DATENVERARBEITUNGSZUSATZ

Dieser Datenverarbeitungszusatz („**Data Processing Addendum, DPA**“) ist ein Teil des Rahmenvertrags („**Vertrag**“), unter dem der Anbieter Dienstleistungen für Software und professionelle Produkte erbringt. Alle großgeschriebenen Begriffe, die in diesem Datenverarbeitungszusatz (DPA) nicht definiert sind, haben die Bedeutung, die ihnen in anderen Teilen des Vertrages gegeben wird.

1. Definitionen und Auslegung

„**Autorisiertes verbundenes Unternehmen**“ bezeichnet ein verbundenes Unternehmen des Kunden, das (a) den Datenschutzgesetzen und -vorschriften eines abgedeckten Rechtsgebiets unterliegt und (b) berechtigt ist, die Dienste gemäß der Vereinbarung zwischen dem Anbieter und dem Kunden zu nutzen, aber kein eigenes Bestellformular mit dem Anbieter unterzeichnet hat und kein „Kunde“ im Sinne der Vereinbarung ist.

„**Abgedecktes Rechtsgebiet**“ bezeichnet eine grenzüberschreitende Verarbeitung personenbezogener Daten, die aufgrund von Datenschutzgesetzen eingeschränkt ist, weil die Weitergabe an eine Person oder Einrichtung erfolgt, die sich in einem Rechtsgebiet befindet, in dem die jeweils zuständige Regierungsbehörde oder der Datenverarbeiter feststellt, dass es nicht das gleiche oder ein höheres Datenschutzniveau gewährleistet wie das Rechtsgebiet, aus dem die personenbezogenen Daten stammen.

„**Datenverantwortlicher**“ bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für die Zwecke dieses Datenverarbeitungszusatzes (DPA) ist der Datenverantwortliche der Kunde und gegebenenfalls seine verbundenen Unternehmen, die entweder vom Kunden die Erlaubnis erhalten haben, personenbezogene Daten an den/die Dienst(e) zu übermitteln, oder deren personenbezogene Daten im Rahmen des/der Dienst(e) verarbeitet werden.

„**Datenverarbeiter**“ bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet. Für die Zwecke dieses Datenverarbeitungszusatzes (DPA) ist der Datenverarbeiter die Einrichtung des Anbieters, die eine Partei der Vereinbarung ist.

„**Datenschutzgesetze**“ bezeichnet alle anwendbaren Gesetze und Vorschriften in Bezug auf die Verarbeitung personenbezogener Daten, insbesondere und in der jeweils geänderten, überholten oder ersetzten Fassung das Argentina Personal Data Protection Act (***ARGENTINIEN***); das Australia Privacy Act 1988 und die 13 Australian Privacy Principles (***AUSTRALIEN***); der California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (***CA, USA***); der Canada Personal Information Protection and Electronic Documents Act 2000 und der Quebec Private Sector Act, Law 25 (***KANADA***); die Gesetze der Volksrepublik China zum Schutz personenbezogener Daten (***CHINA***); die Datenschutzgesetze und -vorschriften des Dubai International Financial Centre (***DUBAI***); die Datenschutz-Grundverordnung (EU) 2016/679 der Europäischen Union (***EUROPÄISCHE UNION***); die Hong Kong Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong) (***HONG KONG***); die India Information Technology Rules 2011 und der Digital Personal Data Protection Act, 2023 (***INDIEN***); der Japan Personal Information Protection Act (Kojin Joho no Hogo ni Kansuru Houritsu, Law No. 57 von 2003) (***JAPAN***); das malaysische Gesetz zum Schutz personenbezogener Daten 2010 (***MALAYSIA***); das mexikanische Bundesgesetz zum Schutz personenbezogener Daten (***MEXIKO***); das neuseeländische Datenschutzgesetz 2020 (***NEUSEELAND***); das philippinische Datenschutzgesetz 2012 (***PHILIPPINEN***); das saudi-arabische Gesetz zum Schutz personenbezogener Daten 2021 (***SAUDI ARABIA***); das Gesetz zum Schutz personenbezogener Daten in Singapur von 2012 (***SINGAPUR***); das Gesetz zum Schutz personenbezogener Daten in Südafrika (2021) (***SÜDAFRIKA***); das türkische Gesetz Nr. 6698 über den Schutz personenbezogener Daten (**TÜRKEI**); das Gesetz der Vereinigten

Arabischen Emirate über den Schutz personenbezogener Daten 2021 (***VAE***); und der United Kingdom Data Protection Act 2018 und die UK General Data Protection Regulation (***VEREINIGTES KÖNIGREICH***).

„**Betroffene Person**" bezeichnet eine natürliche Person, auf die sich die personenbezogenen Daten beziehen oder die durch die personenbezogenen Daten direkt oder indirekt identifiziert werden kann. „**Personenbezogene Daten**" bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare betroffene Person beziehen und vom oder für den Kunden im Rahmen der Dienste als Kundendaten hochgeladen werden.

„**Verarbeitung, Verarbeitungsvorgänge und Verarbeitungsprozess**" bezeichnet jede Aktivität, die die Verwendung personenbezogener Daten beinhaltet, oder wie die einschlägigen Datenschutzgesetze die Begriffe Verarbeitung, Verarbeitungsvorgänge oder Verarbeitungsprozess gegebenenfalls anders definieren. Sie umfasst die Erhebung, Aufzeichnung oder Speicherung der Daten oder die Durchführung von Vorgängen oder einer Reihe von Vorgängen mit den Daten, einschließlich der Organisation, Änderung, Abfrage, Verwendung, Offenlegung, Löschung oder Vernichtung der Daten. Die Verarbeitung umfasst auch die Übermittlung von personenbezogenen Daten an Dritte.

„**Sicherheitsverletzung**" bezeichnet jede versehentliche oder unrechtmäßige Zerstörung, jeden Verlust, jede Änderung, jede unbefugte Offenlegung personenbezogener Daten oder jeden unbefugten Zugriff darauf.

„**Unterauftragsverarbeiter**" bezeichnet jede juristische Person oder Einrichtung, die mit der Verarbeitung personenbezogener Daten durch den Datenverarbeiter beauftragt ist.

2. Art, Umfang und Zweck der Verarbeitung

2.1 Bei der Erbringung der Dienstleistungen wird der Anbieter die Datenschutzrichtlinien des Anbieters einhalten, die unter https://gomomentus.com/privacy-policy abrufbar sind und durch Verweis hierin aufgenommen werden. Die Datenschutzrichtlinie des Anbieters kann nach eigenem Ermessen geändert werden; Änderungen der Richtlinie des Anbieters führen jedoch nicht zu einer wesentlichen Verringerung des Schutzniveaus für personenbezogene Daten, die im Rahmen der Dienstleistungen gemäß der Vereinbarung bereitgestellt werden.

2.2 Der Kunde und der Anbieter nehmen zur Kenntnis, dass im Sinne der geltenden Datenschutzgesetze der Kunde der Datenverantwortliche und der Anbieter der Datenverarbeiter ist.

2.3 Der Kunde behält die Kontrolle über die personenbezogenen Daten und bleibt verantwortlich für die Einhaltung seiner Verpflichtungen gemäß den geltenden Datenschutzgesetzen, einschließlich der Bereitstellung aller erforderlichen Mitteilungen und der Einholung aller erforderlichen Einwilligungen, sowie für die Verarbeitungsanweisungen, die er dem Anbieter erteilt.

2.4 Der Anbieter wird personenbezogene Daten nur in Übereinstimmung mit den Anweisungen des Kunden und nur in dem Umfang verarbeiten, der für die Erbringung der Dienstleistungen erforderlich ist. Der Kunde nimmt zur Kenntnis, dass alle personenbezogenen Daten, deren Verarbeitung er dem Anbieter zum Zwecke der Erbringung der Dienste anweist, auf die im Rahmen des Dienstes verarbeiteten Kundendaten beschränkt sein müssen. Einzelheiten zur Verarbeitung personenbezogener Daten im Rahmen dieses Datenverarbeitungszusatzes (DPA) sind in Anhang A dargelegt.

