VERTRAG ZUR AUFTRAGSVERARBEITUNG VON IVANTI

Dieser Vertrag zur Auftragsverarbeitung von Ivanti („DPA“) ist Teil der Endnutzerlizenz- und Dienstleistungsvereinbarung von Ivanti („Vereinbarung“) und wurde zwischen dem unten oder in der Vereinbarung angegebenen Kunden („Datenverantwortlicher“) und der jeweiligen, in diesem DPA angegebenen Geschäftseinheit von Ivanti („Ivanti“ oder „Auftragsverarbeiter“) zum Zeitpunkt der letzten Unterzeichnung angenommen und geschlossen (das „Wirksamkeitsdatum“) (einzeln als „Partei“ und gemeinsam als die „Parteien“ bezeichnet). Alle in diesem Dokument nicht definierten, großgeschriebenen Begriffsbestimmungen haben dieselbe Bedeutung wie die in der Vereinbarung.

PRÄAMBEL

IN ERWÄGUNG DESSEN, DASS der Auftragsverarbeiter personenbezogene Daten im Auftrag des Datenverantwortlichen im Zuge der Erbringung der Dienstleistungen im Rahmen der Vereinbarung verarbeiten darf,

IN ERWÄGUNG DESSEN, DASS angemessene Garantien in Bezug auf die Verarbeitung der von dem Datenverantwortlichen an den Auftragsverarbeiter bereitgestellten personenbezogenen Daten gewährt werden, vereinbaren die Parteien, den folgenden Bestimmungen in Bezug auf die personenbezogenen Daten zu entsprechen und jede für sich vernünftig und im guten Glauben zu handeln und haben die Parteien die Vereinbarung geschlossen.

AUFGRUNDDESSEN und unter Berücksichtigung der vorstehenden Voraussetzungen, der gegenseitigen Zusicherungen und der unten aufgeführten Vertragsabreden vereinbaren der Datenverantwortliche und der Auftragsverarbeiter Folgendes:

VEREINBARUNG

1. BEGRIFFSBESTIMMUNGEN

Sämtliche großgeschriebene Begriffsbestimmungen, die nicht in diesem Nachtrag definiert werden, haben die in der Vereinbarung genannte Bedeutung.

„Verbundenes Unternehmen”: eine juristische Person, die direkt oder indirekt die betreffende juristische Person beherrscht, von dieser beherrscht wird oder unter dem gemeinsamen beherrschenden Einfluss mit der betreffenden juristischen Person steht. Zum Zwecke dieser Begriffsbestimmung bedeutet „beherrschender Einfluss” die direkte oder indirekte Beteiligung an oder der Einfluss auf mehr als 50 % der stimmberechtigten Anteile der betreffenden juristischen Person.

„Geltendes Datenschutzrecht”: Hierunter werden alle geltenden Gesetze, Vorschriften, behördlichen Leitlinien oder Anforderungen in einer Gerichtsbarkeit verstanden, die sich auf den Datenschutz, die Privatsphäre oder die Vertraulichkeit von personenbezogenen Daten beziehen, einschließlich, jedoch nicht beschränkt auf (a) die DSGVO in Verbindung mit etwaigen Rechtsvorschriften zur Umsetzung, Durchführung und Ergänzung und (b) der CCPA.

„Ermächtigtes verbundenes Unternehmen”: verbundene Unternehmen des Datenverantwortlichen, die (a) den Datenschutzgesetzen und -vorschriften des Europäischen Wirtschaftsraums bzw. seiner Mitgliedsstaaten, dem Vereinigten Königreich oder der Schweiz unterliegen, (b) den Datenschutzgesetzen und -vorschriften außerhalb des Europäischen Wirtschaftsraums bzw. seiner Mitgliedsstaaten, der Schweiz oder des Vereinigten Königreichs (falls zutreffend) unterliegen und (c) zur Beauftragung des Auftragsverarbeiters zur Datenverarbeitung im Rahmen dieser Vereinbarung befugt sind.

„CCPA”: Der California Consumer Privacy Act, Cal. Civ. Code [Kalifornisches Zivilgesetzbuch] § 1798.100 ff. und seine Durchführungsbestimmungen.

„Datenverantwortlicher”: die Geschäftseinheit, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt. Zur Klarstellung ist die oben als „Datenverantwortlicher“ bezeichnete Partei der Datenverantwortliche im Rahmen dieses DPA.

„Datenschutzverletzung”: eine Verletzung des Datenschutzes, die zu einer versehentlichen, unbefugten oder rechtswidrigen Zerstörung, dem Verlust, einer Änderung, Offenlegung von oder dem Zugang zu Daten oder einer Verarbeitung von personenbezogenen Daten geführt hat, die übertragen, gespeichert oder auf sonstige Art und Weise verarbeitet wurden.

„Datenschutzaufsichtsbehörde”: ein Vertreter oder ein Regierungsbeauftragter einer Regierungsbehörde oder einer staatlichen Stelle, die die Befugnis hat, das geltende Datenschutzrecht durchzusetzen.

„Betroffene Person”: eine natürliche Person, auf die sich die personenbezogenen Daten beziehen.

„DSGVO“: Unter der DSGVO wird die 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/EC (Datenschutz-Grundverordnung) verstanden.

