COMMAND ALKON INCORPORATED
DATENVERARBEITUNGSZUSATZ

Aktualisiert: 12/06/2022

Dieser Datenverarbeitungszusatz („**DVZ**“) ist Teil des *Rahmenlizenz- und Dienstleistungsvertrags* („**Vertrag**“) zwischen: (I) Kunde (in der nachstehenden Unterschriftszeile angegeben) und seinen EWR-Tochtergesellschaften **("Kunde");** und (ii) Command Alkon Incorporated und seinen Tochtergesellschaften („**Unternehmen**“) nur wenn dies durch die Datenschutz-Grundverordnung („DSGVO“) oder andere geltende Datenschutzgesetze vorgeschrieben ist.

Dieser Nachtrag ersetzt alle vorherigen Vereinbarungen zwischen den Parteien in Bezug auf den hierin enthaltenen Gegenstand, d. h. Datenschutz und Sicherheit gemäß der DSGVO.

In Anbetracht der hier dargelegten gegenseitigen Verpflichtungen vereinbaren die Parteien hiermit, dass die nachstehenden Bedingungen als Zusatz zum Vertrag hinzugefügt werden.

1. Definitionen

„**Personenbezogen Daten des Kunden**“ sind personenbezogene Daten, die das Unternehmen im Namen des Kunden bei der Bereitstellung der produkte und/oder dienstleistungen verarbeitet.

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

„**Datenschutzgesetze**“ bezeichnet die Datenschutz-Grundverordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr solcher Daten, und durch die die Richtlinie 95/46/EG (und jede Änderung oder Ersetzung derselben) aufgehoben ist, das Schweizerische Bundesgesetz über den Datenschutz vom 19. Juni 1992 (und jede Änderung oder Ersetzung desselben) oder die EU-DSGVO in der geänderten Fassung, die gemäß dem Gesetz zum Austritt des Vereinigten Königreichs aus der Europäischen Union 2018 (UK European Union (Withdrawal) Act 2018) in das britische Recht übernommen wurde, und das gemäß diesem Gesetz erlassene Sekundärrecht (und jede Änderung oder Ersetzung desselben), je nachdem, was anwendbar ist.

“**Personenbezogene Daten**” sind alle Informationen die sich auf eine betroffene Person beziehen, einschließlich aber nicht beschränkt auf einen Namen, eine Kennnummer, Standortdaten, einer Online-Kennung, oder auf ein oder mehrere Merkmale die spezifisch für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität der betroffenen Person sind.

„**Privacy Shield**“ bezeichnet die rechtlichen Rahmenwerke des EU-U.S. Privacy Shield und des Schweiz-U.S. Privacy Shield. Obwohl beide Rahmenwerke derzeit für ungültig erklärt sind, hält sich das Unternehmen weiterhin an dessen Anforderungen, und diese Klausel gilt für jede erneuerte und genehmigte Version des Privacy-Shield-Abkommens zwischen den Vereinigten Staaten und dem Europäischen Wirtschaftsraum („EWR“).

„**Verarbeiten**“ oder „**Verarbeitung**“ ist jeder Vorgang oder jede Reihe von Vorgängen, die mit den personenbezogenen Daten des Kunden durchgeführt werden, unabhängig davon, ob sie automatisiert sind oder nicht, wie z. B. das Erheben, das Aufzeichnen, die Organisation, die Strukturierung, die Speicherung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung, die Beseitigung, die Einschränkung, der Zugang, die Verbreitung, die Kombination, die Anpassung, das Kopieren, die Übertragung, das Löschen und/oder die Vernichtung der personenbezogenen Daten des Kunden.

„**Sicherheitsverletzung**“ ist eine bestätigt Verletzung der Sicherheit, die zu einer versehentlichen oder unrechtmäßigen Zerstörung, einem Verlust, einer Änderung, einer unbefugten Offenlegung von oder einem Zugriff auf persönliche Daten des Kunden führt, die übertragen, gespeichert oder anderweitig verarbeitet werden.

„**Dritte**“ bezeichnet eine andere Partei als der Kunde oder das Unternehmen.

Die Begriffe „**Verantwortlicher**“, „**Auftragsverarbeiter**“, und „**Aufsichtsbehörde**” wie sie in dieser DVZ verwendet werden, haben die ihnen in der DSGVO zugewiesene Bedeutung.

Alle anderen nicht definierten, aber großgeschriebenen Begriffe haben die im Vertrag festgelegte Bedeutung.