2.5 Die Parteien nehmen zur Kenntnis und erklären sich damit einverstanden, dass der Kunde diesen Datenverarbeitungszusatz (DPA) in seinem eigenen Namen und gegebenenfalls im Namen seiner autorisierten verbundenen Unternehmen abschließt, wodurch ein separater Datenverarbeitungszusatz zwischen dem Anbieter und jeder dieser autorisierten verbundenen Unternehmen gemäß den Bestimmungen des Vertrags

zustande kommt. Jedes autorisierte verbundene Unternehmen erklärt sich mit den Verpflichtungen im Rahmen dieses Datenverarbeitungszusatzes (DPA) einverstanden. Zur Klarstellung: Ein autorisiertes verbundenes Unternehmen ist keine Partei der Vereinbarung und wird auch nicht zu einer solchen, sondern ist nur eine Partei dieses Datenverarbeitungszusatzes (DPA). Jeder Zugriff auf und jede Nutzung der Dienste durch autorisierte verbundene Unternehmen muss den Bedingungen der Vereinbarung entsprechen, und jede Verletzung der Bedingungen der Vereinbarung durch ein autorisiertes verbundenes Unternehmen gilt als Verletzung durch den Kunden.

3. Maßnahmen zur Datenverarbeitung

3.1 Wenn der Anbieter der Meinung ist, dass die Befolgung der Anweisungen des Kunden zu einem Verstoß gegen Datenschutzgesetze führen würde oder nicht im Rahmen der normalen Verpflichtungen des Anbieters im Rahmen des Betriebs der Dienste liegt, wird der Anbieter den Kunden unverzüglich darüber informieren.

3.2 Personen, die vom Anbieter zur Verarbeitung personenbezogener Daten bevollmächtigt wurden, sind an entsprechende Vertraulichkeitsverpflichtungen gebunden. Der Anbieter hat einen Datenschutzbeauftragten ernannt. Die ernannte Person kann unter privacy@gomomentus.com kontaktiert werden.

3.3 Der Anbieter muss jederzeit angemessene technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten vor unbefugter oder unrechtmäßiger Verarbeitung, unbefugtem Zugriff, unbefugter Vervielfältigung, Änderung, Speicherung, Vervielfältigung, Anzeige oder Verbreitung sowie vor zufälligem Verlust, vor Nichtverfügbarkeit, Zerstörung oder Beschädigung zu schützen. Für bestimmte Dienste stellt der Anbieter auch Sicherheitsfunktionen und -kontrollen bereit, die der Kunde wahlweise nutzen kann. Der Kunde ist für die Umsetzung aller optionalen technischen und organisatorischen Maßnahmen zum Schutz der Kundendaten verantwortlich, wie im Vertrag oder in der Dokumentation beschrieben.

3.4 Der Anbieter wird den Kunden in angemessener Weise bei der Erfüllung seiner Verpflichtungen zur Einhaltung der Datenschutzgesetze unterstützen, wobei er auch die Art der Verarbeitung durch den Anbieter und die dem Anbieter zur Verfügung stehenden Informationen berücksichtigt.

4. Sicherheit & Benachrichtigung über Datenschutzverletzungen

4.1 Der Anbieter wird den Kunden unverzüglich benachrichtigen, wenn er Kenntnis von Fortschritten in der Technologie und den Arbeitsmethoden erhält, die darauf hindeuten, dass die Parteien ihre Sicherheitsmaßnahmen anpassen sollten.

4.2 Der Anbieter muss angemessene Vorsichtsmaßnahmen ergreifen, um die Integrität der von ihm verarbeiteten personenbezogenen Daten zu bewahren und eine Beeinträchtigung oder einen Verlust der personenbezogenen Daten zu verhindern. Die Lieferantensysteme sind so programmiert, dass sie routinemäßig tägliche Daten-Backups nach Maßgabe der jeweils in Kraft befindlichen Backup-Richtlinie des Lieferanten anlegen. Der Lieferant übermittelt dem Kunden seine jeweils aktuellsten Backups von Kundendaten. In Fällen des Verlusts, der Vernichtung, der Beschädigung oder Verfälschung von Kundendaten, die auf die Lieferantensysteme oder Dienstleistungen zurückzuführen sind, hat der Lieferant als seine einzige Verpflichtung und Haftungsverbindlichkeit sowie als einzige Abhilfemaßnahme des Kunden wirtschaftlich zumutbare Anstrengungen zu unternehmen, um die Kundendaten aus dem jüngsten Backup der betreffenden Kundendaten wiederherzustellen.

4.3 Der Anbieter wird dem Kunden jede Sicherheitsverletzung unverzüglich melden, nachdem der Anbieter festgestellt hat, dass eine Sicherheitsverletzung vorliegt.

4.4 Die erste Meldung erfolgt an den/die im Kunden-Support-Portal des Anbieters benannten Sicherheits- oder Datenschutzkontakt(e) des Kunden (oder, falls kein(e) solcher/solchen Kontakt(e) benannt ist/sind, an den vom Kunden benannten primären technischen Kontakt). Sobald relevante Informationen in Bezug auf den Verstoß gesammelt werden oder dem Anbieter anderweitig zur Verfügung stehen, wird er diese Informationen unverzüglich an den Kunden weitergeben, um ihn bei der Erfüllung seiner Meldepflichten gemäß den Datenschutzgesetzen zu unterstützen. Insbesondere wird der Anbieter dem Kunden die in Artikel 33 der DSGVO beschriebenen Informationen bereitstellen, soweit dies in angemessenem Rahmen möglich und zulässig ist.

4.5 Der Kunde wird mit dem Anbieter zusammenarbeiten, indem er genaue Kontaktinformationen im Kunden-Support-Portal pflegt und alle Informationen zur Verfügung stellt, die in angemessener Weise angefordert werden, um Sicherheitsverletzungen zu beheben, ihre Ursache(n) zu ermitteln und eine Wiederholung zu verhindern. Der Kunde ist als Datenverantwortlicher allein dafür verantwortlich, zu entscheiden, ob er die zuständigen Aufsichts- oder Regulierungsbehörden und die betroffenen Personen in Bezug auf eine Sicherheitsverletzung benachrichtigt und diese Benachrichtigung vorzunehmen.

5. Ersuchen von betroffenen Personen und Behörden.

5.1 Während der Laufzeit stellt der Anbieter dem Kunden die Möglichkeit zur Verfügung, innerhalb des Abonnementdienstes auf personenbezogene Daten zuzugreifen, sie zu korrigieren, zu berichtigen, zu löschen oder zu sperren oder solche personenbezogenen Daten zu übertragen oder zu portieren, soweit dies nach den geltenden Datenschutzgesetzen erforderlich ist (zusammenfassend als „**Anfragen von betroffenen Personen**“ bezeichnet).

5.2 Der Kunde ist allein für die Beantwortung von Anfragen betroffener Personen verantwortlich, vorausgesetzt, dass der Anbieter in angemessener Weise mit dem Kunden in Bezug auf Anfragen betroffener Personen zusammenarbeitet, soweit der Kunde nicht in der Lage ist, solche Anfragen betroffener Personen mit Hilfe der Funktionalität im Rahmen der Dienste zu erfüllen. Der Anbieter wird die betroffene Person anweisen, sich mit dem Kunden in Verbindung zu setzen, falls er eine Anfrage der betroffenen Person direkt erhält.