„Ivanti”: Die nachfolgend aufgeführte Geschäftseinheit, die sich in derselben geografischen Region wie der Kunde befindet:

- Ivanti, Inc., eine nach dem Recht des Bundesstaates Delaware gegründete Kapitalgesellschaft, niedergelassen in Nord- und Südamerika, mit Ausnahme von Brasilien.
- Ivanti Comércio de Software Brasil Ltda, eine brasilianische Gesellschaft mit Sitz in Brasilien.
- Ivanti Software K.K., eine japanische Gesellschaft mit Sitz in Japan.
- Ivanti Software Technology (Beijing) Co., Ltd., eine chinesische Gesellschaft mit Sitz in China.
- Ivanti International Limited, ein Unternehmen nach irischem Recht, für Produkte und Dienstleistungen der Marken Wavelink und Naurtech in Europa, dem Nahen Osten, Afrika und der Region Asien-Pazifik.
- Ivanti UK Limited, eine Gesellschaft mit beschränkter Haftung, eingetragen in England und Wales, an allen sonstigen Standorten.

„Personenbezogene Daten”: Alle Informationen, die direkt oder indirekt eine natürliche Person oder einen bestimmten Haushalt identifizieren oder mit diesen identifiziert werden können, sich auf diese beziehen, diese beschreiben, mit diesen in Verbindung gebracht werden oder vernünftigerweise mit ihnen verbunden werden können. Eine identifizierbare natürliche Person ist jemand, der direkt oder indirekt identifiziert werden kann, insbesondere mittels Zuweisung zu einer Kennung wie einem Namen, einer Ausweisnummer, Standortdaten, einer Onlinekennung oder einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person.

„Verarbeitung”: Jeder Vorgang oder eine Abfolge von Vorgängen, der bzw. die sich auf personenbezogene Daten bezieht und von oder im Zusammenhang mit und zum Zweck der Erbringung von Dienstleistungen, die mit oder ohne Hilfe automatisierter Verfahren wie der Erhebung, Erfassung, Organisation, Speicherung, Anpassung oder Veränderung, dem Auslesen, dem Abfragen, der Verwendung, der Offenlegung durch Übermittlung, der Verbreitung oder einer sonstigen Art der Bereitstellung, dem Abgleich oder der Verknüpfung, der Einschränkung, dem Löschen oder der Vernichtung gemäß geltenden Datenschutzrechts erfolgt.

„Auftragsverarbeiter”: eine juristische Person, die personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet. Zur Klarstellung ist die als „Auftragsverarbeiter“ identifizierte Partei ein Auftragsverarbeiter im Sinne dieses DPA.

„Dienstleistungen”: die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Zusammenhang mit und zum Zweck der Erbringung der Dienstleistungen, die vom Auftragsverarbeiter der Vereinbarung gemäß erfolgt.

„Dienstleister”: ein Einzelunternehmen, eine Personengesellschaft, eine Gesellschaft mit beschränkter Haftung, eine Kapitalgesellschaft, eine Vereinigung oder eine sonstige juristische Person, das bzw. die zum Gewinn oder zum finanziellen Nutzen ihrer Aktionäre oder sonstigen Anteilhaber bzw. Mitglieder organisiert oder betrieben wird und Daten im Auftrag eines Datenverantwortlichen verarbeitet und an das bzw. die der Datenverantwortliche personenbezogene Daten einer betroffenen Person zu einem geschäftlichen Zweck eines schriftlichen Vertrags gemäß zur Verarbeitung offenlegt, vorausgesetzt, dass der Vertrag es dem Dienstleister untersagt, die personenbezogenen Daten zu einem anderen Zweck als dem in dem Vertrag vereinbarten spezifischen Zweck oder der Erbringung der Dienstleistungen oder auf sonstige, von dem CCPA zugelassene Weise die personenbezogenen Daten zurückzuhalten, zu verwenden oder offenzulegen, einschließlich der Zurückbehaltung, der Nutzung oder der Offenlegung der personenbezogenen Daten zu einem gewerblichen Zweck, bei dem es sich nicht um die im Vertrag mit dem Datenverantwortlichen festgelegten Dienstleistungen handelt. Die Begriffe „geschäftlicher Zweck” und „gewerblicher Zweck” entsprechen dabei den in dem CCPA verwandten Begriffsbestimmungen. Zur Klarstellung handelt es sich bei dem Auftragsverarbeiter um einen Dienstleister.

„Unterauftragsverarbeiter”: jede juristische Person, die personenbezogene Daten im Auftrag des Auftragsverarbeiters verarbeitet.

2. VERARBEITUNG VON PERSONENBEZOGENEN DATEN

2.1 Aufgaben der Parteien. Die Parteien erkennen an und vereinbaren, dass im vorliegenden Fall der Datenverantwortliche der Datenverantwortliche im Sinne dieses Nachtrags und der Auftragsverarbeiter der Auftragsbearbeiter oder Dienstleister im Sinne dieses Nachtrags für die Verarbeitung der personenbezogenen Daten ist. Gegenstand, Dauer, Zweck der Verarbeitung und die Arten der personenbezogenen Daten und Kategorien der betroffenen Personen, die im Rahmen dieses DPA verarbeitet werden, sind weiter in Anhang 1 festgelegt.

2.2 Pflichten des Datenverantwortlichen. Die Anweisungen des Datenverantwortlichen zur Verarbeitung personenbezogener Daten entspricht den Datenschutzgesetzen und -vorschriften. Der Datenverantwortliche trägt die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Daten und die Mittel, mit denen der Datenverantwortliche die personenbezogenen Daten bezieht und sie dem Auftragsverarbeiter weitergibt.

