NACHTRAG ZUR DATENVERARBEITUNG VON COMMAND ALKON INCORPORATED

Aktualisiert: 23.08.2023

Dieser Zusatz zur Datenverarbeitung („**DPA**“) ist Teil der *Hauptlizenz- und Dienstleistungsver*

*einbarung („*Vereinbarung“), die zwischen: (i) dem Kunden (im Hauptlizenz- und Dienstleistungsvertrag identifiziert) und seinen EWR-Tochtergesellschaften („**Kunde**“) geschlossen wurde; und (ii) Command Alkon Incorporated und seinen Tochtergesellschaften („**Unternehmen**“) nur, wenn die Allgemeine Datenschutzverordnung („**GDPR**“) oder andere geltende Gesetze im Bereich der Vertraulichkeit dies erfordern.

Dieser Nachtrag ersetzt alle vorherigen Vereinbarungen zwischen den Parteien in Bezug auf das angesprochene Thema, nämlich die Vertraulichkeit und Sicherheit von Daten gemäß den Datenschutzgesetzen.

In Anbetracht der gegenseitigen Verpflichtungen, die in diesem Dokument dargelegt sind, vereinbaren die Parteien, dass die unten aufgeführten Bedingungen als Ergänzung zum Vertrag hinzugefügt werden.

1. Definitionen

„**Personenbezogene Kundendaten**“ beziehen sich auf personenbezogene daten, die vom Unternehmen im Namen des Kunden im Zusammenhang mit der Bereitstellung von Produkten und/oder Dienstleistungen verarbeitet werden.

„**CCPA**“ bedeutet den California Consumer Privacy Act, geändert durch den California Privacy Rights Act oder andere kalifornische Gesetze/Vorschriften.

„**Betroffene Person**“ bedeutet die Person, auf die sich die personenbezogenen Daten des Kunden beziehen.

„Datenschutzrahmen“ bezeichnet den Rechtsrahmen zwischen der EU und den Vereinigten Staaten für die grenzüberschreitende Übertragung personenbezogener Daten zwischen der Europäischen Union und den Vereinigten Staaten und beinhaltet die britische Erweiterung auf die EU und die Vereinigten Staaten. DPF und DPF zwischen der Schweiz und den Vereinigten Staaten.

„**Datenschutzgesetze**“ bedeutet die Allgemeine Datenschutzverordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten und zur Aufhebung der Richtlinie 95/46/EG (und deren Änderung oder Ersetzung) oder die EU-DSGVO in ihrer geänderten und in britisches Recht übernommenen Fassung gemäß dem British European Union (zurückgezogen) Act von 2018 und den nach diesem Gesetz geltenden Sekundärgesetzen (und aller Änderungen oder Ersetzungen).) oder irgendein anderer geltender Datenschutz Gesetzgebung, die gegebenenfalls eine Datenschutzbehörde vorschreibt (einschließlich des CCPA).

„**Personenbezogene Daten**“ sind alle Informationen, die sich auf eine Betroffene Person beziehen, einschließlich, aber nicht beschränkt auf, einen Namen, eine Identifikationsnummer, Standortdaten, eine Online-Kennung oder einen oder mehrere Faktoren, die spezifisch für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität der betroffenen Person sind.

„**Verarbeiten**“ oder „**Verarbeitung**“ bezeichnet jeden Vorgang oder jede Reihe von Vorgängen, die mit den personenbezogenen Daten des Kunden ausgeführt werden, ob automatisiert oder nicht, wie das Sammeln, Aufzeichnen, Organisieren, Strukturieren, Speichern, Ändern, Abrufen, Verwenden, Löschen, Beschränken, Zugreifen, Verbreiten, Kombinieren, Kopieren, Übertragen, Löschen und/oder Vernichten personenbezogener Kundendaten.

„**Sicherheitsverletzung**“ bedeutet eine bestätigte Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, Offenlegung oder zum unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete Personenbezogene Kundendaten führt.

„**Drittanbieter**“ bedeutet eine andere Partei als den Kunden oder das Unternehmen.

Die Begriffe „**verantwortlicher**“, „**auftragsverarbeiter**“ und „**aufsichtsbehörde**“, wie sie in dieser Datenschutzvereinbarung verwendet werden, werden dieselbe Bedeutung haben, die ihnen in der DSGVO zugewiesen wurde.

Alle anderen Begriffe, die nicht definiert, aber großgeschrieben sind, haben die Bedeutung, die im Vertrag oder in den geltenden Datenschutzgesetzen festgelegt ist.