5.3 Im Falle einer Mitteilung, Prüfung, Untersuchung oder Ermittlung durch eine staatliche Stelle, eine Datenschutzbehörde oder eine Strafverfolgungsbehörde in Bezug auf die Verarbeitung personenbezogener Daten wird der Anbieter den Kunden unverzüglich benachrichtigen, sofern dies nicht durch geltendes Recht untersagt ist. Jede Partei wird mit der anderen Partei kooperieren, indem sie alle angeforderten und verfügbaren angemessenen Informationen zur Verfügung stellt.

6. Audits

6.1 Der Anbieter ermöglicht Audits, einschließlich Inspektionen, und trägt dazu bei, indem er dem Kunden Zugang zu angemessenen und branchenüblichen Unterlagen gewährt, die die Richtlinien und Verfahren für die Sicherheit und den Schutz personenbezogener Daten belegen („**Audit**“). Die im Rahmen eines Audits zur Verfügung stehenden Informationen umfassen Unterlagen, die die Datenschutzrichtlinien und -verfahren in Bezug auf verarbeitete personenbezogene Daten belegen, sowie Kopien von Zertifizierungen und Bescheinigungsberichten, die zu diesem Zeitpunkt vorliegen (einschließlich von Audits). Soweit der Kunde nicht in der Lage war, seine Audit-Anforderungen durch das in dieser Klausel beschriebene Verfahren zu erfüllen, wird der Anbieter dem Kunden die weitere Unterstützung gewähren, die nach vernünftigem Ermessen (in Übereinstimmung mit den hierin beschriebenen Unterstützungspflichten) erforderlich ist, um diese Anforderungen im Wesentlichen zu erfüllen.

6.2 Auf Anfrage des Kunden per E-Mail an privacy@gomomentus.com können der Anbieter und der Kunde einen für beide Seiten günstigen Termin zur Besprechung des Audits vereinbaren. Falls bei dem Audit eine wesentliche Nichteinhaltung des Datenverarbeitungszusatzes (DPA) festgestellt wird, wird sich der

Anbieter unverzüglich um diese Verstöße kümmern. Der Anbieter kann nach eigenem Ermessen und in Übereinstimmung mit den Branchenstandards und -praktiken des Anbieters wirtschaftlich angemessene Anstrengungen unternehmen, um die im Audit festgestellten Verbesserungsvorschläge des Kunden zur Verbesserung des Sicherheitsprogramms des Anbieters umzusetzen. Das Audit und die daraus resultierenden Ergebnisse stellen vertrauliche Informationen des Anbieters dar.

7. Unterauftragsverarbeiter.

7.1 Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass (a) die verbundenen Unternehmen des Anbieters als Unterauftragsverarbeiter eingesetzt werden können und (b) der Anbieter bzw. die verbundenen Unternehmen des Anbieters im Zusammenhang mit der Erbringung der Dienste externe Unterauftragsverarbeiter einsetzen können. Der Anbieter oder ein verbundenes Unternehmen des Anbieters muss mit jedem Unterauftragsverarbeiter einen schriftlichen Vertrag abschließen, der im Wesentlichen Datenschutzverpflichtungen enthält, die in Bezug auf den Schutz der Kundendaten nicht weniger schützend sind als die in diesem Vertrag enthaltenen Verpflichtungen, soweit dies auf die Art der von diesem Unterauftragsverarbeiter erbrachten Dienstleistungen zutrifft. Die aktuelle Liste der Unterauftragsverarbeiter, die mit der Verarbeitung personenbezogener Daten für die Erbringung der jeweiligen Dienstleistung beauftragt sind, einschließlich einer Beschreibung ihrer Verarbeitungstätigkeiten und der Länder, in denen sie ansässig sind, ist in Anhang B aufgeführt, der von Zeit zu Zeit oder in Übereinstimmung mit Klausel 7.2 aktualisiert werden kann. Der Kunde erteilt hiermit seine Einwilligung bezüglich dieser Unterauftragsverarbeiter, ihrer Standorte und Verarbeitungstätigkeiten in Bezug auf die personenbezogenen Daten des Kunden.

7.2 Für abgedeckte Rechtsgebiete wird der Anbieter vor der Beauftragung eines neuen Unterauftragsverarbeiters für die Dienste: (a) den Kunden per E-Mail an die vom Kunden benannte Kontaktperson in den Support-Portalen oder Konten des Anbieters (oder über einen anderen zur Benachrichtigung seines Kundenstamms verwendeten Kanal) benachrichtigen; und (b) diesen Unterauftragsverarbeiter dazu veranlassen, eine schriftliche Vereinbarung mit dem Anbieter (oder dem entsprechenden verbundenen Unternehmen des Anbieters) abzuschließen, die den Unterauftragsverarbeiter dazu verpflichtet, sich an Bedingungen zu halten, die nicht weniger schützend sind als die in diesem Datenverarbeitungszusatz (DPA) vorgesehenen. In Bezug auf die im vorstehenden Satz beschriebene Benachrichtigung wird der Anbieter mindestens 30 Tage im Voraus eine schriftliche Benachrichtigung versenden, bevor er einen Unterauftragsverarbeiter in Bezug auf bestehende Dienste, die der Kunde erworben hat, beauftragt. Wenn ein neuer Unterauftragsverarbeiter mit der Unterstützung eines neuen Dienstes oder einer neuen Funktion eines bestehenden Abonnementdienstes beauftragt wird, erfolgt die in dieser Klausel beschriebene Mitteilung zu oder vor dem Zeitpunkt, zu dem diese Funktion oder dieser Abonnementdienst allgemein verfügbar gemacht wird. Auf schriftliche Anfrage des Kunden per E-Mail an privacy@gomomentus.com wird der Anbieter dem Kunden eine Zusammenfassung der Datenverarbeitungsbedingungen mit dem Unterauftragsverarbeiter zur Verfügung stellen. Der Kunde kann schriftlich per E-Mail an privacy@gomomentus.com angemessene zusätzliche Informationen in Bezug auf die Fähigkeit des Unterauftragsverarbeiters anfordern, die relevanten Verarbeitungsaktivitäten in Übereinstimmung mit dieser DSGVO durchzuführen.

7.3 Der Kunde kann dem Einsatz eines neuen Unterauftragsverarbeiters durch den Anbieter widersprechen, indem er den Anbieter unverzüglich schriftlich innerhalb von dreißig (30) Tagen nach Erhalt der Mitteilung des Anbieters entsprechend dem in Ziffer 7.2 dargelegten Verfahren benachrichtigt. Wenn der Kunde einem neuen Unterauftragsverarbeiter gemäß dem vorstehenden Satz widerspricht, wird sich der Anbieter in angemessener Weise bemühen, dem Kunden eine Abänderung der Dienste anzubieten oder eine wirtschaftlich vertretbare Änderung der Konfiguration oder Nutzung der Dienste durch den Kunden zu empfehlen, um die Verarbeitung personenbezogener Daten durch den beanstandeten neuen Unterauftragsverarbeiter zu vermeiden, ohne den Kunden unangemessen zu belasten. Sollte der Anbieter nicht in der Lage sein, eine solche Anpassung innerhalb einer angemessenen Frist, die neunzig (90) Tage nicht überschreiten darf, nachdem sich beide Parteien in gutem Glauben darauf verständigt haben, bereitzustellen,

kann der Kunde das/die entsprechende(n) Bestellformular(e) mit einer Frist von dreißig (30) Tagen kündigen, und zwar nur in Bezug auf die Dienste, die vom Anbieter nicht ohne den beanstandeten neuen Unterauftragsverarbeiter erbracht werden können. Das Recht des Kunden, die betreffenden Dienstleistungen gemäß dieser Klausel zu kündigen, entbindet den Kunden nicht von seinen Zahlungsverpflichtungen aus dem Vertrag bis zum Datum der Kündigung. Wenn sich die Kündigung gemäß dieser Klausel nur auf einen Teil der Dienstleistungen im Rahmen eines Auftragsformulars bezieht, erklärt sich der Kunde damit einverstanden, einen Änderungs- oder Ersatzauftrag zu erteilen, der diese teilweise Kündigung widerspiegelt.

