahren unterliegen; und
v. Kundendaten nur insoweit verarbeiten dürfen, wie dies für den zulässigen Zweck erforderlich ist.

(f) NinjaOne wird den Kunden unverzüglich unterrichten, wenn Kundendaten aufgrund von Insolvenz- oder sonstigen Verfahren oder Maßnahmen Dritter gepfändet oder beschlagnahmt werden oder gefährdet sind, es sei denn, NinjaOne ist dies gerichtlich oder durch Anordnung der zuständigen Behörde untersagt. NinjaOne informiert die zuständigen Behörden darüber, dass die Nutzung der Kundendaten im alleinigen Ermessen des Kunden liegt.

4.4 Unterauftragsverarbeiter

(a) Einsatz von Unterauftragsverarbeitern: NinjaOne kann von Zeit zu Zeit Unterauftragsverarbeiter damit beauftragen, Dienstleistungen in seinem Namen zu erbringen. Zu diesen Unterauftragsverarbeitern können Tochtergesellschaften oder verbundene Unternehmen von NinjaOne gehören. Der Kunde stimmt hiermit der Beauftragung von Unterauftragsverarbeitern durch NinjaOne zur Verarbeitung Personenbezogener Daten im Rahmen der Vereinbarung und vorbehaltlich der hier dargelegten Bedingungen zu.

(b) Verpflichtungen: NinjaOne schließt mit solchen Unterauftragsverarbeitern („**Genehmigter Unterauftragsverarbeiter**“) schriftliche Verträge ab, die mindestens das hierin vorgesehene Datenschutz- und Informationssicherheitsniveau gewährleisten. In jedem Fall haftet NinjaOne gegenüber dem Kunden für jeden Verstoß des Genehmigten Unterauftragsverarbeiters, der durch eine Handlung, einen Fehler oder eine Unterlassung des Genehmigten Unterauftragsverarbeiters verursacht wird in demselben Umfang, in dem NinjaOne haften würde, als wäre die Handlung, der Fehler oder die Unterlassung von NinjaOne selbst begangen worden.

(c) Aktuelle Unterauftragsverarbeiter: Der Kunde genehmigt hiermit die folgenden Unterauftragsverarbeiter als Genehmigte Unterauftragsverarbeiter: https://www.ninjaone.com/approved-subprocessors/ (die „**Webseite für Genehmigte Unterauftragsverarbeiter**“). Die Genehmigten Unterauftragsverarbeiter behalten sich das Recht vor, weitere Unterauftragsverarbeiter zu beauftragen und ihre spezifische Sicherheitsstrategie zu überarbeiten, solange das allgemeine Sicherheitsniveau nicht gesenkt wird.

(d) Neue Unterauftragsverarbeiter: NinjaOne informiert den Kunden mindestens 30 Tage im Voraus über die Ernennung eines Genehmigten Unterauftragsverarbeiters, einschließlich seiner Identität, wo er die Personenbezogenen Daten verarbeiten wird sowie

über die entsprechenden Datenverarbeitungstätigkeiten, indem NinjaOne (i) die Webseite für Genehmigte Unterauftragsverarbeiter (oder eine andere dort beschriebene Webseite) aktualisiert und (ii) dem Kunden am selben Tag der Aktualisierung eine E-Mail sendet, wenn der Kunde solche E-Mails abonniert hat, indem er eine E-Mail-Adresse im Anmeldeformular auf der Webseite für Genehmigte Unterauftragsverarbeiter angegeben hat.

(e) Einsprüche: Der Kunde hat das Recht, gegen den Einsatz eines Unterauftragsverarbeiters Einspruch zu erheben, indem er innerhalb von 10 Tagen nach der Mitteilung von NinjaOne über die Beauftragung des Unterauftragsverarbeiters eine Mitteilung in Textform an privacyteam@ninjaone.com richtet, in der er die Gründe für den Einspruch erläutert („**Einspruch**"). Legt der Kunde innerhalb dieser Frist keinen Widerspruch ein, gilt dies als Zustimmung zur Beauftragung des Unterauftragsverarbeiters durch NinjaOne. Im Falle eines solchen Widerspruchs arbeiten die Parteien für einen Zeitraum von bis zu 30 Tagen in bestem Bemühen zusammen, um eine angemessene Lösung für die Bedenken des Kunden zu finden. Wenn nach Ablauf dieser 30 Tage keine angemessene Lösung gefunden wurde, kann der Kunde diese DPA und die Vereinbarung mit einer Frist von 10 Tagen schriftlich gegenüber NinjaOne kündigen.

5. Internationale Übermittlung von Personenbezogenen Daten

NinjaOne oder ein Genehmigter Unterauftragsverarbeiter darf keine Kundendaten außerhalb des Europäischen Wirtschaftsraums verarbeiten oder übertragen (und auch nicht zulassen, dass die Kundendaten übermittelt werden), es sei denn, es wird ein angemessenes Schutzniveau in Übereinstimmung mit dem anwendbaren Datenschutzrecht gewährleistet (die „**Sicherheitsvorkehrungen**").