2. Verarbeitung Personenbezogener Kundendaten

2.1 Zweck der Behandlung. Der Zweck der Datenverarbeitung im Rahmen dieser Datenschutzvereinbarung besteht darin, die Produkte und/oder Dienstleistungen gemäß dem Vertrag bereitzustellen. Anhang 1 beschreibt den Zweck und die Einzelheiten der Verarbeitung personenbezogener Kundendaten.

2.2 Verantwortlichkeiten des Prozessors und des Datenverantwortlichen. Die Parteien erkennen an und vereinbaren, dass: (a) das Unternehmen Personenbezogene Kundendaten gemäß den Datenschutzgesetzen verarbeitet; (b) der Kunde für die Verarbeitung der personenbezogenen Daten des Kunden gemäß den Datenschutzgesetzen verantwortlich ist; (c) der Kunde dafür verantwortlich ist, alle erforderlichen Genehmigungen und Genehmigungen einzuholen, um die personenbezogenen Daten des Kunden einzugeben, zu verwenden, zu speichern und zu verarbeiten, damit das Unternehmen die Produkte und/oder Dienstleistungen liefern kann; und (d) jede Partei wird die geltenden Verpflichtungen einhalten gemäß Datenschutzgesetze in Bezug auf die Verarbeitung von Persönliche Daten des Kunden.

2.3 Amerikanische Datenschutzgesetze. Für die Zwecke der US-Datenschutzgesetze (einschließlich des CCPA) umfasst „datenverantwortlicher“ „unternehmen“, „auftragsverarbeiter“ umfasst „dienstleister“, „Betroffene Person“ umfasst

„verbraucher“ und „Personenbezogene Daten“ umfasst „personenbezogene daten“. Das Unternehmen ist ein dienstleister und der Kunde ist ein unternehmen.

2.4 Anweisungen für Kunden. Der Kunde verlangt, dass das Unternehmen seine personenbezogenen Daten verarbeitet: (a) gemäß dem Vertrag und allen anwendbaren Ergänzungen; (b) soweit erforderlich, um dem Kunden die Produkte und/oder Dienstleistungen zur Verfügung zu stellen; (c) gemäß den geltenden Gesetzen oder Vorschriften; und (d) andere angemessene schriftliche Anweisungen des Kunden zu befolgen, wenn diese Anweisungen den Vertragsbedingungen entsprechen. Der Kunde wird sicherstellen, dass seine Anweisungen für die Verarbeitung seiner personenbezogenen Daten den Datenschutzgesetzen entsprechen. Zwischen den Parteien ist der Kunde allein verantwortlich für die Richtigkeit, Qualität und Rechtmäßigkeit seiner personenbezogenen Daten und die Art und Weise, wie der Kunde sie erhalten hat.

2.5 Einhaltung der Anweisungen des Kunden durch das Unternehmen. Das Unternehmen verarbeitet die personenbezogenen Daten des Kunden nur gemäß den Anweisungen des Kunden und behandelt die personenbezogenen Daten des Kunden als vertrauliche Informationen. Wenn das Unternehmen glaubt oder erfährt, dass Anweisungen des Kunden gegen Datenschutzgesetze verstoßen, wird es den Kunden innerhalb einer angemessenen Frist informieren. Das Unternehmen kann Personenbezogene Kundendaten auf andere Weise als gemäß den schriftlichen Anweisungen des Kunden Verarbeiten, wenn dies nach geltendem Recht, dem das Unternehmen unterliegt, erforderlich ist. In diesem Fall wird das Unternehmen den Kunden vor der Verarbeitung der personenbezogenen Daten des Kunden über diese Anforderung informieren, sofern dies nicht nach geltendem Recht verboten ist.

2.6 CCPA-Behandlung. Soweit die Verarbeitung personenbezogener Daten durch das Unternehmen dem CCPA unterliegt, bestätigt das Unternehmen, dass es nicht: (a) Personenbezogene Kundendaten verwalten, verwenden oder weitergeben darf, um die Produkte und/oder Dienstleistungen bereitzustellen, die Qualität der Produkte und/oder Dienstleistungen zu schaffen oder zu verbessern, Sicherheitsvorfälle aufzudecken, vor betrügerischen oder illegalen Aktivitäten zu schützen, Subunternehmer gemäß dieser DPA einzusetzen oder wie von der CCPA; oder (b) persönliche Kundendaten verkaufen oder weitergeben.