7.4 Der Einsatz eines Unterauftragsverarbeiters entbindet den Anbieter nicht von seinen Verpflichtungen im Rahmen dieses Datenverarbeitungszusatzes (DPA), und der Anbieter haftet für die Handlungen und Unterlassungen eines Unterauftragsverarbeiters in gleichem Maße, wie wenn die Handlungen oder Unterlassungen vom Anbieter selbst vorgenommen würden.

8. Haftungsbeschränkung und Laufzeit.

8.1 Die Gesamthaftung jeder Partei und aller ihrer verbundenen Unternehmen aus oder im Zusammenhang mit diesem Datenverarbeitungszusatz (DPA) und allen Datenverarbeitungszusätzen zwischen autorisierten verbundenen Unternehmen und dem Anbieter, sei es aus Vertrag, unerlaubter Handlung oder aufgrund einer anderen Haftungstheorie, unterliegt dem Abschnitt „Haftungsbeschränkung“ des Vertrags, und jede Bezugnahme in diesem Abschnitt auf die Haftung einer Partei bezieht sich auf die Gesamthaftung dieser Partei und aller ihrer verbundenen Unternehmen aus dem Vertrag und allen Datenverarbeitungszusätzen zusammen. Zur Klarstellung: Die Gesamthaftung des Anbieters und seiner verbundenen Unternehmen für alle Ansprüche des Kunden und aller seiner autorisierten verbundenen Unternehmen, die sich aus dem Vertrag und allen Datenverarbeitungszusätzen ergeben oder damit in Zusammenhang stehen, gilt insgesamt für alle Ansprüche sowohl aus dem Vertrag als auch aus allen Datenverarbeitungszusätzen, die im Rahmen des Vertrags eingerichtet wurden, einschließlich der Ansprüche des Kunden und aller autorisierten verbundenen Unternehmen, und ist insbesondere nicht so zu verstehen, dass sie für den Kunden und/oder jedes autorisierte verbundene Unternehmen, das Vertragspartei eines solchen DPAs ist, individuell und einzeln gilt.

8.2 Dieser Datenverarbeitungszusatz (DPA) bleibt in vollem Umfang in Kraft, solange die Laufzeit der Vereinbarung in Kraft bleibt oder der Anbieter personenbezogene Daten im Zusammenhang mit der Vereinbarung in seinem Besitz oder unter seiner Kontrolle behält. Im Falle eines Widerspruchs zwischen den Bedingungen dieses Datenverarbeitungszusatzes (DPA) und den Bedingungen der Vereinbarung in Bezug auf den hierin enthaltenen Gegenstand, hat dieser Datenverarbeitungszusatz (DPA) Vorrang. Der primäre Datenverarbeiter ist ein amerikanisches Unternehmen und daher ist die englische Version des Datenverarbeitungszusatzes (DPA) die Standardversion. Im Falle einer Fehlinterpretation aufgrund der Übersetzung der Dokumente ins Französische oder Deutsche ist immer die englische Version maßgebend.

9. Internationale Datenübertragungen

9.1 Die Übermittlung personenbezogener Daten aus einem abgedeckten Rechtsgebiet in ein Land, das sich nicht in einem Rechtsgebiet befindet, für das ein gültiger Angemessenheitsbeschluss (gemäß den anwendbaren Datenschutzgesetzen in Bezug auf die Personen, über die die personenbezogenen Daten verarbeitet werden) vorliegt (eine „**Datenübermittlung**“), unterliegt den nachstehenden Standardvertragsklauseln der SCCs, vorbehaltlich der erforderlichen Anpassungen zur Einhaltung der anwendbaren Datenschutzgesetze. Für alle Dienste werden personenbezogene Daten in der Region des Rechenzentrums gespeichert/gehostet, die im Bestellformular/Vertrag für diese Dienste angegeben ist, oder, falls zutreffend, in der geografischen Region, die bei der Aktivierung der Produktionsinstanz für diese Dienste ausgewählt wurde. Ungeachtet solcher Speicher-/Hosting-Anforderungen und vorbehaltlich dieses Datenverarbeitungszusatzes (DPA) kann der Anbieter personenbezogene Daten weltweit verarbeiten, soweit dies für die Erbringung der Dienste erforderlich ist, z. B. für Support-, Störungsmanagement- oder Datenwiederherstellungszwecke.

9.2 EWR-Datenschutzrecht.

(a) Wenn es einen Datenverarbeitungszusatz gibt, der den Datenschutzgesetzen des EWR unterliegt, unterliegt die Datenübermittlung den Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates im Anhang des Durchführungsbeschlusses 2021/914 der Kommission und aller Aktualisierungen dazu („**SCCs**"), die durch diesen Verweis in diesen Datenverarbeitungszusatz (DPA) aufgenommen werden.

(b) **SCC-Module**. Modul Zwei (Datenverantwortlicher an Datenverarbeiter) gilt für eine Datenübermittlung, wenn der Kunde ein Datenverantwortlicher ist. Modul Drei (Datenverarbeiter an Datenverarbeiter) gilt für eine Datenübermittlung, wenn der Kunde ein Datenverarbeiter ist.

(c) **Fakultative Bestimmungen der SCCs**. Wenn die SCCs optionale Bestimmungen enthalten:

(i) Klausel 7 (Andockklausel) - die optionale Bestimmung gilt als aufgenommen und angewendet;

(ii) Klausel 8.3 - Vor der Offenlegung einer Kopie der SCCs gemäß Klausel 8.3 muss die offenlegende Partei alle wirtschaftlich vertretbaren Anstrengungen unternehmen, um alle geschäftlichen Klauseln zu schwärzen, aber eine aussagekräftige Zusammenfassung bereitzustellen, wenn die betroffene Person andernfalls nicht in der Lage wäre, den Inhalt zu verstehen oder ihre Rechte auszuüben, weil die Schwärzung nicht erfolgt;

(iii) Klausel 9(a) (Einsatz von Unterauftragsverarbeitern) - es gilt Option 2 (und die Parteien folgen dem im Datenverarbeitungszusatz (DPA) vereinbarten Verfahren und Zeitplan für die Beauftragung von Unterauftragsverarbeitern);

(iv) Klausel 11(a) (Rechtsmittel) - die optionale Bestimmung findet keine Anwendung;

(v) Klausel 12 - alle Ansprüche, die im Rahmen der SCCs geltend gemacht werden, unterliegen den in der Vereinbarung festgelegten Geschäftsbedingungen. In keinem Fall darf eine Partei ihre Haftung in Bezug auf die Rechte der betroffenen Person gemäß den EU-SCCs einschränken;

(vi) Klausel 17 (Anwendbares Recht) - es gilt Option 1, und wenn die Vereinbarung dem Recht eines EU-Mitgliedstaates unterliegt, gilt das Recht dieses EU-Mitgliedstaates; andernfalls gilt irisches Recht; und

(vii) Klausel 18(b) (Wahl des Gerichtsstandes und der Gerichtsbarkeit) - unterliegt die Vereinbarung der Gerichtsbarkeit eines EU-Mitgliedstaates, sind die Gerichte dieses EU-Mitgliedstaates zuständig; andernfalls sind die Gerichte von Dublin, Irland, zuständig.

(d) **Anhänge der SCCs.**

(i) Anhang 1A: Der/die Datenexporteur(e) ist/sind der Kunde und seine verbundenen Unternehmen, der/die die Datenübermittlung vornimmt/vornehmen (der „**Datenexporteur**") und die Datenimporteure sind die Anbieter, die die Datenübermittlung empfangen (der „**Datenimporteur**"). Der vollständige Name, die Adresse und die Kontaktdaten

des Datenexporteurs und des Datenimporteurs sind in der Vereinbarung aufgeführt oder können von jeder Partei angefordert werden.