2. Verarbeitung von personenbezogenen Kundendaten

2.1 Zweck der Verarbeitung. Der Zweck der Datenverarbeitung gemäß dieser DVZ ist die Bereitstellung der produkte und/oder dienstleistungen gemäß dem Vertrag. Anhang 1 beschreibt den Gegenstand und die Einzelheiten der Verarbeitung der personenbezogenen Daten des Kunden.

2.2 Verantwortlichkeiten des Auftragsverarbeiters und des Verantwortlichen. Die Parteien erkennen an und vereinbaren, dass: (a) das Unternehmen ein Auftragsverarbeiter der personenbezogenen Daten des Kunden gemäß den Datenschutzgesetzen ist; (b) der Kunde ein Verantwortlicher für die personenbezogenen Daten des Kunden gemäß den Datenschutzgesetzen ist; und (c) jede Partei die für sie geltenden Verpflichtungen gemäß den Datenschutzgesetzen in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden einhalten wird.

2.3 Anweisungen des Kunden. Der Kunde weist das Unternehmen an, die persönlichen Daten des Kunden zu verarbeiten: (a) in Übereinstimmung mit dem Vertrag und allen anwendbaren Ergänzungen; (b) wie anderweitig erforderlich, um die Produkte und/oder Dienstleistungen für den Kunden bereitzustellen; (c) wie erforderlich, um anwendbare Gesetze oder Vorschriften einzuhalten; und (d) um andere angemessene schriftliche Anweisungen des Kunden zu befolgen, sofern diese Anweisungen mit den Bedingungen des Vertrages übereinstimmen. Der Kunde stellt sicher, dass seine Anweisungen für die Verarbeitung der personenbezogenen Daten des Kunden mit den Datenschutzgesetzen übereinstimmen. Im Verhältnis zwischen den Parteien trägt der Kunde die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Daten des Kunden sowie für die Mittel, mit denen der Kunde die personenbezogenen Daten des Kunden erhalten hat.

2.4 Einhaltung der Anweisungen des Kunden durch das Unternehmen. Das Unternehmen darf personenbezogene Daten des Kunden nur in Übereinstimmung mit den Anweisungen des Kunden verarbeiten und muss personenbezogene Daten des Kunden als vertrauliche Informationen behandeln. Wenn das Unternehmen der Meinung ist oder davon Kenntnis erlangt, dass Anweisungen des Kunden gegen Datenschutzgesetze verstoßen, muss das Unternehmen den Kunden innerhalb eines angemessenen Zeitraums darüber informieren. Das Unternehmen darf personenbezogene Daten des Kunden auf andere Weise als auf schriftliche Anweisung des Kunden verarbeiten, wenn dies nach geltendem Recht, dem das Unternehmen unterliegt, erforderlich ist. In diesem Fall informiert das Unternehmen den Kunden über diese Anforderung, bevor das Unternehmen die personenbezogenen Daten des Kunden verarbeitet, es sei denn, dies ist nach geltendem Recht verboten.

3. Unterauftragsverarbeiter

3.1 Ernennung von Unterauftragsverarbeitern. Der Kunde erteilt dem Unternehmen hiermit die allgemeine schriftliche Genehmigung, Dritte als Unterauftragsverarbeiter mit der Erbringung begrenzter oder zusätzlicher Dienstleistungen in Verbindung mit der Bereitstellung von Produkten und/oder Dienstleistungen zu beauftragen. Auf der Website des Unternehmens sind die Unterauftragsverarbeiter aufgeführt, die derzeit vom Unternehmen mit der Durchführung bestimmter Verarbeitungstätigkeiten im Zusammenhang mit den personenbezogenen Daten des Kunden beauftragt sind. Das Unternehmen wird die Liste der Unterauftragsverarbeiter aktualisieren, bevor es einen neuen Unterauftragsverarbeiter mit der Durchführung einer bestimmten Verarbeitung beauftragt. Der Kunde kann sich jederzeit für elektronische Updates anmelden, wenn die Liste der Unterauftragsverarbeiter des Unternehmens geändert wird, indem er eine solche Anfrage an privacy@commandalkon.com sendet. Der Kunde kann gegen jeden Unterauftragsverarbeiter Einspruch erheben, indem er dem Unternehmen diesen Einspruch innerhalb von dreißig (30) Tagen nach einer Aktualisierung mitteilt, und die Parteien werden nach Treu und Glauben daran arbeiten, den Einspruch zu berücksichtigen. Der Kunde stimmt hiermit den Unterverarbeitungsaktivitäten der aktuellen Unterauftragsverarbeiter zu, die auf der Website des Unternehmens aufgeführt sind.