3. Unterauftragsverarbeiter

3.1 Benennung von Subunternehmern. Der Kunde erteilt hiermit eine allgemeine schriftliche Genehmigung, die es dem Unternehmen ermöglicht, externe Subunternehmer zu beauftragen, um eingeschränkte oder ergänzende Dienstleistungen im Zusammenhang mit der Bereitstellung von Produkten und/oder Dienstleistungen zu erbringen. Auf der Website des Unternehmens sind die Unterauftragsverarbeiter aufgeführt, die das Unternehmen derzeit mit der Durchführung bestimmter Verarbeitungsaktivitäten im Zusammenhang mit personenbezogenen Kundendaten beauftragt (https://commandalkon.com/sub-processor-list/) und das Unternehmen wird die Liste der Unterauftragsverarbeiter aktualisieren, bevor es einen neuen Auftragsverarbeiter mit der Durchführung einer bestimmten Verarbeitung beauftragt. Der Kunde kann sich anmelden, um elektronische Updates zu erhalten, wenn sich die

Liste der Subunternehmer des Unternehmens ändert, indem er eine solche Anfrage an privacy@commandalkon.com sendet. Der Kunde kann gegen jeden Subunternehmer Einspruch erheben, indem er dem Unternehmen seinen Einwand innerhalb von dreißig (30) Tagen nach der Aktualisierung mitteilt, und die Parteien werden nach bestem Wissen und Gewissen daran arbeiten, den Einwand zu lösen. Der Kunde akzeptiert hiermit die Unterverarbeitungsaktivitäten, die von den aktuellen Subunternehmern durchgeführt werden, die auf der Website des Unternehmens aufgeführt sind.

3.2 Sicherheit von Unterprozessoren. Wenn das Unternehmen seine Verpflichtungen an Unterauftragnehmer vergibt, wird es dies nur durch eine schriftliche Vereinbarung mit dem Subunternehmer tun, die vertraglichen Verpflichtungen auferlegt, die mindestens denen entsprechen, die dem Unternehmen im Rahmen dieses Zusatzes auferlegt wurden.

3.3 Verantwortung. Wenn der Subunternehmer seinen Datenschutzverpflichtungen aus einer solchen schriftlichen Vereinbarung nicht nachkommt, bleibt das Unternehmen dem Kunden gegenüber voll verantwortlich für die Erfüllung der Verpflichtungen des Subunternehmers aus dieser Vereinbarung.

4. Verantwortlichkeiten im Bereich Sicherheit

4.1 Unternehmenssicherheit. Das Unternehmen wird angemessene technische und organisatorische Maßnahmen ergreifen, um die personenbezogenen Daten der Kunden zu schützen („**Informationssicherheitsprogramm**“), wobei der Stand der Technik, die Implementierungskosten, die Art, der Umfang, der Kontext und die Ziele der Verarbeitung sowie das mehr oder weniger wahrscheinliche Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden. Das Unternehmen arbeitet nach den folgenden Sicherheitsstandards: NIST 800-171; AWS CIS.

4.2 Kundensicherheit. Der Kunde erkennt an, dass die Produkte und/oder Dienstleistungen bestimmte Merkmale und Funktionen beinhalten, die er nutzen kann und die Auswirkungen auf die Sicherheit der personenbezogenen Daten des Kunden haben, die im Zusammenhang mit der Nutzung der Produkte und/oder Dienstleistungen verarbeitet werden. Der Kunde ist dafür verantwortlich, die vom Unternehmen zur Verfügung gestellten Informationen zur Sicherheit seiner Daten zu überprüfen und unabhängig festzustellen, ob die Produkte und/oder Dienstleistungen den gesetzlichen Anforderungen und Verpflichtungen des Kunden entsprechen, einschließlich seiner Verpflichtungen gemäß den geltenden Datenschutzgesetzen. Der Kunde ist auch für die korrekte Konfiguration der Produkte und/oder Dienstleistungen und die Nutzung der vom Unternehmen zur Verfügung gestellten Funktionen verantwortlich, um angesichts der Art der personenbezogenen Daten des Kunden, die im Zusammenhang mit der Nutzung der Produkte und/oder Dienstleistungen durch den Kunden verarbeitet werden, angemessene Sicherheit zu gewährleisten. Der Kunde ist verantwortlich für die Nutzung der Produkte und/oder Dienstleistungen und für die Speicherung aller Kopien seiner personenbezogenen Daten außerhalb der Systeme des Unternehmens oder der Subunternehmer des Unternehmens, einschließlich, aber nicht beschränkt auf die Sicherung von Anmeldeinformationen,

Kontoauthentifizierungssystemen und Geräten sowie die Aufbewahrung von Kopien seiner personenbezogenen Kundendaten, falls zutreffend.

4.3 Mitarbeiter des Unternehmens. Das Unternehmen muss sicherstellen, dass sein Personal, das für die Verarbeitung personenbezogener Kundendaten verantwortlich ist, über den vertraulichen Charakter personenbezogener Kundendaten informiert ist, eine angemessene Schulung zu seinen Aufgaben erhalten hat und Vertraulichkeitsverpflichtungen unterliegt, wobei diese Verpflichtungen auch nach dem Ende der Tätigkeit dieser Person im Unternehmen fortbestehen.