(ii) Anhang 1B: Die: relevanten Details sind die, die in der Vereinbarung festgelegt sind, einschließlich Anhang 1 „Details der Verarbeitung“ dieses Datenverarbeitungszusatzes (DPA).

(iii) Anhang 1C: Die zuständige Aufsichtsbehörde ist die für den Kunden (oder gegebenenfalls für den Vertreter des Kunden) zuständige Aufsichtsbehörde.

(iv) Anhang 2: Es gelten die in Nachtrag 1 enthaltenen Sicherheitsbestimmungen oder andere sicherheitsrelevante Bestimmungen der Vereinbarung.

(e) **Mitteilungen**. Alle Mitteilungen, Anfragen, Überwachungs-/Audit-Rechte, die Geltendmachung von Ansprüchen, die Haftung und die Löschung oder Rückgabe von Daten in Bezug auf die SCCs werden, soweit anwendbar, in Übereinstimmung mit den entsprechenden Bestimmungen in der Vereinbarung bereitgestellt/verwaltet/ausgelegt, soweit diese Bestimmungen nicht im Widerspruch zu den SCCs stehen.

9.3 Schweizer Datenschutzgesetz.

(a) Wenn es eine Datenübermittlung gibt, die dem schweizerischen Datenschutzrecht unterliegt, gelten die SCCs mit den folgenden Änderungen:

(i) Verweise auf „DSGVO“ in den SCCs sind als Verweise auf das Schweizer Bundesgesetz über den Datenschutz („**DSG**“) zu verstehen;

(ii) Verweise auf einen „Mitgliedstaat“ und „EU-Mitgliedstaat“ sind nicht so zu verstehen, dass betroffene Personen in der Schweiz nicht die Möglichkeit haben, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) einzuklagen; und

(iii) die zuständige Aufsichtsbehörde in Anhang 1.C unter Klausel 13 wird der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte („**EDÖB**“) sein. Unterliegen die übermittelten personenbezogenen Daten jedoch sowohl dem DSG als auch den SCC, sollte eine parallele Aufsicht Anwendung finden: Für das (revidierte) DSG ist der EDÖB die zuständige Aufsichtsbehörde, soweit die Übermittlung dem (revidierten) DSG unterliegt; und für die SCC ist die zuständige Aufsichtsbehörde (a) die Aufsichtsbehörde des Landes, in dem der Datenexporteur niedergelassen ist, wenn der Datenexporteur im EWR niedergelassen ist, oder (b) die Aufsichtsbehörde von Irland, wenn der Datenexporteur nicht im EWR niedergelassen ist.

9.4 UK-Datenschutzgesetz.

(a) Wenn es eine Datenübermittlung gibt, die den Datenschutzgesetzen des Vereinigten Königreichs unterliegt, gilt der internationale Datenübermittlungszusatz zu den SCCs („**UK IDTA**“), wie er vom Information Commissioner im Vereinigten Königreich herausgegeben wurde, und wird durch Verweis in diesen Datenverarbeitungszusatz (DPA) aufgenommen. Die Informationen, die zum Ausfüllen der Tabellen des UK IDTA benötigt werden, sind in der Vereinbarung aufgeführt, einschließlich Anhang 1 „Details der Verarbeitung“ dieses Datenverarbeitungszusatzes (DPA).

(b) In Tabelle 2 des UK IDTA aktivieren die Parteien das Kontrollkästchen, das wie folgt lautet: „Genehmigte EU-SCCs, einschließlich der Informationen im Anhang und mit ausschließlich den folgenden Modulen, Klauseln oder optionalen Bestimmungen der genehmigten EU-SCCs, die für die Zwecke dieses Nachtrags in Kraft gesetzt werden“, und die dazugehörige Tabelle gilt als entsprechend

den in diesem Datenverarbeitungszusatz (DPA) dargelegten Präferenzen der Parteien ausgefüllt. Für die Zwecke des britischen IDTA gilt das Recht von England und Wales als anwendbar.

(c) In Tabelle 4 vereinbaren die Parteien, dass jede Partei den Nachtrag gemäß Klausel 19 des UK IDTA kündigen kann.

9.5 Datenschutzgesetz der Volksrepublik China.

(a) Wenn es zu einer Datenübermittlung kommt, die den Datenschutzgesetzen der Volksrepublik China unterliegt, muss der Kunde den Anbieter unverzüglich benachrichtigen und alle notwendigen Schritte unternehmen, um den Umfang der mit dem Anbieter geteilten personenbezogenen Daten zu minimieren.

(b) Alle Streitigkeiten, die sich aus den Datenschutzgesetzen der Volksrepublik China ergeben, werden der China International Economic and Trade Arbitration Commission (CIETAC) Shanghai Sub-Commission zur Schlichtung vorgelegt, die in Shanghai in Übereinstimmung mit der zum Zeitpunkt der Schlichtung gültigen Schiedsordnung der CIETAC durchgeführt wird. Alle vom Schiedsgericht getroffenen Entscheidungen sind endgültig und für die Parteien bindend.

9.6 Argentinisches Datenschutzrecht.

(a) Wenn eine Datenübermittlung stattfindet, die den argentinischen Datenschutzgesetzen unterliegt, stimmen der Anbieter und der Kunde hiermit den zusätzlichen Klauseln zu, die in den Anhängen der Verordnung Nr. 60- E/2016 beschrieben sind, verfügbar unter http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm.

(b) Zu den Ländern, die nach den argentinischen Datenschutzgesetzen ein angemessenes Datenschutzniveau bieten, gehören die Mitglieder des Europäischen Wirtschaftsraums (EWR), die Schweiz, Guernsey, Jersey, die Insel Man, die Färöer Inseln, Kanada (nur für den privaten Sektor), das Fürstentum Andorra, Neuseeland, die Republik Uruguay, der Staat Israel (nur für Daten, die einer automatisierten Verarbeitung unterliegen) und das Vereinigte Königreich Großbritannien sowie Nordirland.

9.7 Ungeachtet der Tatsache, dass die SCCs und/oder der UK IDTA durch Verweis in diese Vereinbarung aufgenommen werden, ohne dass die Unterschriftenseiten der SCCs tatsächlich vom Datenexporteur oder Datenimporteur unterzeichnet werden, vereinbaren die Parteien, dass ihre jeweilige Unterzeichnung der Vereinbarung als Unterzeichnung der SCCs und/oder des UK IDTA im Namen des Datenexporteurs/Datenimporteurs (je nach Fall) gilt.

9.8 Wenn ein alternativer Übermittlungsmechanismus, wie z. B. Binding Corporate Rules, vom Anbieter angenommen wird oder das Trans-Atlantic Data Privacy Framework (ein „**Alternativer Mechanismus**“) während der Laufzeit der Vereinbarung verfügbar wird und der Anbieter dem Kunden mitteilt, dass einige oder alle Datenübermittlungen in Übereinstimmung mit den Datenschutzgesetzen gemäß dem alternativen Mechanismus durchgeführt werden können, werden sich die Parteien für die Datenübermittlungen, auf die der alternative Mechanismus Anwendung findet, auf den alternativen Mechanismus anstelle der oben genannten Bestimmungen berufen.

(i) Der Anbieter kann diesen Datenverarbeitungszusatz (DPA) ändern, wenn die Änderung eine Änderung des Namens oder der Rechtsform einer juristischen Person widerspiegelt und/oder notwendig ist, um die Datenschutzgesetze (einschließlich der von einer Datenschutzbehörde in einem abgedeckten Rechtsgebiet herausgegebenen Leitlinien) oder eine verbindliche behördliche oder gerichtliche Anordnung einzuhalten

ANHANG A

Zweck der Verarbeitung personenbezogener Daten und Einzelheiten

1. Gegenstand. Gegenstand der Datenverarbeitung im Rahmen dieses DPA sind die in den Kundendaten enthaltenen personenbezogenen Daten.