3.2 Sicherheit seitens der Unterauftragsverarbeiter. Vergibt das Unternehmen seine Verpflichtungen an Unterauftragnehmer, so darf es dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter tun, die vertragliche Verpflichtungen auferlegt, die den Verpflichtungen, die dem Unternehmen gemäß diesem Zusatz auferlegt sind, mindestens gleichwertig sind.

3.3 Haftung. Kommt der Unterauftragsverarbeiter seinen Datenschutzverpflichtungen gemäß einer solchen schriftlichen Vereinbarung nicht nach, bleibt das Unternehmen dem Kunden gegenüber in vollem Umfang für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters gemäß dieser Vereinbarung haftbar.

4. Sicherheit und Datenschutz-Folgenabschätzungen

4.1 Sicherheitsmaßnahmen des Unternehmens. Das Unternehmen wird angemessene technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten des Kunden („Informationssicherheitsprogramm“) ergreifen und dabei den

Stand der Technik, die Kosten der Umsetzung, die Art, den Umfang, den Kontext und die Zwecke der Verarbeitung sowie das Risiko für die Rechte und Freiheiten natürlicher Personen mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere berücksichtigen. Die derzeitigen technischen und organisatorischen Maßnahmen des Unternehmens sind in Anhang II der Standardvertragsklauseln (im Anhang) aufgeführt, und das Unternehmen richtet sich nach den folgenden Sicherheitsstandards: NIST 800-171; AWS CIS.

4.2 Sicherheitsmaßnahmen des Kunden. Der Kunde erkennt an, dass die Produkte und/oder Dienstleistungen bestimmte Elemente und Funktionen enthalten, die der Kunde nutzen kann, und die sich auf die Sicherheit der persönlichen Daten des Kunden auswirken, die bei der Nutzung der Produkte und/oder Dienstleistungen durch den Kunden verarbeitet werden. Es liegt in der Verantwortung des Kunden, die vom Unternehmen zur Verfügung gestellten Informationen hinsichtlich Datensicherheit zu überprüfen und eine eigenständige Entscheidung darüber zu treffen, ob die Produkte und/oder Dienstleistungen den Anforderungen und Rechtspflichten des Kunden entsprechen, einschließlich seiner Verpflichtungen nach dem geltenden Datenschutzrecht. Es liegt ferner in der Verantwortung des Kunden, die Produkte und/oder Dienstleistungen ordnungsgemäß zu konfigurieren und die vom Unternehmen zur Verfügung gestellten Elemente und Funktionen zu nutzen, um eine angemessene Sicherheit in Anbetracht der Art der personenbezogenen Daten des Kunden, die infolge der Nutzung der Produkte und/oder Dienstleistungen durch den Kunden verarbeitet werden, zu gewährleisten. Der Kunde trägt die Verantwortung für seine Nutzung der Produkte und/oder Dienstleistungen und seine Speicherung von Kopien personenbezogener Kundendaten außerhalb der Systeme des Unternehmens oder der Unterauftragsverarbeiter des Unternehmens, einschließlich, aber nicht beschränkt auf die Sicherung der Authentifizierungsdaten des Kontos, der Systeme und Geräte, und die Aufbewahrung von Kopien seiner personenbezogenen Kundendaten, wenn angebracht.

4.3 Personal des Unternehmens. Das Unternehmen stellt sicher, dass seine Mitarbeiter, die mit der Verarbeitung personenbezogener Kundendaten befasst sind, über die Vertraulichkeit der personenbezogenen Kundendaten informiert werden und einer Vertraulichkeitsverpflichtung unterliegen, die nach der Beendigung des Arbeitsverhältnisses der betreffenden Person mit dem Unternehmen weiterbesteht.

4.4 Sicherheitsprüfung. Das Unternehmen wird die Wirksamkeit des Informationssicherheitsprogramms zur Gewährleistung der sicheren Verarbeitung personenbezogener Kundendaten testen, bewerten und evaluieren. Das Unternehmen wird sein Informationssicherheitsprogramm einhalten und sichert zu, dass sein Informationssicherheitsprogramm im Einklang mit geltendem Recht steht und stehen wird.