4.4 Sicherheitstests. Das Unternehmen wird die Wirksamkeit des Informationssicherheitsprogramms testen, bewerten und bewerten, um die sichere Verarbeitung personenbezogener Kundendaten zu gewährleisten. Das Unternehmen wird sein Informationssicherheitsprogramm einhalten und versichert und garantiert, dass sein Informationssicherheitsprogramm den geltenden Gesetzen entspricht und dies auch weiterhin tun wird.

4.5 Folgenabschätzungen. Das Unternehmen wird angemessene Schritte Unternehmen, um mit dem Kunden zusammenzuarbeiten und ihn bei der Durchführung von Folgenabschätzungen und damit verbundenen Konsultationen mit Aufsichtsbehörden zu unterstützen, falls der Kunde aufgrund der Datenschutzgesetze verpflichtet ist, solche Folgenabschätzungen durchzuführen.

5. Rechte der Betroffenen Personen

5.1 Unterstützung bei der Erfüllung von Kundenverpflichtungen. Soweit der Kunde bei der Nutzung oder beim Empfang der Produkte und/oder Dienstleistungen nicht in der Lage ist, seine personenbezogenen Daten gemäß den Datenschutzgesetzen zu korrigieren, zu ändern, einzuschränken, zu sperren oder zu löschen, muss das Unternehmen umgehend auf angemessene Anfragen des Kunden reagieren, um solche Maßnahmen zu ermöglichen, soweit das Unternehmen dazu berechtigt und in der Lage ist. Sofern gesetzlich zulässig, ist der Kunde für alle Kosten verantwortlich, die mit der Bereitstellung dieser Unterstützung durch das Unternehmen verbunden sind.

5.2 Mitteilungspflichten. Soweit gesetzlich zulässig, wird das Unternehmen den Kunden umgehend informieren, wenn es einen Antrag auf Zugang, Korrektur, Änderung, Löschung oder Widerspruch gegen die Verarbeitung personenbezogener Kundendaten, die diese Person betreffen, erhält. Das Unternehmen wird ohne die vorherige schriftliche Zustimmung des Kunden keine solche Anfrage bezüglich der personenbezogenen Daten des Kunden beantworten, es sei denn, um zu bestätigen, dass sich die Anfrage auf den Kunden bezieht. Darüber hinaus wird das Unternehmen, soweit gesetzlich zulässig, den Kunden umgehend informieren, wenn es von einer Strafverfolgungsbehörde, einer zuständigen Behörde oder einer zuständigen Datenschutzbehörde eine Anfrage zur Offenlegung oder Korrespondenz, eine Mitteilung oder eine andere Mitteilung über die personenbezogenen Daten des Kunden erhält. Das Unternehmen bietet dem Kunden angemessene und angemessene Zusammenarbeit und Unterstützung bei der Bearbeitung einer solchen Anfrage, soweit dies gesetzlich zulässig ist und sofern der Kunde durch die Nutzung oder den Erhalt der Produkte und/oder Dienstleistungen keinen Zugriff auf diese personenbezogenen Kundendaten hat. Sofern gesetzlich zulässig, ist der Kunde für

alle Kosten verantwortlich, die mit der Bereitstellung dieser Unterstützung durch das Unternehmen verbunden sind.

6. Verletzung Personenbezogener Daten

6.1 Mitteilungspflichten. Wenn das Unternehmen von einer nachgewiesenen Sicherheitsverletzung erfährt, die die personenbezogenen Daten des Kunden betrifft, wird es den Kunden so schnell wie möglich und in jedem Fall nicht später als zweiundsiebzig (72) Stunden nach ihrer Entdeckung informieren. Die in diesem Abschnitt 6 festgelegten Verpflichtungen gelten nicht für Vorfälle, die von Kunden oder Kundenpersonal oder Endbenutzern verursacht wurden, oder für erfolglose Versuche oder Aktivitäten, die die Sicherheit personenbezogener Kundendaten nicht gefährden, einschließlich erfolgloser Anmeldeversuche, Pings, Port-Scans, Denial-of-Service-Angriffe und andere Netzwerkangriffe gegen Firewalls oder Netzwerksysteme.

6.2 Benachrichtigungsmodus. Benachrichtigungen über Sicherheitsverletzungen, falls vorhanden, werden per E-Mail oder Telefon an den Ansprechpartner des Kunden gesendet. Es liegt in der alleinigen Verantwortung des Kunden, dafür zu sorgen, dass er jederzeit korrekte Kontaktinformationen in den Supportsystemen des Unternehmens hat. Der Kunde ist allein verantwortlich für die Einhaltung der für den Kunden geltenden Meldepflichten und für jegliche Verpflichtung, Dritte im Zusammenhang mit einer Verletzung der Sicherheit personenbezogener Daten zu benachrichtigen.