2. Dauer Im Rahmen dieses DPA ist die Dauer der Datenverarbeitung zwischen Anbieter und Kunde die Laufzeit der Vereinbarung.

3. Zweck und Art. Der Zweck und die Art der Datenverarbeitung im Rahmen dieses DPA besteht in der Erbringung der Dienstleistungen durch den Anbieter gemäß der Vereinbarung und den anwendbaren Bestellformularen.

4. Art der personenbezogenen Daten Zu den Kundendaten gehörende personenbezogene Daten, die vom Kunden oder von autorisierten Benutzern in die Dienste hochgeladen werden.

5. Kategorien der betroffenen Personen Zu den betroffenen Personen können die Mitarbeiter, Lieferanten, Vertreter, Partner und/oder Endbenutzer des Kunden gehören, wie sie in den Bestellformularen zugelassen sind.

Datensicherheitsmaßnahmen

1. SICHERHEITSPROGRAMM

   Während der Erbringung der Dienstleistung(en) stellt der Anbieter sicher, dass ein schriftliches Informationssicherheitsprogramm mit Richtlinien, Verfahren und Kontrollen vorhanden ist, das sich an den Industriestandards orientiert und die Verarbeitung, Speicherung, Übertragung und Sicherheit der Kundendaten regelt. Das Sicherheitsprogramm umfasst branchenübliche Prozesse und Verfahren zum Schutz der Kundendaten vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Änderung, unbefugter Weitergabe oder Zugriff. Der Anbieter aktualisiert das Sicherheitsprogramm, um neue und sich entwickelnde Sicherheitstechnologien, Änderungen der branchenüblichen Praktiken und sich ändernde Sicherheitsbedrohungen zu berücksichtigen, vorausgesetzt, dass eine solche Aktualisierung das Gesamtniveau der Verpflichtungen oder des Schutzes, die dem Kunden wie hier beschrieben geboten werden, nicht wesentlich verringert.

   1.1 SICHERHEITSORGANISATION Es wird einen Chief Information Security Officer oder eine vergleichbare leitende Position geben, der/die für die Koordinierung, Verwaltung und Überwachung der Informationssicherheitsfunktion, -richtlinien und -verfahren verantwortlich ist.

   1.2 RICHTLINIEN Die Richtlinien zur Informationssicherheit werden: (i) dokumentiert; (ii) von der Geschäftsleitung überprüft und genehmigt, einschließlich nach wesentlichen Änderungen; und (iii) veröffentlicht und dem Personal und den Auftragnehmern mitgeteilt, einschließlich angemessener Konsequenzen bei Nichteinhaltung.

   1.3 RISIKOMANAGEMENT Es werden Risikobewertungen zur Informationssicherheit als Teil eines Risiko-Management-Programms vorgenommen, das mit dem Ziel eingerichtet wird, die Wirksamkeit des Sicherheitsprogramms regelmäßig zu testen, zu bewerten und zu evaluieren. Diese Bewertungen dienen dazu, die Auswirkungen von Risiken zu erkennen und zu bewerten und ermittelte Strategien zur Risikominderung oder -abschwächung umzusetzen, um neuen und sich entwickelnden Sicherheitstechnologien, Änderungen von Industriestandards und veränderten

Sicherheitsbedrohungen zu begegnen.

2. AUDITS

2.1 AUDIT Der Anbieter lässt Audits, die Inspektionen beinhalten, zu und trägt dazu bei, indem er dem Kunden über ein Dokumentationsportal für den Selbstzugang und ohne zusätzliche Kosten gang zu einer angemessenen und branchenweit anerkannten Dokumentation gewährt, die die Richtlinien und Verfahren für die Sicherheit und den Schutz der Kundendaten und des Sicherheitsprogramms belegt. Die im Portal verfügbaren Informationen umfassen eine Dokumentation, die das Sicherheitsprogramm einschließlich der Datenschutzrichtlinien und -verfahren in Bezug auf die verarbeiteten personenbezogenen Daten belegt. Soweit der Kunde nicht in der Lage war, seine Audit-Anforderungen durch das in dieser Klausel beschriebene Verfahren zu erfüllen, wird der Anbieter dem Kunden die weitere Unterstützung gewähren, die nach vernünftigem Ermessen (in Übereinstimmung mit den hierin beschriebenen Unterstützungspflichten) erforderlich ist, um diese Anforderungen im Wesentlichen zu erfüllen.

2.2 ERGEBNIS Auf Anfrage des Kunden können der Anbieter und der Kunde einen für beide Seiten günstigen Termin zur Besprechung des Audits vereinbaren. Sollte das Audit eine wesentliche Nichteinhaltung des Datenverarbeitungszusatzes oder dieser Datensicherheitsmaßnahmen (Data Security Measures, DSM) ergeben, wird der Anbieter diese Nichteinhaltung unverzüglich beheben. Der Anbieter kann nach eigenem Ermessen und in Übereinstimmung mit den Branchen- und Anbieterstandards und -praktiken wirtschaftlich angemessene Anstrengungen unternehmen, um die im Audit festgestellten Verbesserungsvorschläge des Kunden zur Verbesserung des Sicherheitsprogramms des Anbieters umzusetzen. Das Audit und die daraus resultierenden Ergebnisse stellen vertrauliche Informationen des Anbieters dar.

3. PHYSISCHE, TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMASSNAHMEN

3.1 PHYSISCHE SICHERHEITSMASSNAHMEN

3.1.1. RECHENZENTRUMSEINRICHTUNGEN Die Einrichtungen des Rechenzentrums werden Folgendes bieten: (1) physische Zugangsbeschränkungen und -überwachung, die eine Kombination der folgenden Maßnahmen umfassen: Mehrzonen-Sicherheit, Sicherheitsschleusen, geeignete Abschreckungsmaßnahmen, Wachpersonal vor Ort, biometrische Kontrollen, Videoüberwachung und Schutzkäfige; und (2) Brandmelde- und Brandbekämpfungssysteme, sowohl lokal als auch im gesamten Rechenzentrum.

3.1.2. MEDIEN Für die Löschung von Daten wird ein Industriestandard wie NIST 800-88 oder ein im Wesentlichen gleichwertiger Standard für die Löschung von sensiblen Daten, einschließlich Kundendaten, vor der endgültigen Vernichtung solcher Medien angewendet.

3.2 TECHNISCHE SICHERHEITSMASSNAHMEN.

3.2.1. ZUGRIFFSVERWALTUNG Der Zugriff durch Mitarbeiter auf Kundendaten erfolgt in einer Weise, die: (i) durch Authentifizierungs- und Autorisierungsmechanismen geschützt ist; (ii) erfordert, dass dem Personal ein eindeutiges Benutzerkonto zugewiesen wird; (iii) die gemeinsame Nutzung einzelner Benutzerkonten einschränkt; (iv) eine starke Authentifizierung mit komplexen Passwörtern erfordert; (v) sicherstellt, dass die Konten mit einer Sperrfunktion versehen sind; (vi) den Zugang über ein VPN erfordert; (vii) verlangt, dass die Zugriffsrechte auf den beruflichen Anforderungen beruhen und auf das Maß beschränkt sind, das für die betreffenden Mitarbeiter zur Erfüllung ihrer Aufgaben erforderlich ist; (viii) gewährleistet, dass der Zugriff bei Beendigung des Beschäftigungs-

oder Beratungsverhältnisses widerrufen wird; und (ix) verlangt, dass die Zugriffsberechtigungen vierteljährlich vom Management überprüft werden.