NinjaOne ist nach AICPA Service Organization Control (SOC 2) Typ II zertifiziert. Bei der jährlichen SOC 2-Prüfung werden 144 von 150 Einzelkontrollen überprüft, die sich mit dem ISO 27001-Standard überschneiden. NinjaOne schützt Personenbezogene Daten auch durch Compliance- und Sicherheitskontrollen, die auf den folgenden Rahmenwerken und Richtlinien basieren (auf nicht zertifizierter Basis):

- NIST Cyber Security Framework Revision 1.1
- U.S.-Verteidigungsministerium DFARS 252.204-712
- NIST Sonderveröffentlichung 800-171 Revision 2
- NIST Sonderveröffentlichung 800-53 Revision 5
- United States Cybersecurity Maturity Model Certification (CMMC) Level 3.

In dem Maße, in dem dies notwendig werden sollte, werden weitere Schutzmaßnahmen ergriffen, die unter anderem Folgendes umfassen können: (i) eine Übermittlung nur in Länder, die gemäß einem Angemessenheitsbeschluss der Europäischen Kommission ein angemessenes Datenschutzniveau gewährleisten, oder (ii) einen alternativen anerkannten Standard für die rechtmäßige Übermittlung Personenbezogener Daten - wie in der DSGVO definiert - außerhalb des Europäischen Wirtschaftsraums, wie z. B. die EU-Standardvertragsklauseln.

Wenn der Kunde die Dienstleistung nutzt, um Personenbezogene Daten an einen Dritten zu übertragen, der kein zugelassener Unterauftragsverarbeiter ist, ist der Kunde für die Rechtmäßigkeit einer solchen Übertragung verantwortlich.

Um die Übertragung von Kundendaten, die der DSGVO unterliegen, vom Kunden an

NinjaOne zu legitimieren, schließen die Parteien hiermit die EU-Standardvertragsklauseln, die als Anlage 3 beigefügt sind und im gesetzlich vorgeschriebenen Umfang gelten, ab. Sollten die aktuellen EU-Standardvertragsklauseln durch weitere Klauseln ersetzt werden, werden die Parteien zusammenarbeiten, um die überarbeiteten Klauseln umzusetzen.

In Bezug auf personenbezogene Daten, für die das Datenschutzrecht des Vereinigten Königreichs die Übermittlung des Kunden an NinjaOne regelt, soweit rechtlich erforderlich, gilt das United Kingdom International Data Transfer Addendum zu den Standardvertragsklauseln der EU-Kommission (verfügbar unter https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/; „**UK SCC Addendum**“) als Teil dieser DPA. Es gilt dabei als wie folgt ausgefüllt (wobei Begriffe, die nicht anderweitig definiert sind, die im UK SCC Addendum festgelegte Bedeutung haben):

- Tabelle 1 des UK SCC Addendums: Die Parteien, ihre Angaben und ihre Kontakte sind in Anhang A aufgeführt
- Tabelle 2 des UK SCC-Addendums: Die Genehmigten EU-Standardvertragsklauseln sind die EU-Standardvertragsklauseln, die in Anlage 3 dieses DPA aufgeführt sind
- Tabelle 3 des UK SCC Addendum: Die Anhänge werden am Ende der EU-Standardvertragsklauseln in Anhang 3 dieses DPA aufgeführt
- Tabelle 4 des UK SCC-Addendums: Keine der Parteien kann das in Abschnitt 19 des UK SCC-Addendums festgelegte Kündigungsrecht ausüben.

In Bezug auf personenbezogene Daten, für die das Schweizerische Bundesgesetz über den Datenschutz („**DSG**“) die Übermittlung durch den Kunden an NinjaOne regelt, gelten die EU-Standardvertragsklauseln als mit den folgenden Abweichungen versehen, soweit das Schweizer DSG dies erfordert:

- Verweise auf die DSGVO in den EU-Standardvertragsklauseln sind als Verweise auf das Schweizer DSG zu verstehen, sofern die Datenübermittlung ausschließlich dem Schweizer DSG und nicht der DSGVO unterliegt
- Der Begriff "Mitgliedstaat" in den EU-Standardvertragsklauseln ist nicht so auszulegen, dass betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) gemäß Klausel 18(c) der EU-Standardvertragsklauseln einzuklagen
- Verweise auf personenbezogene Daten in den EU-Standardvertragsklauseln beziehen sich auch auf Daten über identifizierbare juristische Personen bis zum Inkrafttreten der Revisionen des schweizerischen DSG, die diesen breiteren Anwendungsbereich aufheben
- Gemäß Anhang I(C) der EU-Standardvertragsklauseln (zuständige Aufsichtsbehörde):
    - Wenn die Übermittlung ausschließlich dem Schweizer DSG und nicht der DSGVO unterliegt, ist die Aufsichtsbehörde der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte
    - Wenn die Übermittlung sowohl dem DSG als auch der DSGVO unterliegt, ist die Aufsichtsbehörde der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, sofern die Übermittlung durch das DSG geregelt ist, und die Aufsichtsbehörde ist die in den EU-Standardvertragsklauseln festgelegte Aufsichtsbehörde, sofern die Übermittlung unter die DSGVO fällt.