2.3 Pflichten des Auftragsverarbeiters. Bei sämtlichen personenbezogenen Daten, die vom Auftragsverarbeiter im Rahmen dieser Vereinbarung verarbeitet werden, handelt es sich um vertrauliche Informationen und der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich den in Anhang 1 dokumentierten Anweisungen gemäß oder auf sonstige, durch den Datenverantwortlichen schriftlich mitgeteilte Weise. Der Auftragsverarbeiter verkauft die im Rahmen dieses DPA verarbeiteten personenbezogenen Daten nicht und wird diese weder speichern, noch nutzen oder personenbezogene Daten außerhalb der direkten Geschäftsbeziehung zwischen dem Auftragsverarbeiter und dem Datenverantwortlichen offenlegen. Der Auftragsverarbeiter entspricht im Zusammenhang mit der Verarbeitung von personenbezogenen Daten sämtlichem geltenden Datenschutzrecht. Der Auftragsverarbeiter wird die vom Datenverantwortlichen bereitgestellten personenbezogenen Daten nicht mit Daten kombinieren, die er aus sonstigen quellen erhält. Sollte der Auftragsverarbeiter der Auffassung sein, dass die Befolgung der Anweisungen des Datenverantwortlichen zu einer Verletzung geltenden Datenschutzrechts führt, teilt der Auftragsverarbeiter dem Datenverantwortlichen dies unverzüglich schriftlich mit. Der Auftragsverarbeiter stellt dem Datenverantwortlichen daraufhin sämtliche erforderlichen Informationen zur Verfügung, die belegen, wie der Auftragsverarbeiter seinen Pflichten im Rahmen dieses DPA entspricht.

2.3.1. Anforderungen an die Zusammenarbeit. Der Auftragsverarbeiter unterstützt den Datenverantwortlichen bei: der Beachtung geltenden Datenschutzrechts; vermuteten und relevanten Datenschutzverletzungen, Mitteilungen an oder Aufforderungen von einer Datenschutzbehörde, Mitteilungen an als auch Aufforderungen von betroffenen Personen und der Pflicht des Datenverantwortlichen zur Durchführung von Datenschutz-Folgenabschätzungen und vorherigen Konsultationen mit einer Datenschutzbehörde.

3. MITTEILUNGSPFLICHTEN

3.1 Mitteilungspflichten des Auftragsverarbeiters. Der Auftragsverarbeiter teilt dem Datenverantwortlichen unverzüglich und schriftlich Folgendes mit:

3.1.1 eine Aufforderung einer betroffenen Person zur Ausübung ihrer Datenschutzrechte wie dem Recht zur Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, dem Widerspruch oder der Einschränkung ihrer personenbezogenen Daten;

3.1.2 eine von den Kunden oder Mitarbeitern des Datenverantwortlichen erhaltene Anfrage oder Beschwerde;

3.1.3 eine Frage, Beschwerde, Ermittlung oder sonstige Erhebung einer Datenschutzbehörde;

3.1.4 eine Aufforderung zur Offenlegung personenbezogener Daten, die sich auf die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen dieses DPA bezieht;

3.1.5 eine Verletzung des Schutzes personenbezogener Daten im Sinne der Mitteilungspflichten gemäß Artikel 7.1 und

3.1.6 Wenn die personenbezogenen Daten im Laufe ihrer Verarbeitung Gegenstand einer Untersuchung oder Beschlagnahme, eines Pfändungsbeschlusses, einer Einziehung im Rahmen eines Konkurs- oder Insolvenzverfahrens oder sonstiger Ereignisse oder Maßnahmen Dritter werden.

Der Auftragsverarbeiter unterstützt den Datenverantwortlichen bei der Erfüllung seiner Pflichten, um auf Aufforderungen bzw. Anfragen gemäß den Artikeln (3.1.1) - (3.1.6) oben zu reagieren und der Auftragsverarbeiter wird nicht auf diese Aufforderungen bzw. Anfragen ohne die vorherige schriftliche Zustimmung des Datenverantwortlichen reagieren, sofern der Auftragsverarbeiter dazu nicht gesetzlich verpflichtet ist.

4. VERTRAULICHKEIT

4.1 Vertrauliche Informationen. Sämtliche, dem Auftragsverarbeiter im Rahmen dieser Vereinbarung zur Verfügung gestellten Informationen sind vertraulich.

4.2 Mitarbeiter des Auftragsverarbeiters. Der Auftragsverarbeiter stellt sicher, dass seine an der Verarbeitung von personenbezogenen Daten beteiligten Mitarbeiter über die Vertraulichkeit der personenbezogenen Daten informiert sind, eine angemessene Einführung zu ihren Verantwortlichkeiten erhalten und schriftliche Vertraulichkeitsvereinbarungen unterzeichnet haben. Der Auftragsverarbeiter garantiert ebenso, dass diese Vertraulichkeitspflichten auch nach der Beendigung des jeweiligen Beschäftigungsverhältnisses mit diesen Mitarbeitern fortdauern.

4.3 Einschränkung des Zugangs. Der Auftragsverarbeiter garantiert, dass der Zugang zu den personenbezogenen Daten für die Mitarbeiter, die Dienstleistungen im Rahmen dieser Vereinbarung ausführen, eingeschränkt ist.