3.2.2. PROTOKOLLIERUNG UND ÜBERWACHUNG Die Protokollierungsaktivitäten der Produktionsinfrastruktur werden zentral erfasst, gesichert, um Manipulationen zu verhindern, und von einem geschulten Sicherheitsteam auf Anomalien überwacht.

3.2.3. SCHWACHSTELLENMANAGEMENT Innerhalb der Umgebung werden Schwachstellen-Scans durchgeführt, um potenzielle Schwachstellen in Übereinstimmung mit den jeweils aktuellen Sicherheitsverfahren zu ermitteln, und zwar mindestens vierteljährlich. Wenn Software-Schwachstellen aufgedeckt und durch einen Hersteller-Patch behoben werden, wird der Patch von dem betreffenden Hersteller bezogen und innerhalb eines angemessenen, risikobasierten Zeitrahmens in Übereinstimmung mit den jeweils aktuellen Standardarbeitsanweisungen für die Verwaltung von Schwachstellen und Sicherheitspatches installiert, und zwar erst, nachdem der Patch getestet und als sicher für die Installation in Produktionssystemen befunden wurde.

3.2.4. ANTIVIRUS Antiviren-, Anti-Malware- und Anti-Spyware-Software wird in regelmäßigen Abständen aktualisiert und zentral protokolliert.

3.2.5. ÄNDERUNGSKONTROLLE Alle Änderungen an der Umgebung werden überprüft, um das Risiko zu minimieren. Solche Änderungen werden in Übereinstimmung mit den aktuellen Standardarbeitsanweisungen implementiert.

3.2.6. KONFIGURATIONSMANAGEMENT Für die Systemkomponenten innerhalb der Umgebung werden standardmäßige abgesicherte Konfigurationen beibehalten, die sich an branchenüblichen Absicherungsleitfäden orientieren, wie z. B. den Leitfäden des Center for Internet Security.

3.2.7. DATENVERSCHLÜSSELUNG BEI DER ÜBERTRAGUNG Für die Verschlüsselung von Kundendaten bei der Übertragung über öffentliche Netzwerke wird eine dem Industriestandard entsprechende Verschlüsselung verwendet.

3.2.8. DATENVERCHLÜSSELUNG IM RUHEZUSTAND Die Verschlüsselung von Kundendaten im Ruhezustand wird vom Kunden festgelegt und, falls verschlüsselt, wird sie gemäß den geltenden Angeboten vom Kunden festgelegt.

3.2.9. ILLEGALER CODE UND SICHERE SOFTWAREENTWICKLUNG Der Anbieter befolgt
die in dieser Klausel beschriebenen Praktiken zur sicheren Softwareentwicklung und Codeüberprüfung, um Schäden durch Malware, wie z. B. Viren, Würmer, Datums- oder Zeitbomben oder abgeschaltete Geräte zu verhindern. Die Software wird unter Verwendung von Richtlinien und Verfahren für die sichere Anwendungsentwicklung entwickelt, die sich an Industriestandards wie den OWASP Top Ten oder einem im Wesentlichen gleichwertigen Standard orientieren. Das für den Entwurf und die Entwicklung sicherer Anwendungen zuständige Personal erhält eine angemessene Schulung in Bezug auf die Praktiken zur sicheren Anwendungsentwicklung.

3.2.10. SICHERE CODE-ÜBERPRÜFUNG Vor der Freigabe des Codes an den Kunden wird eine Kombination aus statischen und dynamischen Tests durchgeführt. Schwachstellen werden in Übereinstimmung mit dem jeweils aktuellen Programm zum Management von Software-Schwachstellen behoben. Um Schwachstellen zu beheben, wenn der Code den Kunden zur

Verfügung gestellt wurde, werden den Kunden regelmäßig Software-Patches zur Verfügung gestellt.

3.3 ORGANISATORISCHE SICHERHEITSMASSNAHMEN

3.3.1. PERSONALSICHERHEIT Alle Mitarbeiter und Auftragnehmer, die Zugang zu Kundendaten haben, werden gemäß den geltenden Standardarbeitsanweisungen und vorbehaltlich der geltenden Gesetze einer Hintergrundprüfung unterzogen.

3.3.2. Auftragnehmer, die Zugang zu Kundendaten haben, werden im Hinblick auf Sicherheit und Datenschutz geschult und ausgebildet. Diese Schulungen werden bei der Einstellung und mindestens einmal jährlich während des gesamten Beschäftigungsverhältnisses durchgeführt.

3.3.3. RISIKOMANAGEMENT FÜR ANBIETER Jeder Anbieter, der auf Kundendaten zugreift, sie speichert, verarbeitet oder überträgt, wird daraufhin überprüft, ob er über angemessene Sicherheits- und Datenschutzkontrollen verfügt.

3.3.4. SOFTWARE- UND ASSETINVENTUR Es wird ein Inventar der Softwarekomponenten, einschließlich, aber nicht beschränkt auf Open-Source-Software, die in der Umgebung verwendet wird, geführt.

3.3.5. SICHERHEIT VON ARBEITSPLÄTZEN Auf den Arbeitsplatzrechnern der Mitarbeiter werden Sicherheitsmechanismen wie Firewalls, Virenschutz und eine vollständige Festplattenverschlüsselung mit mindestens AES 256-Bit-Verschlüsselung implementiert und aufrechterhalten. Das Personal wird daran gehindert, die Sicherheitsmechanismen zu deaktivieren.

4. SERVICEKONTINUITÄT

4.1 STANDORT DER DATEN Der Anbieter wird die abonnierten Instanzen in Rechenzentren hosten, die sich in der im Datenverarbeitungszusatz (DPA) oder anderweitig in der vertraglichen Vereinbarung angegebenen geografischen Standardregion befinden und die eine Zertifizierung nach SOC2 Typ 2, ISO 27001 oder eine gleichwertige Zertifizierung bzw. eine Nachfolgezertifizierung erhalten haben.

4.2 DATENSICHERUNG Es werden Backups aller Kundendaten gemäß dem aktuellen, im Portal veröffentlichten Betriebsverfahren durchgeführt.

4.3 NOTFALLWIEDERHERSTELLUNG Es wird ein Plan zur Geschäftskontinuität/Notfallwiederherstellung (Business Continuity/Disaster Recovery Plan, BC/DRP) aufrechterhalten, der mit den Industriestandards für die Umgebung übereinstimmt und: (i) Prozesse zum Schutz von Personal und Vermögenswerten enthält; (ii) den BC/DRP mindestens einmal jährlich testet; (iii) zusammenfassende Testergebnisse zur Verfügung stellt, die den tatsächlichen Wiederherstellungspunkt und die Wiederherstellungszeiten enthalten; und (iv) alle Aktionspläne in den zusammenfassenden Testergebnissen dokumentiert, um etwaige Mängel, Bedenken oder Probleme, die eine Wiederherstellung der Umgebung in Übereinstimmung mit dem BC/DRP verhindert haben oder verhindern könnten, unverzüglich anzugehen und zu beheben.

5. ÜBERWACHUNG UND VORFALLSMANAGEMENT

5.1 ÜBERWACHUNG UND MANAGEMENT VON VORFÄLLEN Systemereignisse werden in

Übereinstimmung mit den aktuellen Standardbetriebsverfahren des Anbieters überwacht und zeitnah analysiert. Bei einem Sicherheitsvorfall werden bei Bedarf Notfallteams eingeschaltet und involviert.

5.2 BENACHRICHTIGUNG ÜBER VERLETZUNGEN

5.2.1. BENACHRICHTIGUNG Der Anbieter meldet dem Kunden jede versehentliche oder unrechtmäßige Zerstörung, jeden Verlust, jede Änderung, jede unbefugte Offenlegung von oder jeden Zugriff auf Kundendaten unverzüglich, nachdem der Anbieter festgestellt hat, dass ein Verstoß vorliegt.