6.3 Inhalt der Benachrichtigung. Wenn eine Benachrichtigung erforderlich ist, sollte sie mindestens:

6.3.1 beschreiben Sie die Art der Sicherheitsverletzung, die Kategorien und die Anzahl der betroffenen Personen sowie die Kategorien und die Anzahl der betroffenen personenbezogenen Datensätze;

6.3.2 teilen Sie den Namen und die Kontaktdaten des jeweiligen Unternehmenskontakts mit, bei dem weitere Informationen erhältlich sind;

6.3.3 beschreiben Sie die wahrscheinlichen Folgen der Sicherheitsverletzung; und

6.3.4 Beschreiben Sie die Maßnahmen, die ergriffen oder vorgeschlagen wurden, um diese Sicherheitsverletzung zu beheben.

7. Löschung oder Rückgabe personenbezogener Kundendaten

7.1 Entfernen oder Zurückgeben. Vorbehaltlich von Abschnitt 7.3 verpflichtet sich das Unternehmen, die personenbezogenen Daten des Kunden umgehend und in jedem Fall innerhalb von dreißig (30) Tagen ab dem Datum der Einstellung aller Dienstleistungen, die die Verarbeitung personenbezogener Kundendaten beinhalten (das „**Kündigungsdatum**“), die personenbezogenen Daten des Kunden sicher zu löschen oder, auf schriftliche Anfrage des Kunden rechtzeitig, eine vollständige Kopie

aller personenbezogenen Kundendaten durch sichere Dateiübertragung in dem vom Kunden vernünftigerweise gewünschten Format zurückzugeben..

7.2 Definition von Unterdrückung. Für weitere Informationen bedeutet „**Löschen**“, die personenbezogenen Daten des Kunden zu löschen oder zu löschen, sodass sie nicht wiederhergestellt oder rekonstruiert werden können.

7.3 Aufzeichnungen. Das Unternehmen kann Personenbezogene Kundendaten speichern, soweit dies nach geltendem Recht oder gemäß dem Zeitplan des Unternehmens zur Aufbewahrung von Dokumenten erforderlich ist, vorausgesetzt, dass das Unternehmen die Vertraulichkeit all dieser personenbezogenen Kundendaten gewährleistet.

8. Prüfungsrechte

8.1 Prüfungsrechte. Nicht öfter als einmal pro Jahr darf der Kunde einen einvernehmlich vereinbarten Dritten mit der Prüfung des Unternehmens beauftragen, ausschließlich zu dem Zweck, seine Prüfanforderungen gemäß Artikel 28, Abschnitt 3 (h) der DSGVO zu erfüllen. Um ein Audit zu beantragen, muss der Kunde mindestens vier (4) Wochen vor dem geplanten Audittermin einen detaillierten Auditplan einreichen, in dem der vorgeschlagene Umfang, die Dauer und das Startdatum des Audits beschrieben werden. Prüfanfragen sollten an privacy@commandalkon.com gesendet werden. Der Wirtschaftsprüfer muss vor der Durchführung des Audits eine schriftliche Vertraulichkeitsvereinbarung unterzeichnen, die für das Unternehmen akzeptabel ist. Das Audit sollte während der regulären Geschäftszeiten gemäß den Unternehmensrichtlinien durchgeführt werden und sollte die Geschäftsaktivitäten des Unternehmens nicht unangemessen beeinträchtigen. Alle Audits erfolgen auf Kosten und Kosten des Kunden. Das Unternehmen wird mit jedem Kunden oder jeder Prüfungsanfrage einer zuständigen Regulierungs- oder Aufsichtsbehörde zusammenarbeiten, um zu überprüfen, ob das Unternehmen seinen Verpflichtungen gemäß dieser DPA nachkommt, indem es, vorbehaltlich der Vertraulichkeitsverpflichtungen, Prüfberichte Dritter, falls zutreffend, und/oder Beschreibungen von Sicherheitskontrollen und andere Informationen, die der Kunde vernünftigerweise verlangt, über die Sicherheitspraktiken und -richtlinien des Unternehmens zur Verfügung stellt.

8.2 Unterstützung bei der Einhaltung von Vorschriften. Angesichts der Art der Verarbeitung und der dem Unternehmen zur Verfügung gestellten Informationen wird das Unternehmen dem Kunden eine angemessene und angemessene Zusammenarbeit und Unterstützung in Bezug auf die in den Artikeln 32 bis 36 der RGPD beschriebenen Compliance-Verpflichtungen des Kunden bieten.