Wenn der Kunde die Dienstleistung nutzt, um Personenbezogene Daten an einen Dritten zu übertragen, der kein zugelassener Unterauftragsverarbeiter ist, ist der Kunde für die Rechtmäßigkeit einer solchen Übertragung verantwortlich.

6. Melde- und Mitwirkungspflicht

NinjaOne wird den Kunden unverzüglich schriftlich benachrichtigen und/oder umfassend mit ihm zusammenarbeiten:

(a) Wenn NinjaOne aus irgendeinem Grund (i) einen Teil dieser DPA nicht einhalten kann oder nicht eingehalten hat, (ii) gegen anwendbares Datenschutzrecht verstoßen würde oder verstoßen hat, das die Verarbeitung von Kundendaten regelt, oder (iii) anwendbares Datenschutzrecht die rechtmäßige Übermittlung von Kundendaten vom Kunden an NinjaOne nicht mehr zulässt. In solchen Fällen ergreift NinjaOne alle angemessenen, notwendigen und geeigneten Maßnahmen, um die Nichteinhaltung zu beheben oder die weitere Verarbeitung von Kundendaten einzustellen und der Kunde kann die Vereinbarung und diese DPA oder den Zugang zu den Kundendaten unverzüglich kündigen oder andere angemessene Maßnahmen ergreifen, die er nach eigenem Ermessen bestimmt.

(b) Um den Kunden in die Lage zu versetzen, seinen Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung von Kundendaten nachzukommen, wobei die Art der Verarbeitung und die NinjaOne zur Verfügung stehenden Informationen berücksichtigt werden.

(c) Sobald er von einer Datenschutzverletzung erfährt. In diesem Fall informiert NinjaOne den Kunden unverzüglich über die Datenschutzverletzung und stellt ihm alle Informationen und die Zusammenarbeit zur Verfügung, die der Kunde vernünftigerweise verlangen kann, auch damit der Kunde seine Meldepflichten bei Datenschutzverletzungen gemäß dem anwendbaren Datenschutzrecht (und in Übereinstimmung mit den dort vorgeschriebenen Fristen) erfüllen kann. NinjaOne ergreift ferner alle angemessenen Maßnahmen und Handlungen, die erforderlich sind, um die Auswirkungen der Datenschutzverletzung zu beheben oder abzumildern, und hält den Kunden über die Entwicklungen im Zusammenhang mit der Datenschutzverletzung auf dem Laufenden.

(d) Bei der Vorbereitung von Datenschutz-Folgenabschätzungen, die vom Kunden durchgeführt werden, unabhängig davon, ob es sich um eine obligatorische oder freiwillige Prüfung handelt. NinjaOne unterstützt den Kunden in angemessenem Umfang und rechtzeitig bei der Durchführung einer Datenschutz-Folgenabschätzung in Bezug auf die Kundendaten und, falls erforderlich, bei der Konsultation der zuständigen Datenschutzbehörde. NinjaOne erklärt sich damit einverstanden und erkennt an, dass der Kunde im Falle einer Anfrage einer Datenschutzbehörde die Bedingungen dieser DPA, die Vereinbarung und alle anderen Informationen, die NinjaOne zum Nachweis der Einhaltung dieser DPA oder des anwendbaren Datenschutzrechts bereitstellt, weitergeben kann.

Zusätzlich zu den vorangegangenen Bestimmungen wird NinjaOne den Kunden unverzüglich informieren, wenn NinjaOne der Ansicht ist oder davon Kenntnis erlangt, dass die Verarbeitung der Kundendaten wahrscheinlich zu einem hohen Risiko (im Sinne des anwendbaren Datenschutzgesetzes, der einschlägigen regulatorischen Leitlinien und der Rechtsprechung) in Bezug auf die Datenschutzrechte und -Freiheiten der betroffenen Personen führen wird.

(e) Jede vom Kunden geforderte angemessene Zusammenarbeit leisten, um (i) die Ausübung von Rechten betroffener Personen gemäß geltendem Datenschutzrecht (z. B. das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Widerspruch gegen die Verarbeitung ihrer Personenbezogenen Daten, das Recht auf Löschung und das Recht auf Einschränkung der Verarbeitung ihrer Personenbezogenen Daten sowie das Recht auf Datenübertragbarkeit) und (ii) jede andere Korrespondenz, Anfrage oder Beschwerde einer betroffenen Person, einer Aufsichtsbehörde oder eines sonstigen Dritten in Bezug auf Kundendaten, die von NinjaOne im Rahmen dieser DSGVO verarbeitet werden, beantworten und erfüllen zu können. NinjaOne unterrichtet den Kunden unverzüglich über alle Ersuchen in Bezug auf die Ausübung dieser Rechte oder Beschwerden, Anfragen oder Korrespondenz, wenn diese direkt bei NinjaOne eingehen, und übermittelt alle Einzelheiten dazu. Darüber hinaus stellt NinjaOne alle vom Kunden angeforderten Kundendaten innerhalb eines vom Kunden festgelegten angemessenen Zeitrahmens zur Verfügung und unterstützt den Kunden bei der Erfüllung der jeweiligen Anfrage innerhalb der geltenden Fristen. NinjaOne ist sich darüber im Klaren, dass die Beantwortung solcher direkten Anfragen der vorherigen schriftlichen Genehmigung durch den Kunden bedarf. Falls erforderlich, wird NinjaOne mit der zuständigen Aufsichtsbehörde zusammenarbeiten.