5. UNTERAUFTRAGSVERARBEITER

5.1 Ernennung von Unterauftragsverarbeitern. Der Datenverantwortliche erkennt an und stimmt zu, dass der Auftragsverarbeiter und die verbundenen Unternehmen des Auftragsverarbeiters im Zusammenhang mit der Erbringung der Dienstleistungen Dritt-Unterauftragsverarbeiter beauftragen dürfen. Der Auftragsverarbeiter und seine verbundenen Unternehmen schließen einen schriftlichen Vertrag, der für jeden Unterauftragsverarbeiter Pflichten zum Datenschutz enthält, die keinen geringeren Datenschutz bieten als die Pflichten in diesem DPA, sofern dieser auf die Natur der vom Unterauftragsverarbeiter erbrachten Dienstleistung anwendbar ist. Der Datenverantwortliche ermächtigt hiermit den Auftragsverarbeiter, die auf seiner der Liste aufgeführten Unterauftragsverarbeiter gemäß der Aufführung auf https://www.ivanti.com/company/legal/ivanti-subprocessors zur Verarbeitung der personenbezogenen Daten gemäß dieses DPA zu beauftragen. Der Datenverantwortliche kommuniziert nicht direkt mit den Unterauftragsverarbeitern des Auftragsverarbeiters über die Dienstleistungen, sofern dies nicht mit dem Auftragsverarbeiter in dessen Ermessen zuvor vereinbart wurde.

5.2 Mitteilung von Änderungen der Unterauftragsverarbeiter. Der Auftragsverarbeiter informiert den Datenverantwortlichen über beabsichtigte Änderungen im Zusammenhang mit einer Hinzunahme oder einem Ersatz eines Unterauftragsverarbeiters, indem dem Datenverantwortlichen ein Mechanismus zur Verfügung gestellt wird, sich für Mitteilungen über neue Unterauftragsverarbeiter auf https://www.ivanti.com/company/legal/ivanti-subprocessors anzumelden. Beabsichtigte Änderungen im Zusammenhang mit einer Hinzunahme oder dem Ersatz eines Unterauftragsverarbeiters vor dem Einsatz des Unterauftragsverarbeiters werden dem Datenverantwortlichen durch den Auftragsverarbeiter mitgeteilt.

5.3 Einspruchsrecht für neue Unterauftragsverarbeiter. Der Datenverantwortliche darf angemessener Weise Einspruch gegen den Einsatz eines neuen Unterauftragsverarbeiters durch den Auftragsverarbeiter einlegen, indem er den Auftragsverarbeiter darüber unverzüglich und schriftlich innerhalb von fünfzehn (15) Werktagen nach Erhalt der Mitteilung durch den Auftragsverarbeiter in Kenntnis setzt. Sollte der Datenverantwortliche Einspruch gegen einen neuen Unterauftragsverarbeiter einlegen, dann wird der Auftragsverarbeiter angemessene Anstrengungen unternehmen, um dem Datenverantwortlichen eine Änderung der Dienstleistungen vorzulegen, durch die eine Verarbeitung personenbezogener Daten durch den abgelehnten neuen Unterauftragsverarbeiter vermieden wird. Sollte es dem Auftragsverarbeiter unmöglich sein, eine solche Änderung vorzunehmen, dann kann der Datenverantwortliche die geltende Vereinbarung im Zusammenhang mit diesen Dienstleistungen, die vom Auftragsverarbeiter nicht ohne den Einsatz des abgelehnten Unterauftragsverarbeiter erbracht werden können, beenden.

5.4 Haftung für Handlungen der Unterauftragsverarbeiter. Der Auftragsverarbeiter haftet in demselben Umfang für sämtliche Handlungen und Unterlassungen seiner Unterauftragsverarbeiter, als wenn er die Dienstleistungen jedes Unterauftragsverarbeiters im Rahmen dieses DPA selbst erbringen würde.

6. SICHERHEIT

6.1 Schutz personenbezogener Daten. Der Auftragsverarbeiter führt geeignete technische und organisatorische Maßnahmen zum Schutz der Sicherheit (einschließlich des Schutzes vor unbefugter oder rechtswidriger Verarbeitung von personenbezogenen Daten und vor versehentlicher oder rechtswidriger Zerstörung, Verlust, Veränderung oder Beschädigung, unbefugter Offenlegung von oder Zugang zu personenbezogenen Daten), Vertraulichkeit und Integrität personenbezogener Daten durch.

6.2 Prüfrechte. Der Datenverantwortliche stimmt zu, dass sein Prüfrecht gegenüber dem Auftragsverarbeiter durch die Vorlage von aktuellen Bescheinigungen, Berichten und Auszügen unabhängiger Stellen, einschließlich, jedoch nicht beschränkt auf externe oder interne Prüfer, den Datenschutzbeauftragen des Auftragsverarbeiters, die IT-Sicherheitsabteilung, Datenschutz- bzw. Qualitätsprüfer oder sonstige, im Einvernehmen vereinbarte Dritten oder