4.5 Folgenabschätzungen. Das Unternehmen wird angemessene Maßnahmen ergreifen, um mit dem Kunden zusammenzuarbeiten und ihn bei der Durchführung von Folgenabschätzungen und damit zusammenhängenden Konsultationen mit Aufsichtsbehörden zu unterstützen, wenn der Kunde gemäß den Datenschutzgesetzen zur Durchführung solcher Folgenabschätzungen verpflichtet ist.

5. Rechte der betroffenen Person

5.1 Unterstützung bei der Erfüllung der Verpflichtungen des Kunden. Soweit der Kunde bei der Nutzung oder dem Erhalt der Produkte und/oder Dienstleistungen nicht in der Lage ist, die persönlichen Daten des Kunden zu korrigieren, zu ändern, einzuschränken, zu sperren oder zu löschen, wie es die Datenschutzgesetze vorschreiben, kommt das Unternehmen angemessenen Aufforderungen des Kunden zur Erleichterung solcher Maßnahmen unverzüglich nach, soweit es dem Unternehmen gesetzlich zulässig und möglich ist. Sofern gesetzlich zulässig, ist der Kunde für alle Kosten verantwortlich, die durch die Bereitstellung einer solchen Unterstützung durch das Unternehmen entstehen.

5.2 Benachrichtigungspflichten. Soweit gesetzlich zulässig, benachrichtigt das Unternehmen den Kunden unverzüglich, wenn es einen Antrag einer betroffenen Person auf Auskunft, Berichtigung, Ergänzung, Löschung oder Widerspruch gegen die Verarbeitung personenbezogener Daten des Kunden erhält, die sich auf diese Person beziehen. Das Unternehmen wird ohne vorherige schriftliche Zustimmung des Kunden nicht auf eine solche Anfrage einer betroffenen Person in Bezug auf personenbezogene Daten des Kunden reagieren, außer, um zu bestätigen, dass sich die Anfrage auf den Kunden bezieht. Darüber hinaus wird das Unternehmen, soweit gesetzlich zulässig, den Kunden unverzüglich benachrichtigen, wenn es von einer Strafverfolgungsbehörde, einer zuständigen Behörde oder einer relevanten Datenschutzbehörde ein Ersuchen um Offenlegung von oder Korrespondenz, eine Benachrichtigung oder eine andere Mitteilung in Bezug auf die personenbezogenen Daten des Kunden erhält. Das Unternehmen gewährt dem Kunden eine angemessene Zusammenarbeit und Unterstützung bei der Bearbeitung solcher Anfragen, soweit dies gesetzlich zulässig ist und soweit der Kunde durch die Nutzung oder den Erhalt der Produkte und/oder Dienstleistungen keinen Zugang zu den personenbezogenen Daten des Kunden hat. Sofern gesetzlich zulässig, ist der Kunde für alle Kosten verantwortlich, die durch die Bereitstellung einer solchen Unterstützung durch das Unternehmen entstehen.

6. Verletzung des Schutzes personenbezogener Daten

6.1 Benachrichtigungspflichten. Falls das Unternehmen von einer verifizierten Sicherheitsverletzung Kenntnis erlangt, wird das Unternehmen den Kunden unverzüglich und in jedem Fall spätestens zweiundsiebzig (72) Stunden nach Entdeckung über die Sicherheitsverletzung informieren. Die Verpflichtungen in diesem Abschnitt 6 gelten nicht für Vorfälle, die durch den Kunden oder dessen Personal oder Endbenutzer verursacht werden, oder für erfolglose Versuche oder Aktivitäten, die die Sicherheit der personenbezogenen Daten des Kunden nicht gefährden, einschließlich erfolgloser Anmeldeversuche, Pings, Port-Scans, Denial-of-Service-Angriffe und anderer Netzwerkangriffe auf Firewalls oder vernetzte Systeme.

6.2 Art und Weise der Benachrichtigung. Die Benachrichtigung über etwaige Sicherheitsverletzungen erfolgt per E-Mail oder telefonisch an die DSGVO-Kontaktstelle des Kunden. Es liegt in der alleinigen Verantwortung des Kunden dafür zu sorgen, dass seine Kontaktinformationen in den Supportsystemen des Unternehmens stets korrekt sind. Der Kunde ist allein verantwortlich für die

Einhaltung der für den Kunden geltenden Anforderungen zur Benachrichtigung bei Verstößen und zur Erfüllung aller Benachrichtigungspflichten gegenüber Dritten im Zusammenhang mit einer Verletzung der Sicherheit personenbezogener Daten.