(f) Auf berechtigtes Verlangen des Kunden alle Aufzeichnungen, geeignetes Personal, Datenverarbeitungseinrichtungen und alle relevanten Materialien im Zusammenhang mit der Verarbeitung der Kundendaten dem Kunden zur Verfügung stellen, damit der Kunde die Einhaltung seiner Verpflichtungen nach dem geltenden Datenschutzrecht nachweisen kann. Der Kunde ergreift alle angemessenen Maßnahmen, um eine unnötige Störung des Betriebs von NinjaOne zu vermeiden. Der Kunde wird seine, in dieser Klausel festgelegten, Überprüfungsrechte nicht öfter als einmal innerhalb eines Zeitraums von zwölf (12) Kalendermonaten und mit einer Vorankündigung von neunzig (90) Tagen ausüben, es sei denn, (i) der Kunde ist auf Anweisung einer zuständigen Datenschutzbehörde dazu verpflichtet oder (ii) hält eine weitere Überprüfung aufgrund einer von NinjaOne erfolgten Datenschutzverletzung für erforderlich. Der Kunde hat das Recht, geeignete und angemessene Maßnahmen zu ergreifen, um die unbefugte Nutzung Personenbezogener Daten zu unterbinden und zu beheben.

NinjaOne bestätigt hiermit, seine Verpflichtungen aus dieser DPA zu kennen und sie einzuhalten.

7. Wirkung der Beendigung

Innerhalb von neunzig (90) Tagen nach Ablauf oder Beendigung der Vereinbarung löscht NinjaOne auf eigene Kosten alle Kundendaten und alle vorhandenen Kopien davon, die sich in seinem Besitz befinden, es sei denn, ein anwendbares Gesetz schreibt die weitere Speicherung der Kundendaten vor. Auf Verlangen des Kunden bescheinigt NinjaOne dem Kunden, dass alle Kundendaten in Übereinstimmung mit dem Vorstehenden gelöscht wurden. Ist NinjaOne aus technischen Gründen nicht in der Lage, die Kundendaten zu löschen, wird NinjaOne den Kunden unverzüglich informieren und alle geeigneten und angemessen Maßnahmen ergreifen, um:

i. einer vollständigen und dauerhaften Löschung der Kundendaten möglichst nahe zu kommen und die verbleibenden Kundendaten vollständig und wirksam zu anonymisieren; und
ii. die verbleibenden Kundendaten, die nicht gelöscht oder wirksam anonymisiert werden, für jede weitere Verarbeitung unzugänglich zu machen, es sei denn, dies

ist gesetzlich vorgeschrieben.

8. Vorrangige Reihenfolge

Mit der Unterzeichnung durch den Kunden wird diese DPA (einschließlich der EU-Standardvertragsklauseln, die wie in der DPA beschrieben, für das Vereinigte Königreich und die Schweiz ergänzt werden) Teil des Vertrags. Die EU-Standardvertragsklauseln haben im Falle von Abweichungen Vorrang vor dem Rest der DPA, und die DPA hat im Falle von Abweichungen Vorrang vor dem Rest der Vereinbarung.

NINJAONE, LLC	**Firma der Kunden:**
Durch: DocuSigned by: Brian Krupczak B12C09F15DB4479...	Durch:
Name: Brian Krupczak	Name:
Funktion: Asst. General Counsel	Funktion:
Datum: 8/18/2023	Datum:
	Anschrift des Kunden:

Zeitplan 1:
Zeitplan für die Datenverarbeitung

1. Kategorien von Daten

Die von NinjaOne verarbeiteten Kundendaten umfassen die folgenden Daten (unter der Voraussetzung, dass die Bestimmungen der DPA nur gelten, wenn und soweit diese Daten Personenbezogene Daten darstellen):

- IP-Adresse(n) für Endgeräte des NinjaOne-Kunden und/oder seiner Kunden, z. B. Laptops, Desktop-PCs
- Systemnamen für Endnutzergeräte, die dem NinjaOne-Kunden und/oder seinen Kunden gehören, z. B. Laptops, Desktop-PCs
- Angaben zur Hardware der Endnutzergeräte des NinjaOne-Kunden und/oder seiner Kunden, z. B. Laptops, Desktop-PCs
- Software-Details der Endgeräte des NinjaOne-Kunden und/oder seiner Kunden, z. B. Laptops, Desktop-PCs
- Benutzernamen, die dem NinjaOne-Kunden und/oder seinen Kunden gehören
- Personenbezogene Daten in den Namen von Dateien oder Ordnerstrukturen, die der Kunde mit Hilfe der Dienstleistung verwaltet;
- Personenbezogene Daten in Dateien, die der Kunde durch die Dienstleistung überträgt oder empfängt;
- Browser-/Benutzer-Agenten-Details von Endgeräten des NinjaOne-Kunden und/oder seiner Kunden, z. B. Laptops, Desktop-PCs
- Leistungs- und Nutzungskennzahlen von Endnutzergeräten des NinjaOne-Kunden und/oder seiner Kunden, z. B. Laptops, Desktop-PCs
- Fehlercodes von Endgeräten des NinjaOne-Kunden und/oder seiner Kunden, z. B. Laptops, Desktop-PCs.