9. Datenübertragungen

9.1 Allgemeine Genehmigung. Der Kunde erklärt sich damit einverstanden, dass das Unternehmen, vorbehaltlich von Abschnitt 9.2, Personenbezogene Kundendaten in den Vereinigten Staaten von Amerika und jedem anderen Land, in dem das Unternehmen oder einer seiner Subunternehmer Einrichtungen hat oder Personenbezogene Daten anderweitig verarbeitet, speichern und Verarbeiten kann. Jede solche Übertragung wird in erster Linie durch die Data Privacy Framework-

Zertifizierung des Unternehmens oder, falls nicht, durch die miteinander verbundenen Standardvertragsklauseln des Unternehmens geregelt. Das Unternehmen wird die personenbezogenen Daten des Kunden nicht von einer Gerichtsbarkeit in eine andere übertragen oder deren Übertragung veranlassen, außer in Übereinstimmung mit geltendem Recht, und es wird vom Kunden nicht verlangen, gegen Datenschutzgesetze zu verstoßen.

9.2 Standardvertragsklauseln. In dem Umfang und nur in dem Umfang, in dem das Unternehmen Personenbezogene Kundendaten aus dem Europäischen Wirtschaftsraum verarbeitet und Standardvertragsklauseln erforderlich sind, gilt Modul 2 der Standardvertragsklauseln und ist hier enthalten. Für die Zwecke der Standardvertragsklauseln ist der Kunde der „Datenexporteur“ und das Unternehmen der „Datenimporteur“.

9.3 Britischer Nachtrag zu den EU-Standardvertragsklauseln. In dem Umfang und nur in dem Umfang, in dem das Unternehmen Personenbezogene Kundendaten aus dem Vereinigten Königreich verarbeitet und Standardvertragsklauseln erforderlich sind, vereinbaren die Parteien, dass der britische Zusatz für Personenbezogene Daten gilt, die über die Produkte und/oder Dienstleistungen aus dem Vereinigten Königreich direkt oder durch Weiterleitung in ein Land oder einen Empfänger außerhalb des Vereinigten Königreichs übertragen werden, das von der zuständigen britischen Aufsichtsbehörde oder Regierungsbehörde für das Vereinigte Königreich nicht als ausreichend Schutzniveau anerkannt ist persönliche Daten.

9.4 Schweizer FADP. In dem Umfang und nur in dem Umfang, in dem das Unternehmen Personenbezogene Kundendaten aus der Schweiz verarbeitet, gelten die folgenden zusätzlichen Anforderungen, sofern Datenübertragungen ausschließlich dem FADP oder sowohl dem FADP als auch der EU-DSGVO unterliegen: (a) Der Begriff „Mitgliedstaat“ sollte nicht so ausgelegt werden, dass Datensubjekte in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (der Schweiz) gemäß Klausel 18 geltend zu machen (c) der Klauseln Standardvertragsklauseln; (b) soweit Datenübertragungen, die den Standardvertragsklauseln zugrunde liegen, unterliegen ausschließlich dem FADP, Verweise auf die EU-DSGVO sollten als Verweise auf das FADP betrachtet werden; (c) soweit Datenübertragungen, die den Standardvertragsklauseln zugrunde liegen, sowohl dem FADP als auch der EU-DSGVO unterliegen, sollten Verweise auf die EU-DSGVO als Verweise auf das FADP betrachtet werden, sofern die Datenübertragungen dem FADP unterliegen; und (d) bis zum Schweizer Recht zum Datenschutz (Rev. (FADP) tritt in Kraft, auch die Bestimmungen der Standardvertragsklauseln schützt die personenbezogenen Daten der Kunden, soweit diese Bestimmungen nach schweizerischem Recht auf sie anwendbar sind.

9.5 Zusätzliche Maßnahmen. Zusätzlich zu den Standardvertragsklauseln gilt: Wenn das Unternehmen erfährt, dass eine Regierungsbehörde (einschließlich Strafverfolgungsbehörden) auf einige oder alle der vom Unternehmen verarbeiteten personenbezogenen Kundendaten zugreifen möchte, sei es auf freiwilliger oder obligatorischer Basis, für Zwecke der nationalen Sicherheitsnachrichtendienste, dann wird das Unternehmen, sofern dies nicht gesetzlich oder gesetzlich vorgeschrieben ist,: 1) den Kunden, für den die personenbezogenen Daten gelten, unverzüglich