durch eine Prüfung der IT-Sicherheit oder des Datenschutzes des Auftragsverarbeiters befriedigt wird. In dem Umfang, in dem es nicht möglich ist, einer durch die geltenden Datenschutzgesetze und -verordnungen vorgeschriebenen Prüfpflicht über derartige Bescheinigungen, Berichte oder Auszüge nachzukommen, hat der Datenverantwortliche oder eine vom Datenverantwortlichen ernannte Person — auf Kosten des Datenverantwortlichen — das Prüf- und Inspektionsrecht im Zusammenhang mit dem Gelände, den Richtlinien, Verfahren und computergestützten Systemen um sicherzustellen, dass der Auftragsverarbeiter den Anforderungen dieses DPA entspricht. Der Datenverantwortliche oder eine vom Datenverantwortlichen ernannte Person benachrichtigt den Auftragsverarbeiter mindestens dreißig (30) Tage vor der Durchführung seiner Prüfung, sofern diese Prüfung nicht aufgrund einer Datenschutzverletzung, an der der Auftragsverarbeiter beteiligt ist, erforderlich ist. Vom Datenverantwortlichen oder der ernannten Person des Datenverantwortlichen durchgeführte Prüfungen verletzen nicht die Vertraulichkeitspflichten des Auftragsverarbeiters gegenüber seinen anderen Kunden. Sämtliche Prüfungen werden während der normalen Geschäftsöffnungszeiten am Geschäftssitz des Auftragsverarbeiters oder sonstiger Standorte des Auftragsverarbeiters durchgeführt, an denen personenbezogene Daten abgerufen, verarbeitet oder verwaltet werden, und werden den üblichen Geschäftsbetrieb des Auftragsverarbeiters nicht stören. Vor Beginn einer solchen Prüfung vereinbaren der Auftragsverarbeiter und der Datenverantwortliche einvernehmlich den Zeitpunkt, den Umfang und die Dauer der Prüfung. Der Datenverantwortliche kann einen bzw. mehrere zusammenfassende(n) Prüfbericht(e) oder eine Prüfung des Auftragsverarbeiters maximal einmal jährlich anfordern.

7. DATENSCHUTZVERLETZUNGEN

7.1 Benachrichtigung über die Datenschutzverletzung. Der Auftragsverarbeiter ist verpflichtet, den Datenverantwortlichen unverzüglich ab dem Bekanntwerden schriftlich über eine vermutliche Datenschutzverletzung zu benachrichtigen. Unter keinen Umständen darf die Benachrichtigung später als 72 Stunden nach der Entdeckung der Datenschutzverletzung durch den Auftragsverarbeiter erfolgen.

7.2 Management von Datenschutzverletzungen. Der Auftragsverarbeiter unternimmt angemessene Anstrengungen, um die Ursache der Datenschutzverletzung zu identifizieren und trifft die Maßnahmen, die der Auftragsverarbeiter für erforderlich und angemessen hält, um der Ursache einer solchen Datenschutzverletzung abzuhelfen, sofern dies im Rahmen des Zumutbaren des Auftragsverarbeiters erfolgt.

8. BEENDIGUNG

8.1 Beendigung. Dieser DPA endet automatisch mit der (a) Beendigung oder dem Ablauf der Vereinbarung oder (b) der Löschung oder Rückgabe der personenbezogenen Daten durch den Auftragsverarbeiter, je nachdem, was später eintritt. Der Datenverantwortliche ist ferner berechtigt, diesen DPA aus wichtigem Grund zu beenden, wenn der Auftragsverarbeiter nach alleiniger Auffassung des Datenverantwortlichen diesen DPA wesentlich oder anhaltend verletzt, was vorliegt, wenn der Auftragsverarbeiter eine abhilfefähige Verletzung nicht innerhalb von zehn (10) Tagen ab dem Empfangsdatum einer Mitteilung einer Datenschutzverletzung des Datenverantwortlichen mit der Aufforderung zur Abhilfe behebt.

8.2 Rückgabe oder Löschung der Daten. Mit der Beendigung dieses DPAs löscht der Auftragsverarbeiter sämtliche existierenden Kopien von personenbezogenen Daten bzw. gibt diese zurück, sofern geltendes Recht es nicht erfordert, die personenbezogenen Daten weiterhin aufzubewahren. Auf Verlangen des Datenverantwortlichen bestätigt der Auftragsverarbeiter die Einhaltung dieser Pflichten schriftlich und löscht sämtliche existierenden Kopien. In Fällen, in denen das lokale Recht den Auftragsverarbeiter verpflichtet, die personenbezogenen Daten aufzubewahren, schützt der Auftragsverarbeiter die Vertraulichkeit, Integrität und Zugänglichkeit der personenbezogenen Daten, wird diese nicht aktiv verarbeiten und entspricht er weiterhin den Bedingungen dieses DPAs.

9. MECHANISMEN FÜR INTERNATIONALE ÜBERMITTLUNGEN

9.1 Übermittlungen an ein Land außerhalb der EU/dem Vereinigten Königreich/der Schweiz mit einem Angemessenheitsbeschluss. Der Verarbeiter stützt sich für die Übermittlung personenbezogener Daten auf einen Angemessenheitsbeschluss, wenn ein solcher Beschluss den geltenden Gesetzen zum Datenschutz gemäß gefasst ist. Sollte der Auftragsverarbeiter gemäß dem Datenschutzrahmenprogramm zertifiziert sein, das durch den Durchführungsbeschluss der Kommission vom 10.7.2023 über das angemessene Schutzniveau personenbezogener Daten im Rahmen des EU-US-Datenschutzrahmens („DPF") angenommen wurde, dann gilt, zur Klarstellung, der DPF und ersetzt sämtliche geltenden Mechanismen zur Datenübermittlung, die in Abschnitt 9.2 dieses Auftragsverarbeitungsvertrags („AVV") als ein gültiger Übermittlungsmechanismus von an die Vereinigten Staaten von Amerika übermittelten personenbezogenen Daten genannt werden.