2. Kategorien von betroffenen Personen

Betroffene Personen sind die Personen, deren Daten von NinjaOne verarbeitet werden; dazu können Endnutzer oder Angestellte und Mitarbeiter des Kunden und/oder deren Kunden gehören.

3. Zulässige Verarbeitungen für NinjaOne

Die Verarbeitung umfasst alle Datenverarbeitungsaktivitäten, die nach den Anweisungen des Kunden durchgeführt werden und die für die Erbringung der Dienstleistung an den Kunden und für die in der Vereinbarung genannten Zwecke erforderlich sind.

4. Zulässige Zwecke

NinjaOne kann Daten gemäß den in der Vereinbarung und in der DPA festgelegten Zwecken verarbeiten.

5. Dauer

Die Dauer der Verarbeitung ist auf die Dauer beschränkt, die für die Erfüllung der Verpflichtungen aus der Vereinbarung erforderlich ist, es sei denn, dies ist gesetzlich vorgeschrieben. Die Verpflichtungen von NinjaOne in Bezug auf die Datenverarbeitung bestehen in jedem Fall fort, bis die Daten ordnungsgemäß gelöscht oder auf Verlangen des Kunden zurückgegeben worden sind.

Zeitplan 2:
Technische und organisatorische Maßnahmen (TOM)

Zu den organisatorischen und technischen Maßnahmen in Bezug auf den Datenschutz gehören unter anderem:

- Überprüfung und Auditierung von Anbietern hinsichtlich der Datenschutzstandards
- Geprüfte physische, virtuelle und organisatorische Zugangskontrolle
- Prüfung des Datenzugriffsverhaltens der Mitarbeiter
- Schutz der Daten durch physische und virtuelle Sicherheitssysteme
- Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit von TOMs
- Anonymisierung von Daten in bestimmten Prozessen, in denen keine Personenbezogenen Daten benötigt werden
- Verschlüsselung bestimmter Datenströme mit FIPS 140-2-konformen kryptografischen Modellen
- 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 insgesamt 150) Einzelkontrollen, die sich mit der ISO27001-Norm überschneiden
- Konformitäts- und Sicherheitskontrollen, die sich auf die folgenden Rahmenwerke und Leitlinien stützen (auf nicht zertifizierter Basis):
    - NIST Cyber Security Framework Revision 1.1
    - U.S.-Verteidigungsministerium DFARS 252.204-712
    - NIST Sonderveröffentlichung 800-171 Revision 2
    - NIST Sonderveröffentlichung 800-53 Revision 5
    - United States Cybersecurity Maturity Model Certification (CMMC) Level 3.

STANDARDVERTRAGSKLAUSELN

Modul Drei: Übermittlung von Auftragsverarbeiter 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 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g
  (iii) Klausel 9 Buchstaben a, c, d und e
  (iv) Klausel 12 Buchstaben a, d und f
  (v) Klausel 13
  (vi) Klausel 15.1 Buchstaben c, d und e
  (vii) Klausel 16 Buchstabe e
  (viii) Klausel 18 Buchstaben a und b

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

Klausel 4
Auslegung

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

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

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

Klausel 5
Vorrang

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

Klausel 6
Beschreibung der Datenübermittlung(en)

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

Klausel 7 (fakultativ)
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 Übermittlungszweck(e), sofern keine weiteren Weisungen seitens des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, oder seitens des Datenexporteurs bestehen.

8.3. Transparenz

Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen.

8.4. Richtigkeit

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

8.5. Dauer der Verarbeitung und Löschung oder Rückgabe der Daten

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

8.6. Sicherheit der Verarbeitung

(a) Der Datenimporteur und, während der Datenübermittlung, auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu diesen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffene Person gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann. Im Falle einer Pseudonymisierung verbleiben die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, soweit möglich, unter der ausschließlichen Kontrolle des Datenexporteurs oder des Verantwortlichen. Zur Erfüllung seinen Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

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

angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

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

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

8.7. Sensible Daten

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

8.8. Weiterübermittlungen

Der Datenimporteur gibt die personenbezogenen Daten nur auf der Grundlage dokumentierter Weisungen des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, an Dritte weiter. Die Daten dürfen zudem nur an Dritte weitergegeben werden, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union[2] 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,

[2] Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

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

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

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

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

8.9. Dokumentation und Einhaltung der Klauseln

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

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

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

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

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

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

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

Klausel 9

Einsatz von Unterauftragsverarbeitern

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

unterrichtet den Datenexporteur über die Beauftragung des/der Unterauftragsverarbeiter/s.

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

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

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

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

Klausel 10
Rechte betroffener Personen

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

(b) Der Datenimporteur unterstützt den Verantwortlichen, gegebenenfalls in Zusammenarbeit mit dem Datenexporteur, bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 zu beantworten. Zu diesem Zweck legen die Parteien in Anhang II unter Berücksichtigung der Art der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen, durch die Unterstützung geleistet wird, sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

(c) Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Datenimporteur die Weisungen des Verantwortlichen, die ihm vom Datenexporteur übermittelt wurden.