informieren; 2) wird die zuständige Regierungsbehörde informieren, nicht wurde ermächtigt, den Kunden offenzulegen Personenbezogene Daten und muss, sofern nicht gesetzlich verboten, den Kunden, für den die personenbezogenen Daten des Kunden gelten, unverzüglich informieren; 3) die Regierungsbehörden darüber informieren, dass sie alle Anfragen oder Anfragen direkt an den Kunden richten müssen, für den die personenbezogenen Daten des Kunden gelten; und 4) keinen Zugriff auf die personenbezogenen Kundendaten gewähren müssen, bevor keine schriftliche Genehmigung des betreffenden Kunden eingeholt wurde oder gesetzlich dazu verpflichtet ist. Falls gesetzlich vorgeschrieben, wird das Unternehmen angemessene und rechtliche Anstrengungen Unternehmen, um dieses Verbot oder diese Beschränkung anzufechten. Wenn das Unternehmen verpflichtet ist, die personenbezogenen Daten des Kunden herauszugeben, wird es die personenbezogenen Daten des Kunden nur in dem gesetzlich vorgeschriebenen Umfang gemäß dem geltenden rechtlichen Verfahren weitergeben.

9.6 Gesetz zur Überwachung Ausländischer Nachrichtendienste. Das Unternehmen hatte noch keine Anweisung gemäß Abschnitt 702 des U.S. Foreign Intelligence Surveillance Act, kodifiziert in 50 U.S.C. §1881a („FISA Section 702"), erhalten. Kein Gericht war der Ansicht, dass das Unternehmen für eine Behandlung gemäß FISA-Abschnitt 702 in Frage kommt. Das Unternehmen gehört nicht zu den Lieferanten, die gemäß Abschnitt 702 der FISA, wie in der *Schrems* II-Entscheidung beschrieben, für eine vorgelagerte Abholung („Sammelabholung") in Frage kommen.

9.7 Priorität bei der Übertragung. Wenn die Dienste durch mehrere Übertragungsmechanismen abgedeckt sind, unterliegt die Übertragung personenbezogener Kundendaten einem einzigen Übertragungsmechanismus gemäß der folgenden Prioritätsreihenfolge: (i) Zertifizierung des Corporate Data Privacy Framework; (ii) EU-Standardvertragsklauseln (sofern nach geltendem Datenschutzrecht erforderlich).

10. Dauer und Kündigung

Dauer der DPA. Dieses DPA tritt an dem Tag in Kraft, an dem der Vertrag vollständig ausgeführt wird, und bleibt unabhängig vom Ablauf der Laufzeit eines gekauften Abonnements in Kraft, bis alle personenbezogenen Kundendaten gelöscht sind, wie in dieser DPA beschrieben.

11. Nichteinhaltung; Rechtsbehelfe; Parteien

11.1 Haftungsbeschränkung. Die Haftung des Unternehmens für die Verletzung seiner Verpflichtungen aus diesem DPA unterliegt den Haftungsbeschränkungsbestimmungen des Vertrags.

11.2 Parteien dieser Datenschutzbehörde. Nichts in der DPA verleiht einer anderen Person oder Organisation als den Parteien dieser DPA Vorteile oder Rechte.

12. Allgemeine Bedingungen

Anwendbares recht und gerichtsstand

12.1 Diese Datenschutzvereinbarung wird ein Jahr nach ihrer Veröffentlichung und drei Jahre später, oder gegebenenfalls früher, überprüft.

12.2 Sofern nicht durch die Standardvertragsklauseln vorgeschrieben:

12.2.1 Die Parteien dieses Zusatzes unterwerfen sich der im Vertrag festgelegten Gerichtsstandswahl in Bezug auf alle Streitigkeiten oder Ansprüche, die sich aus diesem Zusatz ergeben, einschließlich Streitigkeiten über seine Existenz, Gültigkeit oder Kündigung; und

12.2.2 Dieser Nachtrag und alle außervertraglichen oder sonstigen Verpflichtungen, die sich aus oder im Zusammenhang damit ergeben, unterliegen den Gesetzen des Landes oder Territoriums, das für diesen Zweck im Vertrag festgelegt ist.

Reihenfolge der rangfolge

12.3 Im Falle eines Konflikts oder einer Inkonsistenz zwischen diesem Nachtrag und den Standardvertragsklauseln, in denen die Standardvertragsklauseln erforderlich sind, haben die Standardvertragsklauseln Vorrang.

12.4 Vorbehaltlich von Abschnitt 12.2, in Bezug auf den Gegenstand dieser Ergänzung, haben im Fall von Widersprüchen zwischen den Bestimmungen dieses Zusatzes und allen anderen Vereinbarungen zwischen den Parteien, einschließlich des Vertrags und einschließlich (sofern nicht ausdrücklich schriftlich vereinbart, im Namen der Parteien unterzeichnet) Vereinbarungen, die nach dem Datum dieses Zusatzes abgeschlossen wurden oder angeblich geschlossen wurden, die Bestimmungen dieses Zusatzes Vorrang.