6.3 Inhalt der Benachrichtigung. Ist eine Benachrichtigung erforderlich, so muss diese mindestens Folgendes enthalten:

6.3.1 Beschreibung der Art des Sicherheitsverstoßes, die Kategorien und die Anzahl der betroffenen Personen sowie die Kategorien und die Anzahl der betroffenen personenbezogenen Datensätze;

6.3.2 den Namen und die Kontaktdaten der zuständigen Kontaktperson des Unternehmens, bei der weitere Informationen eingeholt werden können;

6.3.3 Beschreibung der wahrscheinlichen Folgen der Sicherheitsverletzung; und

6.3.4 Beschreibung der Maßnahmen, die zur Behebung der Sicherheitsverletzung ergriffen wurden oder ergriffen werden sollen.

7. Löschung oder Rückgabe von personenbezogenen Daten des Kunden

7.1 Löschen oder zurückgeben. Vorbehaltlich Abschnitt 7.3 verpflichtet sich das Unternehmen, unverzüglich und in jedem Fall innerhalb von dreißig (30) Tagen nach dem Datum der Beendigung von Dienstleistungen, die die Verarbeitung personenbezogener Daten des Kunden beinhalten (das „**Beendigungsdatum**"), die personenbezogenen Daten des Kunden sicher zu löschen oder auf rechtzeitige schriftliche Anfrage des Kunden eine vollständige Kopie aller personenbezogenen Daten des Kunden durch sichere Dateiübertragung in dem vom Kunden angemessener Weise gewünschten Format an den Kunden zurückzugeben.

7.2 Definition von Löschen. Zur Klarstellung: „**Löschen**" bedeutet, personenbezogene Daten so zu entfernen oder unkenntlich zu machen, dass sie nicht wiederhergestellt oder rekonstruiert werden können.

7.3 Aufbewahrung. Das Unternehmen ist berechtigt, die personenbezogenen Daten des Kunden in dem Umfang aufzubewahren, wie es die geltenden Gesetze vorschreiben oder wie es der Zeitplan des Unternehmens für die Speicherung von Dokumenten vorsieht, vorausgesetzt, das Unternehmen gewährleistet die Vertraulichkeit aller personenbezogenen Daten des Kunden.

8. Audit-Rechte

8.1 Audit-Rechte. Der Kunde ist berechtigt höchstens einmal pro Jahr einen einvernehmlich vereinbarten Dritten damit zu beauftragen, das Unternehmen zu prüfen, und zwar ausschließlich zum Zweck der Erfüllung seiner Audit-Anforderungen gemäß Artikel 28, Abschnitt 3(h) der Datenschutz-Grundverordnung. Um ein Audit zu anzufordern, muss der Kunde mindestens vier (4) Wochen vor dem vorgeschlagenen Audit-Termin einen detaillierten Audit-Plan vorlegen, in dem der vorgeschlagene Umfang, die Dauer und das Anfangsdatum des Audits beschrieben sind. Audit-Anfragen müssen an diese E-Mail-Adresse gesandt werden:

privacy@commandalkon.com. Der Prüfer muss vor der Durchführung des Audits eine für das Unternehmen akzeptable schriftliche Vertraulichkeitsvereinbarung unterzeichnen. Das Audit muss während der regulären Geschäftszeiten durchgeführt werden, unterliegt den Richtlinien des Unternehmens und darf die Geschäftsaktivitäten des Unternehmens nicht unangemessen beeinträchtigen. Alle Audits gehen zu Lasten des Kunden. Das Unternehmen kooperiert mit dem Kunden oder einer zuständigen Regulierungs- oder Aufsichtsbehörde bei allen Audit-Anfragen zur Überprüfung, ob das Unternehmen seinen Verpflichtungen aus dieser DVZ nachkommt, indem es, vorbehaltlich der Geheimhaltungsverpflichtung, Audit-Berichte Dritter, soweit verfügbar, Beschreibungen von Sicherheitskontrollen und andere vom Kunden in angemessener Weise angeforderte Informationen über die Sicherheitspraktiken und -richtlinien des Unternehmens zur Verfügung stellt.

8.2 Unterstützung bei der Einhaltung. Unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Unternehmen zur Verfügung stehen, wird das Unternehmen dem Kunden eine angemessene, zumutbare Zusammenarbeit und Unterstützung hinsichtlich der in den Artikeln 32-36 der DSGVO beschriebenen Verpflichtungen des Kunden gewähren.