9.2 Übermittlungen an ein Land außerhalb der EU/des Vereinigten Königreichs/der Schweiz ohne einen Angemessenheitsbeschluss. Im Rahmen der Erbringung von Dienstleistungen gemäß dem AVV kann es für den Verantwortlichen erforderlich sein, personenbezogene Daten von der Europäischen Union, dem Europäischen Wirtschaftsraum bzw. deren Mitgliedsstaaten, der Schweiz oder dem Vereinigten Königreich, an den in einem Land ansässigen Auftragsverarbeiter zu übermitteln, das nicht über einen Angemessenheitsbeschluss verfügt bzw. sich nicht im Europäischen Wirtschaftsraum befindet.

9.2.1. In Bezug auf personenbezogene Daten, die der DSGVO unterliegen (i) ist der Auftragsverarbeiter der „Datenimporteur" und der Datenverantwortliche der „Datenexporteur"; (ii) gelten die Bedingungen des Moduls 2, wenn der Datenverantwortliche ein Datenverantwortlicher im Sinne dieses DPA und der Auftragsverarbeiter ein Datenverarbeiter im Sinne dieses DPA ist; (iii) wird die optionale Verbindungsklausel in Klausel 7 gelöscht; (iv) ist Option 2 von Klausel 9 des Moduls 2 anwendbar und die Liste der Unterauftragsverarbeiter und die Frist für die Mitteilung von Änderungen entspricht der Vereinbarung gemäß Artikel 5 dieses DPA; (v) ist die optionale Regelung in Klausel 11(a) nicht enthalten; (vi) gilt Option 1 in Klausel 17 und die Standardvertragsklauseln unterliegen dem Recht des Mitgliedsstaats, in dem der Datenverantwortliche niedergelassen ist; (vii) werden in Klausel 18 (b) genannte Streitigkeiten vor den Gerichten des Mitgliedsstaates geschlichtet, in dem der Datenverantwortliche niedergelassen ist; (viii) gelten Anlage I und Anlage II jeweils als mit der in Anhang 1 dieses DPA genannten Information vollständig und (ix) haben die Standardvertragsklauseln im Umfang eines Widerspruchs Vorrang, wenn und soweit die Standardvertragsklauseln im Widerspruch zu einer Bestimmung der Vereinbarung (einschließlich dieses DPAs) stehen. Für diesen Artikel werden die Standardvertragsklauseln aus dem Durchführungsbeschluss der Europäischen Kommission (EU) 2021/914 per Verweis in diesem Dokument aufgenommen und sind hier zu finden: Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer | EU-Kommission (europa.eu)

9.2.2. In Bezug auf die personenbezogenen Daten, die dem Datenschutzrecht des Vereinigten Königreichs unterliegen, gilt das Internationale Abkommen über die Datenübermittlung („IDTA") mit den folgenden Modifikationen: (i) die Kontaktinformationen zu den Parteien der Vereinbarung sind gleichzeitig die Kontaktinformationen für das IDTA; (ii) der Datenverantwortliche ist der Datenexporteur und der Auftragsverarbeiter ist der Datenimporteur; (iii) die Gesetze, denen das IDTA unterliegt und der Gerichtsstand, an dem Rechtsansprüche geltend gemacht werden können, sind die von England and Wales; (iv) die Datenschutzgrundverordnung des Vereinigten Königreichs („GDPR") gilt nicht für die Verarbeitung der übermittelten Daten des Datenimporteurs; (v) die Parteien handhaben nicht die zusätzlichen Sicherheits- und Handelsklauseln des IDTA und (vi) die in diesem DPA und dem Anhang 1 enthaltenen Informationen können für die Tabellen 1–4 verwendet werden. Für diesen Artikel werden die Standardvertragsklauseln des Information Commissioner's Office per Verweis in diesem Dokument aufgenommen und sindhier zu finden: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

9.2.3. In Bezug auf die personenbezogenen Daten, die dem Schweizer DPA unterliegen, gelten die in Artikel 9.1.1 verwiesenen Standardvertragsklauseln mit den folgenden Modifikationen (i) Verweise auf die „Verordnung (EU) 2016/679" sind als Verweis auf den Schweizer DPA auszulegen; (ii) Verweise auf „EU-Recht", „Unionsrecht" und das „Recht der Mitgliedsstaaten" sind als Verweise auf Schweizer Recht auszulegen; und (iii) Verweise auf die „zuständige Aufsichtsbehörde" und „zuständigen Gerichte" werden mit dem „Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten" und den „relevanten Gerichten in der Schweiz" ersetzt.

9.3. Alternative Mechanismen zur Datenübermittlung Die Parteien erkennen an, dass sich die Gesetze, Regeln und Vorschriften in Bezug auf internationale Datenübermittlungen rasant entwickeln. Für den Fall, dass der Verantwortliche einen anderen Mechanismus annimmt, der durch geltende Gesetze, Regeln und Vorschriften zur Übermittlung personenbezogener Daten zugelassen ist („jeder für sich ein alternativer Mechanismus zur Datenübermittlung"), vereinbaren die Parteien im guten Glauben zusammenzuarbeiten, um sämtliche, für den alternativen Datenübermittlungsmechanismus erforderlichen Änderungen an diesem AVV umzusetzen.