Änderungen der Datenschutzgesetze

12.5 Der Kunde kann:

12.5.1 indem Sie das Unternehmen von Zeit zu Zeit schriftlich mit einer Frist von mindestens dreißig (30) Kalendertagen benachrichtigen, alle Änderungen der Standardvertragsklauseln vorschlagen, die aufgrund einer Änderung oder Entscheidung einer zuständigen Behörde nach diesem Datenschutzgesetz erforderlich wären; und

12.5.2 schlagen Sie jede andere Variante dieses Zusatzes vor, die der Kunde für vernünftigerweise notwendig hält, um die Anforderungen aller Datenschutzgesetze zu erfüllen.

12.6 Wenn der Kunde gemäß Abschnitt 12.5 eine Mitteilung macht, werden die Parteien die vorgeschlagenen Varianten umgehend erörtern und in gutem Glauben verhandeln, um diese Varianten oder andere Varianten, die darauf ausgelegt sind, die in der Benachrichtigung des Kunden genannten Anforderungen so schnell wie möglich zu vereinbaren und umzusetzen.

Vergütung

12.7 Falls eine Bestimmung dieses Zusatzes ungültig oder nicht durchsetzbar ist, bleibt der Rest dieses Zusatzes gültig und wirksam. Die ungültige oder nicht durchsetzbare Bestimmung muss entweder: (i) nach Bedarf geändert werden, um ihre Gültigkeit und Durchsetzbarkeit zu gewährleisten, wobei die Absichten der Parteien maximal gewahrt bleiben, oder, falls dies nicht möglich ist; (ii) so ausgelegt werden, dass der ungültige oder nicht durchsetzbare Teil nie darin enthalten war.

Anhang I — Einzelheiten zur Datenverarbeitung

Datenexporteur (Datenverantwortlicher): Kunde, wie im Vertrag angegeben.

Datenimporteur (Auftragsverarbeiter): Firma, wie im Vertrag angegeben.

Zweck: Der Zweck der Datenverarbeitung im Rahmen dieser Datenschutzvereinbarung betrifft Personenbezogene Kundendaten.

Dauer der Verarbeitung: Die Dauer des Vertrags plus der Zeitraum, bis das Unternehmen alle personenbezogenen Kundendaten gemäß dieser Datenschutzvereinbarung löscht.

Zweck: Der Zweck der Datenverarbeitung ist die Bereitstellung von Produkten und/oder Dienstleistungen für den Kunden.

Art der Verarbeitung: Die Art der Datenverarbeitung ist für die Bereitstellung der Produkte und/oder Dienstleistungen vorgesehen, wie im Vertrag beschrieben.

Kategorien von Datensubjekten: Mitarbeiter von Kunden und Mitarbeiter von Tochtergesellschaften, Kunden und Geschäftspartner des Kunden.

Arten Personenbezogener Daten: Der Kunde kann bestimmte Personenbezogene Daten in Bezug auf Produkte und/oder Dienstleistungen hochladen, einreichen oder bereitstellen, deren Umfang im Allgemeinen vom Kunden nach eigenem Ermessen festgelegt und kontrolliert wird und Kontaktinformationen, Informationen über Interaktionen mit der Website, Produkten und Dienstleistungen, Adressen, Geolokalisierungsinformationen, E-Mail-Adressen, Namen, Geschlecht, Titel, Telefonnummern, Führerscheinnummer, Unterschrift, Mitarbeiternummer, Lohnsatz, Passwort beinhalten kann; Leistungsinformationen; Qualifikationen und Einschränkungen; Geräteinformationen.

Sensible Daten Übertragen: keine.

Übertragungsfrequenz: kontinuierlich, je nach Bedarf für die Bereitstellung von Produkten und/oder Dienstleistungen.

Transfers an Subunternehmer: Wie in der Liste der Unterauftragsverarbeiter des Unternehmens beschrieben, die unter verfügbar ist https://commandalkon.com/sub-processor-list/.

Zuständige Aufsichtsbehörde: gemäß den geltenden Datenschutzgesetzen oder, in der Reihenfolge ihres Inkrafttretens, 1) gemäß den Vertragsbedingungen oder 2) der niederländischen Datenschutzbehörde.

Aufbewahrung: gemäß dem Vertrag und dieser Datenschutzvereinbarung.

Technische und Organisatorische Maßnahmen: Die vom Datenimporteur getroffenen technischen und organisatorischen Sicherheitsmaßnahmen sind in Abschnitt 4.1 der Datenschutzvereinbarung beschrieben. Zusätzliche Informationen sind auf Anfrage erhältlich.