Klausel 11
Rechtsbehelf

(a) Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht

zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

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

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

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

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

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

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

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

Klausel 12
Haftung

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

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

(c) Ungeachtet von Buchstabe b haftet der Datenimporteur gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenexporteur oder der Datenimporteur (oder dessen Unterauftragsverarbeiter) der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs und, sofern der Datenexporteur ein im Auftrag eines Verantwortlichen handelnder Auftragsverarbeiter ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.

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

(e) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge

eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

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

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

Klausel 13
Aufsicht

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

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

[*Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 2 der Verordnung (EU) 2016/679 benennen zu müssen:*] Die Aufsichtsbehörde eines der Mitgliedstaaten, in denen die betroffenen Personen niedergelassen sind, deren personenbezogene Daten gemäß diesen Klauseln im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen übermittelt werden oder deren Verhalten beobachtet wird, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

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

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. Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.

(f) Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen, gegebenenfalls in Absprache mit dem Verantwortlichen. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er vom Verantwortlichen oder von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben d und e Anwendung.

Klausel 15

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

15.1 Benachrichtigung

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

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

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

Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.

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

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

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

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

15.2 Überprüfung der Rechtmäßigkeit und Datenminimierung

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

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

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

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 und den Verantwortlichen über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

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

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

Klausel 17

Anwendbares Recht

Diese Klauseln unterliegen dem Recht eines der EU-Mitgliedstaaten, sofern dieses Recht 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.

ANHANG

ANLAGE I

A. LISTE DER PARTEIEN

Datenexporteur(e)	
Name	
Adresse	
Name, Position und Kontaktdaten der Kontaktperson	
Datenschutzbeauftragter	
Für die Datenübermittlung relevante Aktivitäten	
Rolle	Auftragsverarbeiter

Datum

Unterschrift

Datenimporteur(e)	
Name	NinjaOne, LLC
Adresse	Suite 200, 3687 Tampa Road, Oldsmar, Florida, 34677, Vereinigte Staaten von Amerika
Name, Position und Kontaktdaten der Kontaktperson	Mike Arrowsmith Chief Trust Office privacyteam@ninjaone.com
Datenschutzbeauftragter	Mike Arrowsmith
Für die Datenübermittlung relevante Aktivitäten	Der Datenimporteur stellt dem Datenexporteur die Dienstleistung gemäß der Vereinbarung zur Verfügung.
Rolle	Auftragsverarbeiter

8/18/2023	8/18/2023
Datum	Unterschrift

B. BESCHREIBUNG DER ÜBERMITTLUNG

Kategorien von betroffenen Personen, deren personenbezogene Daten übermittelt werden	Betroffene Personen sind die Personen, deren Daten vom Unterauftragsverarbeiter verarbeitet werden, und können Endnutzer oder Mitarbeiter und Angestellte des Auftragsverarbeiters sein.
Kategorien der übermittelten personenbezogenen Daten	Personenbezogene Daten, die der Verantwortliche dem Auftragsverarbeiter direkt oder indirekt durch die Nutzung der SaaS-basierten mandantenfähigen RMM-Plattform und der technischen Supportdienste von NinjaOne (zusammenfassend als "Dienstleistung" bezeichnet) zur Verfügung stellt und die, soweit es sich um personenbezogene Daten handelt, hauptsächlich aus den folgenden Daten bestehen: IP-Adressen und andere technische Details in Bezug auf Endnutzergeräte, Dateinamen, Ordnernamen und beliebige Inhalte von Dateien, die der Auftragsverarbeiter im Rahmen der Dienstleistung übermittelt
Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Sicherheitsvorkehrungen	n/a
Häufigkeit der Übermittlung	Kontinuierlich
Art der Verarbeitung	Die Art der Verarbeitung ist die Verarbeitung von Daten zur Erbringung der Dienstleistung für den Auftragsverarbeiter.
Zweck(e) der Datenübermittlung und Weiterverarbeitung	Der Unterauftragsverarbeiter darf Daten nur verarbeiten, um den Dienst zu erbringen.
Zeitraum, für den die personenbezogenen Daten aufbewahrt werden, oder Kriterien für die Festlegung dieses Zeitraums	Die Dauer der Verarbeitung ist auf die Dauer beschränkt, die für die Erfüllung der Verpflichtungen aus dem Vertrag erforderlich ist, es sei denn, es besteht eine gesetzliche Verpflichtung. Die Verpflichtungen des Unterauftragsverarbeiters in Bezug auf die Datenverarbeitung bestehen in jedem Fall fort, bis die Daten ordnungsgemäß gelöscht oder auf Ersuchen des Auftragsverarbeiters zurückgegeben worden sind.
Bei Übermittlung an (Unter-)Verarbeiter: Gegenstand, Art und Dauer der Verarbeitung	Wie oben beschrieben.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

[Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13]