10. SONSTIGE BESTIMMUNGEN

10.1. Änderungen. Dieser DPA darf weder geändert noch ergänzt werden, noch gelten eine oder alle Bestimmungen als aufgehoben oder auf sonstige Weise geändert, es sei denn per schriftlicher, von den ermächtigten Vertretern beider Parteien ordnungsgemäß ausgeführter Vereinbarung.

10.2 Geltendes Recht. Dieser DPA unterliegt dem geltendes, in dieser Vereinbarung angegebenen Recht.

ZU URKUND DESSEN haben die Parteien diese Vereinbarung in der zum Wirksamkeitsdatum geltenden Fassung ausgeführt.

DATENVERANTWORTLICHER:_____	**IVANTI**
Unterschrift: _____	Unterschrift: _____
Name: _____	Name: _____
Titel: _____	Titel: _____
Datum: _____	Datum: _____

Anhangsverzeichnis:

Anhang 1: Beschreibung der Datenverarbeitung

ANHANG 1

Beschreibung der Datenverarbeitung

Kontaktinformationen Ivanti:

Ivanti

10377 South Jordan Gateway
Suite 110
South Jordan, Utah 84095
USA

Kontakt Datenschutzbeauftragter: privacy@ivanti.com

Gegenstand
Gegenstand der Datenverarbeitung:
Bereitstellung von IT-Softwarelizenzierung, Erbringung von Supportdienstleistungen und deren Umsetzung als On-Premise- oder gehostete SaaS-Lösung zur Verwaltung und Ermöglichung wesentlicher Geschäftsprozesse in den Bereichen Unified Endpoint Management, IT Service Management, IT Asset Management, Sicherheit, Berichte und Analysen sowie der Lieferkette.

Die IT-Dienstleistungen umfassen die Nutzung von Software als On-Premise-Installation oder SaaS-Lösung einschließlich der Installation von Modulen (einschließlich und ohne Einschränkung der Module Incident-, Change-, Asset-, Konfigurations- und Release-Management), Selbstbedienungs- und Servicekataloge, Support- und Instandhaltung, einschließlich und ohne Einschränkung von Remote-Zugriff und Patches, App-Steuerung, Endpoint-/mobile Sicherheits- und Rechteverwaltung.

Datenverarbeitungsfrequenz:
Dauerhaft.

Dauer
Dauer der Datenverarbeitung:
Wie in der Vereinbarung angegeben.

Umfang, Art und Zweck der Datenverarbeitung
Der Umfang, die Art und der Zweck der Datenverarbeitung sind folgendermaßen:
Wie in der Vereinbarung angegeben.

Betroffene Personen
Die Verarbeitung personenbezogener Daten kann sich auf folgende Kategorien betroffener Personen beziehen:
Kunden, Interessenten, Mitarbeiter, Lieferanten, Handelsvertreter, Kontaktpersonen, Auftragnehmer (einschließlich befristet Beschäftigter), Freiwillige, Zeitarbeiter und Gelegenheitsarbeiter, Freiberufler, Agenten, Berater und sonstige Experten und deren Angehörige, Begünstigte und Notfallkontakte, Mitarbeiter, Zeitarbeitskräfte und Kunden, Beschwerdeführer, Korrespondenten und Fragesteller, Berater, und sonstige Fachleute, Mitarbeiter oder Kontaktpersonen der Interessenten, Kunden, Geschäftspartner und Händler des Datenexporteurs, Geschäftspartner und Händler des Datenexporteurs (bei denen es sich um natürliche Personen handelt) und Nutzer des Datenexporteurs, die von diesem zur Nutzung der Software und der Verwandten Dienstleistungen autorisiert wurden.

Datenkategorien
Die verarbeiteten personenbezogenen Daten können die folgenden Datenkategorien betreffen:
In die unter den Kundendiensten und -konten angebotenen Dienstleistungen hochgeladenen Kundendaten.

Technische und organisatorische Maßnahmen
Im Folgenden werden die vom Auftragsverarbeiter umgesetzten technischen und organisatorischen Sicherheitsmaßnahmen beschrieben:

Schulung des Sicherheitsbewusstseins
Der Auftragsverarbeiter wird im Bereich Sicherheitsbewusstseins geschult. Dies umfasst obligatorische Sicherheitsschulungen zu Umgang und Sicherheit von vertraulichen und sensiblen Informationen wie personenbezogenen Daten, Konto- und Gesundheitsdaten, die im Einklang mit geltendem Recht stehen, und regelmäßige Sicherheitskommunikation und Sicherheitskurse, die sich auf den Endbenutzer konzentrieren.

Sicherheitsrichtlinien und -verfahren
Der Auftragsverarbeiter verfügt über Informationssicherheits-, Nutzer- und Managementrichtlinien, die die Handlungen von Mitarbeitern und Auftragnehmern in Bezug auf die angemessene Nutzung, den Zugang zu und die Speicherung von vertraulichen und sensiblen Informationen vorschreiben, Mitarbeitern des Auftragsverarbeiters den Zugang zu vertraulichen und sensiblen Informationen einschränken, auf die sie zur Ausübung ihrer Tätigkeiten zugreifen müssen, verhindern, dass gekündigte Mitarbeiter auf die Informationen des Auftragsverarbeiters nach der Kündigung zugreifen können und verhängen Disziplinarmaßnahmen für die Nichteinhaltung dieser Richtlinien. Der Systemzugriff auf die Ressourcen des Auftragsverarbeiters wird verweigert, sofern der Zugriff nicht ausdrücklich beurteilt und gewährt wird. Im gesetzlich zulässigen Rahmen führt der Auftragsverarbeiter zum Zeitpunkt der Einstellung Hintergrundprüfungen seiner Mitarbeiter durch.