5.2.2. BERICHT Die erste Meldung erfolgt an den Sicherheits- und Datenschutzbeauftragten des Kunden oder den vom Kunden benannten technischen Hauptansprechpartner. Sobald relevante Informationen in Bezug auf den Verstoß gesammelt werden oder dem Anbieter anderweitig zur Verfügung stehen, wird er diese Informationen unverzüglich an den Kunden weitergeben, um ihn bei der Erfüllung seiner Meldepflichten gemäß den Datenschutzgesetzen zu unterstützen. Soweit dies nach vernünftigem Ermessen möglich und angebracht ist, wird der Anbieter dem Kunden die in Artikel 33 der DSGVO beschriebenen Informationen zur Verfügung stellen.

5.2.3. PFLICHTEN DES DATENVERANTWORTLICHEN Der Kunde wird mit dem Anbieter zusammenarbeiten und genaue Kontaktinformationen im Kunden-Support-Portal pflegen und alle Informationen bereitstellen, die vernünftigerweise angefordert werden, um einen Sicherheitsvorfall, einschließlich eines Verstoßes, zu beheben, dessen Ursache(n) zu ermitteln und eine Wiederholung zu verhindern. Der Kunde ist allein dafür verantwortlich, zu entscheiden, ob er die zuständigen Aufsichts- oder Regulierungsbehörden und die betroffenen Personen im Zusammenhang mit einem Verstoß benachrichtigt und dafür, diese Benachrichtigung zu übermitteln.

6. PENETRATIONSTESTS

6.1 VON EXTERNEN DRITTANBIETERN Der Anbieter beauftragt qualifizierte Drittanbieter mit der Durchführung von Penetrationstests der Anwendung und Plattform des Anbieters, um Schwachstellen zu identifizieren. Ausführliche Berichte über die Penetrationstests werden den Kunden im Portal zur Verfügung gestellt.

6.2 VOM KUNDEN Der Kunde kann auf eigene Kosten die Durchführung eines Web-Penetrationstests für Hosting-Umgebungen beantragen, in denen Kundendaten gespeichert sind; vorausgesetzt, der Kunde wird: (i) den Anbieter benachrichtigen und einen Antrag auf Planung eines solchen Tests über das Support-Portal stellen. Falls bei den vom Kunden genehmigten Penetrationstests Schwachstellen festgestellt werden, die der Anbieter reproduzieren kann, wird der Anbieter in Übereinstimmung mit den branchenüblichen Praktiken alle wirtschaftlich vertretbaren Anstrengungen unternehmen, um unverzüglich alle erforderlichen Änderungen vorzunehmen, um die Sicherheit des Dienstes zu verbessern.

7. GEMEINSAME SICHERHEITSVERANTWORTUNG

7.1 PRODUKTFÄHIGKEITEN Der Anbieter stellt eine Vielzahl von Sicherheitseinstellungen zur Verfügung, die es dem Kunden ermöglichen, die Sicherheit der Dienste für seine eigene Nutzung zu konfigurieren, wie z. B.: (i) Benutzer vor dem Zugriff auf die Instanz des Kunden zu authentifizieren; (ii) Passwörter zu verschlüsseln; (iii) Benutzern die Verwaltung von Passwörtern zu ermöglichen; und (iv) auf Anwendungsprotokolle der Instanz zuzugreifen. Der

Kunde verwaltet den Zugriff jedes Benutzers auf die Dienste und deren Nutzung, indem er jedem Benutzer eine Berechtigung und einen Benutzertyp zuweist, der den Grad des Zugriffs auf die entsprechenden Dienste regelt. Der Kunde trägt die alleinige Verantwortung für die Überprüfung des Sicherheitsprogramms und die unabhängige Feststellung, ob es den Anforderungen des Kunden entspricht, wobei die Art und Sensibilität der Kundendaten, die der Kunde dem Anbieter zur Verfügung stellt, berücksichtigt wird. Der Kunde trägt die alleinige Verantwortung für den Schutz der Vertraulichkeit der Anmeldedaten und des Passworts jedes Benutzers und für die Verwaltung des Zugriffs jedes Benutzers auf die Dienste.

7.2 ANSPRECHPARTNER FÜR SICHERHEIT Der Kunde erklärt sich damit einverstanden, für alle Vorfälle im Bereich der Informationssicherheit und für die Kommunikation im Zusammenhang mit der Informationssicherheit innerhalb des Support-Portals einen oder mehrere geeignete Ansprechpartner für die Sicherheit zu benennen und zu unterhalten.

7.3 EINSCHRÄNKUNGEN Ungeachtet anderslautender Bestimmungen in diesen DSM oder anderen Teilen der Vereinbarung gelten die hierin enthaltenen Verpflichtungen des Anbieters nur für die Dienste. Diese DSM gelten nicht für: (i) mit dem Anbieter geteilte Informationen, bei denen es sich nicht um Kundendaten handelt; (ii) Daten im VPN des Kunden oder in einem Netzwerk Dritter; und (iii) Daten, die vom Kunden oder seinen Nutzern unter Verletzung der Vereinbarung oder dieser DSM verarbeitet werden.

ANHANG B

Unterauftragsverarbeiter / Land	Dienstleistungen
Amazon Web Services, Inc. („AWS“) USA; Australien; Kanada; Irland (EU); Singapur; und Vereinigtes Königreich	Cloud-Hosting-Dienst
Microsoft Corporation, USA, Irland, Kanada und Australien	Cloud-Hosting-Dienst
Microsoft Corporation, USA	Outlook-Kalender-Integration
Nournet Company, Saudi-Arabien	Cloud-Hosting-Dienst in Saudi-Arabien
Verbundene Unternehmen des Anbieters • Ungerboeck Systems International, LLC; USA und Neuseeland • Ungerboeck Software International, Pty Ltd.; Australien und Neuseeland • Oletha Pyt Ltd; Indien • Ungerboeck Systems International GmbH; United Kingdom	Kundenbetreuung in Bezug auf Vertragsabwicklung und Dienstleistungen
AC PM, LLC, USA	Anbieter von E-Mail-Diensten (Postmark)

Atlassian US, Inc. USA	Software-Plattform für die Zusammenarbeit
Caffeinated Corporation, USA	Automatisierter Kundensupport, unterstützt durch KI, um den Support zu optimieren und zu automatisieren
Datadog, Inc. USA	Überwachung der Netzwerk- und Infrastrukturleistung

DELIGHTED, LLC, USA	Kundenfeedback-Management-Tool
DocuSign Inc., USA	Integration elektronischer Signaturen und Envelope Provisioning
Dynatrace, LLC, USA	Drittanbieter-Plattform für Überwachung und Protokollierung
Flowgear LLC, USA	Integrationsplattform as a Service
Google, USA	SSO SAML 2.0, Karten- und Kalenderintegration
Jotform, Inc., USA	Integration von Online-Formularen
Okta, Inc., USA	Identitätsanbieter
Pendo.io, Inc., USA	Benutzer-Analyse-Tool
Productboard, Inc., USA	Software zur Produktnachverfolgung
Signiant Inc., USA	Integration des Media-Shuttle-Dienstes zur Datenübermittlung
Stripe, Inc., USA	Zahlungsabwickler
Twilio Inc., USA	Integration der SendGrid-E-Mail-Lösung
Validity, Inc. USA	Plattform für Datenintegrität
Wiz Inc., USA	Cloud-Sicherheitsplattform
Zendesk, Inc. USA	Support-Center und Wissensdatenbank; Ticketing-System für Kunden-Support-Tickets
Full Story, Inc. United States of America	Benutzeranalysetool
CheifSight Corporation United States of America	Geschäftsanalysen
Fivetran, Inc. United States of America	Automatisierte Datenbewegungsplattform
Snowflake, Inc. United States of America	Cloudbasierte Data-Warehouse-Plattform