ANLAGE II

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

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

Maßnahmen zur Pseudonymisierung und Verschlüsselung von personenbezogenen 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 NinjaOne Agent und der NinjaOne Plattform übertragen werden, werden FIPS 140-2 konforme kryptographische Module mittels TLS Verschlüsselung eingesetzt o Im Einzelnen handelt es sich bei allen Verschlüsselungen um Perfect-Forward Secrecy (PFS) mit der folgenden Kryptographie: ▪ ECDHE RSA mit AES128-GCM und SHA256 ▪ ECDHE RSA mit AES128-CBC und SHA256 ▪ ECDHE RSA mit AES128-CBC und SHA ▪ ECDHE RSA mit AES256-GCM und SHA384

	▪ ECDHE RSA mit AES256-CBC und SHA384 ▪ ECDHE RSA mit AES256-CBC und SHA o Für gespeicherte Daten im Backend der NinjaOne-Plattform werden FIPS 140-2-konforme kryptografische Module für die Verschlüsselung im Speicher verwendet. Die Daten werden mit einer Mindeststufe von AES256 verschlüsselt, wobei je nach Bedarf auch eine stärkere Kryptographie verwendet werden kann.
Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit von Verarbeitungssystemen und -diensten	• 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 Oktober 2011 • *Disaster Recovery with Amazon Web Services: A Technical Guide*, Accenture Juni 2016 • *Architecting for the Cloud: AWS Best Practices*, AWS Oktober 2018 • *AWS Well-Architected Framework*, AWS Juli 2019 • *Affordable Enterprise-Grade Disaster Recovery Using AWS*, CloudEndure/AWS 2019 • Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Berichtswege, Notfallpläne
Maßnahmen zur Gewährleistung der Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen	• *Using Amazon Web Services for Disaster Recovery*, AWS Oktober 2011 • *Disaster Recovery with Amazon Web Services: A Technical Guide*, Accenture June 2016 • *Architecting for the Cloud: AWS Best Practices*, AWS Oktober 2018 • *AWS Well-Architected Framework*, AWS Juli 2019 • *Affordable Enterprise-Grade Disaster Recovery Using AWS*, CloudEndure/AWS 2019 • Sicherung (online/offline; vor Ort/außer Haus), schnelle Wiederherstellbarkeit
Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen	• 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* • Datenschutzmanagement, Incident Response Management, Auftragskontrolle (klare Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl von Dienstleistern, Nachkontrollen)
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
Maßnahmen zum Schutz der Daten bei 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 Daten, die zwischen dem NinjaOne Agent und der NinjaOne Plattform übertragen werden, werden FIPS 140-2

	konforme kryptographische Module über TLS Verschlüsselung eingesetzt. o Im Einzelnen handelt es sich bei allen Verschlüsselungen um Perfect-Forward Secrecy (PFS) mit der folgenden Kryptographie: ▪ ECDHE RSA mit AES128-GCM und SHA256 ▪ ECDHE RSA mit AES128-CBC und SHA256 ▪ ECDHE RSA mit AES128-CBC und SHA ▪ ECDHE RSA mit AES256-GCM und SHA384 ▪ ECDHE RSA mit AES256-CBC und SHA384 ▪ ECDHE RSA mit AES256-CBC und 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 gespeicherte Daten im Backend der NinjaOne-Plattform werden FIPS 140-2-konforme kryptografische Module für die Verschlüsselung im Speicher verwendet. Die Daten werden mit einer Mindeststufe von AES256 verschlüsselt, wobei je nach Bedarf auch eine stärkere Kryptographie verwendet werden kann. • Mandantenfähigkeit, Sandboxing, Physikalisch getrennte Speicherung auf separaten Ordnerstrukturen, Mandantentrennung, Autorisierungskonzepte, Datenbankrechte
Maßnahmen zur Gewährleistung der physischen Sicherheit der Orte, an denen personenbezogene Daten verarbeitet werden	• NIST SP # 800-30, *Guide for Conducting Risk Assessments* • NIST SP # 800-39, *Managing Information 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* Außerdem kontrolliert NinjaOne den physischen Zugang durch: 1. Bereitstellung von Anwendungen und Backend-Systemen bei sicheren, geprüften und angesehenen Cloud-Service-Anbietern und nicht auf einem NinjaOne-eigenen Server. 2. Beschränkung des Zugangs zu den NinjaOne-Büros auf Mitarbeiter, Auftragnehmer und eingeladene Gäste (nicht eingeladene Gäste werden gebeten, das Gebäude zu verlassen oder einen späteren Besuch zu vereinbaren, wenn dies erforderlich ist). 3. Professionelle Verwaltung der NinjaOne-Büros durch geprüfte Vermieter und Hausverwaltungsfirmen. 4. Die Verwendung von Schlüsseln, Schlüsselkarten, elektronischen Schlüsselanhängern oder Token für mobile Geräte für den Zugang zu NinjaOne-Büros. 5. Festlegung eines Büroleiters für jedes NinjaOne-Büro, wobei der jeweilige NinjaOne-Büroleiter alle Schlüssel, Schlüsselkarten und Anhänger inventarisiert, ausgibt und verwaltet und alle Zuweisungen von Schlüsseln und Anhängern in einem offiziellen Protokoll festhält. 6. Anforderung, dass verlorene oder gestohlene Schlüssel, Schlüsselkarten oder Anhänger unverzüglich dem Büroleiter von NinjaOne gemeldet werden müssen, woraufhin die Schlüssel, Schlüsselkarten oder Anhänger gesperrt werden. 7. Es wird verlangt, dass eingeladene Besucher von NinjaOne sich beim Büroleiter von NinjaOne melden müssen, der ein offizielles Besucherprotokoll führt,