Physische und umweltbezogene Zugangskontrollen
Der Auftragsverarbeiter beschränkt den physischen Zugriff auf seine Informationssysteme und Einrichtungen durch den Einsatz physischer Kontrollen (z. B. Zugangs-PIN), die die hinreichende Sicherheit bieten, dass der Zugang zu seinen Datenzentren auf die autorisierten Personen begrenzt ist und verwendet Kamera- und Videoüberwachungssysteme an kritischen internen und externen Eintrittspunkten. Der Auftragsverarbeiter verwendet Lufttemperatur- und Feuchtigkeitskontrollen für seine Datenzentren und schützt diese vor Verlust durch Stromausfall.

Logische Zugangskontrollen
Der Auftragsverarbeiter verwendet Protokoll- und Überwachungstechnologie, um unbefugte Zugriffsversuche auf seine Netzwerke und Produktionssysteme zu erkennen und zu verhindern. Die Überwachung des Auftragsverarbeiters umfasst eine Überprüfung der Änderungen, die sich auf die Authentifikation, die Autorisierung und die Prüfung der Systeme auswirken und er handhabt einen privilegierten Zugriff auf seine Produktionssysteme.

Verschlüsselungskontrollen
Der Auftragsverarbeiter wendet geschäftsangemessene Verschlüsselungskontrollen für alle unsere Produkte an. Der Auftragsverarbeiter bewertet In-Transit- und At-Rest-Verschlüsselung unter Handhabung der branchenüblichen Best Practices für Chiffren und wendet diese an. Die Best Practices werden für das Lifecycle Management der Verschlüsselungsschlüssel, einschließlich ihrer Erzeugung, Speicherung, der Zugangskontrolle und Rotation angewandt.

Schwachstellenmanagementt
Der Auftragsverarbeiter führt regelmäßig Schwachstellen-Scans durch und behebt entdeckte Schwachstellen ihrem Risiko gemäß. Die Produkte des Auftragsverarbeiters unterliegen auch regelmäßigen Schwachstellen- und Penetrationstests.

Notfallwiederherstellung und Datensicherungskontrollen
Der Auftragsverarbeiter führt regelmäßige Sicherungen der Produktionsdateisysteme und der Datenbanken nach einem festgelegten Zeitplan durch und unterhält einen formellen Notfallwiederherstellungsplan für das Cloud-Rechenzentrum, einschließlich regelmäßiger Tests.

Cyber Incident Response Plan
Der Auftragsverarbeiter verwendet einen Incident Response Plan, um die Auswirkungen ungeplanter Cyber-Ereignisse zu verwalten und zu minimieren, die Verfahren umfassen, die im Falle einer tatsächlichen oder potenziellen Sicherheitsverletzung zu befolgen sind, einschließlich Folgendem: ein internes Einsatzteam mit einem Einsatzleiter, ein Ermittlungsteam, das eine Analyse zur Grundursache durchführt und die betroffenen Parteien identifiziert, interne

Berichterstattungs- und Meldeverfahren, die Dokumentation reaktionsfähiger Maßnahmen und Sanierungspläne und eine Überprüfung von Ereignissen nach einem Zwischenfall.

Speicher- und Übermittlungssicherheit
Der Auftragsverarbeiter wendet technische Sicherheitsmaßnahmen an, um vor unbefugtem Zugriff auf seine Daten zu schützen, die über ein öffentliches elektronisches Kommunikationsnetzwerk übermittelt oder gespeichert werden.

Sichere Entsorgung
Der Auftragsverarbeiter wendet Richtlinien und Verfahren für die Entsorgung von materiellen und immateriellen Vermögenswerten an, die Daten des Auftragsverarbeiters enthalten, sodass diese Daten nicht gelesen oder rekonstruiert werden können.

Risikoidentifizierung und -bewertung
Der Auftragsverarbeiter verwendet ein Risikobewertungsprogramm zur Unterstützung der vernünftigen Ermittlung vorhersehbarer interner und externer Risiken für seine Informationsressourcen und bestimmt, ob die bestehenden Kontrollen, Richtlinien und Verfahren den festgestellten Risiken angemessen sind.

Händler und Dienstleister
Drittanbieter oder Händler (gemeinsam bezeichnet als „Lieferanten“) mit Zugang zu den vertraulichen Informationen des Auftragsverarbeiters unterliegen den Risikobewertungen zur Beurteilung der Sensibilität der weitergegebenen Informationen des Auftragsverarbeiters. Von den Lieferanten wird erwartet, dass sie allen einschlägigen Vertragsbedingungen, die die Sicherheit der Daten des Auftragsverarbeiters betreffen, sowie sämtlichen geltenden Richtlinien und Verfahren des Auftragsverarbeiters entsprechen. Gegebenenfalls fordert der Auftragsverarbeiter seine Lieferanten regelmäßig auf, ihre Sicherheitslage zu überprüfen, um die Einhaltung der Vorschriften zu gewährleisten.