	in dem der Name des Besuchers, die Identifikationsnummer, die Organisation, der Zweck des Besuchs sowie das Datum und die Uhrzeit des Besuchs festgehalten werden. 8. Die Anforderung, dass alle eingeladenen Besucher durch das Büro begleitet werden müssen. 9. Anforderung, dass alle Besucherausweise am Ende des Tages, am Tag der Ausstellung, ablaufen. 10. Es wird verlangt, dass alle NinjaOne-Mitarbeiter alle Anstrengungen unternehmen, um eine geordnete Arbeitsumgebung zu schaffen, die frei von Unordnung ist und in der keine geschützten oder sensiblen Informationen offengelegt werden. 11. Die Anforderung, dass ungenutzte Akten in Gemeinschaftsbereichen am Ende des Tages geschreddert oder in einem Aktenschrank eingeschlossen werden. 12. Aufzeichnung des Ein- und Ausgangs aller Besucher und Mitarbeiter durch eine der verfügbaren Türen und Aufbewahrung dieser Aufzeichnungen für mindestens 30 Tage. 13. Unverzüglicher Entzug aller Schlüsselkarten, Token und des physischen Zugangs für alle Mitarbeiter, die das Unternehmen auf eigenen Wunsch verlassen haben oder entlassen worden sind.
Maßnahmen zur Sicherstellung der Ereignisprotokollierung	• 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)* Des Weiteren stellt NinjaOne sicher: 1. Nutzung eines 24x7 Security Operations Center durch einen branchenweit

	vertrauenswürdigen externen Sicherheitsdienstleister. 2. Einsatz von Echtzeit-Überwachung, Auditing und Alarmierung von: a. Netzwerkeingang b. Netzwerk-Ausgang c. Dateiveränderungen d. Konfigurationsänderungen e. erfolgreiche und fehlgeschlagene Anmeldungen f. Befehlsausführung g. Ausführung von Anwendungen h. privilegierte Ausführung i. Schwachstellen im Betriebssystem j. Software k. Sicherheitslücken l. Richtlinienänderungen m. völlig neue Aktivität n. atypische Aktivitäten 3. Aufbewahrung der Protokolle und der erfassten Ereignisse für mindestens ein Jahr und, falls erforderlich, bis zu einem unbestimmten Zeitraum.
Maßnahmen zur Sicherstellung 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 zur internen IT- und IT-Sicherheitssteuerung und -verwaltung	• 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/Absicherung von Prozessen und Produkten	Jährliche Prüfungen und Tests von Compliance- und Sicherheitskontrollen im Rahmen des AICPA Service Organization Control (SOC 2)-Prozesses zur Prüfung der Trust Service Principles. Die AICPA SOC 2-Prüfung umfasst 144 [von 150] Einzelkontrollen, die sich mit der ISO27001-Norm überschneiden.
Maßnahmen zur Gewährleistung der Datensparsamkeit	• 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 Sicherung der Datenqualität	• 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 einer begrenzten Datenspeicherung	• 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 Oktober 2011 • *Disaster Recovery with Amazon Web Services: A Technical Guide*, Accenture Juni 2016 • *Architecting for the Cloud: AWS Best Practices*, AWS Oktober 2018 • *AWS Well-Architected Framework*, AWS Juli 2019 • *Affordable Enterprise-Grade Disaster Recovery Using AWS*, CloudEndure/AWS 2019
Maßnahmen zur Gewährleistung der Verantwortlichkeit	• 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 von 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* • 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 NinjaOne Agent und der NinjaOne Plattform übertragen werden, werden FIPS 140-2 konforme kryptographische Module mittels TLS Verschlüsselung eingesetzt o Im Einzelnen handelt es sich bei allen Verschlüsselungen um Perfect-Forward Secrecy (PFS) mit der folgenden Kryptographie: ▪ ECDHE RSA mit AES128-GCM und SHA256 ▪ ECDHE RSA mit AES128-CBC und SHA256 ▪ ECDHE RSA mit AES128-CBC und SHA ▪ ECDHE RSA mit AES256-GCM und SHA384 ▪ ECDHE RSA mit AES256-CBC und SHA384 ▪ ECDHE RSA mit AES256-CBC und SHA • Für gespeicherte Daten im Backend der NinjaOne-Plattform werden FIPS 140-2-konforme kryptografische Module für die Verschlüsselung im Speicher verwendet. • Die Daten werden mit einer Mindeststufe von AES256 verschlüsselt, wobei je nach Bedarf auch eine stärkere Kryptographie verwendet 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 Übermittlungen an (Unter-) Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-) Auftragsverarbeiter ergreifen muss, um den für die Verarbeitung Verantwortlichen und - bei Übermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter - den Datenexporteur unterstützen zu können	• 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*

ANLAGE III – LISTE DER UNTERAUFTRAGSVERARBEITER

Für die Unterauftragsverarbeiter sehen Sie bitte die weiteren Informationen unter Ziffer 4.4. lit. c in der Datenverarbeitungsvereinbarung.