9. Datenübermittlungen

9.1 Allgemeine Ermächtigung. Der Kunde erklärt sich damit einverstanden, dass das Unternehmen vorbehaltlich Abschnitt 9.2 personenbezogene Daten des Kunden in den Vereinigten Staaten von Amerika und jedem anderen Land, in dem das Unternehmen oder einer seiner Unterauftragsverarbeiter Einrichtungen unterhält oder personenbezogene Daten anderweitig verarbeitet, speichern und verarbeiten darf. Solche Übermittlungen unterliegen den Standardvertragsklauseln des Unternehmens zwischen seinen Tochtergesellschaften oder der Privacy-Shield-Zertifizierung des Unternehmens (sollte diese wiederhergestellt werden). Das Unternehmen wird keine personenbezogenen Daten des Kunden von einem Hoheitsgebiet in ein anderes übermitteln oder übermitteln lassen, es sei denn, dies geschieht in Übereinstimmung mit geltendem Recht, und wird nicht dazu führen, dass der Kunde gegen ein Datenschutzgesetz verstößt.

9.2 Standardvertragsklauseln. Soweit, und nur soweit, das Unternehmen personenbezogene Daten des Kunden aus dem Europäischen Wirtschaftsraum, der Schweiz oder dem Vereinigten Königreich verarbeitet und Standardvertragsklauseln erforderlich sind, gelten die anwendbaren Standardvertragsklauseln (EWR oder Vereinigtes Königreich), welche hiermit hierein einbezogen werden. Für die Zwecke der Standardvertragsklauseln ist der Kunde der „Datenexporteur“ und das Unternehmen ist der „Datenimporteur“. Das Unternehmen verfügt über die Standardvertragsklauseln von 2021, die zwischen den Tochtergesellschaften des Unternehmens Anwendung finden, und hält die Selbstzertifizierung nach dem Privacy Shield (für den Fall, dass es wieder in Kraft gesetzt wird) für die Zwecke der Datenübermittlung in die Vereinigten Staaten von Amerika aufrecht.

9.3 Standardvertragsklauseln Vereinigtes Königreich. Die Parteien vereinbaren, dass die Standardvertragsklauseln Vereinigtes Königreich für personenbezogene Daten gelten, die über die Produkte und/oder Dienstleistungen aus dem Vereinigten Königreich

entweder direkt oder im Wege der Weiterübermittlung in ein Land oder einen Empfänger außerhalb des Vereinigten Königreichs übermittelt werden, das bzw. der von der zuständigen britischen Aufsichtsbehörde oder Regierungsstelle für das Vereinigte Königreich nicht als Land anerkannt wird, das ein angemessenes Schutzniveau für personenbezogene Daten bietet. Für Datenübermittlungen aus dem Vereinigten Königreich, die den Standardvertragsklauseln Vereinigtes Königreich unterliegen, gelten die Standardvertragsklauseln Vereinigtes Königreich als abgeschlossen (und werden durch diesen Verweis in diesen Zusatz aufgenommen).

9.4 Ergänzende Maßnahmen. Ergänzend zu den Standardvertragsklauseln gilt: Wenn das Unternehmen davon Kenntnis erlangt, dass eine staatliche Behörde (einschließlich der Strafverfolgungsbehörden) Zugang zu oder eine Kopie von einigen oder allen personenbezogenen Daten des Kunden, die vom Unternehmen verarbeitet werden, sei es auf freiwilliger oder obligatorischer Basis, zu Zwecken der nationalen Sicherheitsaufklärung erhalten möchte, dann wird das Unternehmen, sofern dies nicht gesetzlich verboten ist oder eine zwingende gesetzliche Pflicht etwas anderes vorschreibt: 1) den Kunden, auf den sich die personenbezogenen Daten beziehen, unverzüglich benachrichtigen; 2) die betreffende Regierungsbehörde darüber informieren, dass es nicht befugt ist, die personenbezogenen Daten des Kunden offenzulegen, und, sofern dies nicht gesetzlich verboten ist, es den Kunden, auf den sich die personenbezogenen Daten des Kunden beziehen, unverzüglich benachrichtigen muss; 3) die Regierungsbehörde darüber informieren, dass sie alle Anfragen oder Forderungen direkt an den Kunden richten soll, auf den sich die personenbezogenen Daten des Kunden beziehen; und 4) keinen Zugang zu den personenbezogenen Daten des Kunden gewähren, bis der Kunde, auf den sich die personenbezogenen Daten des Kunden beziehen, dies schriftlich genehmigt hat oder bis es gesetzlich dazu gezwungen ist. Wenn das Unternehmen im Rahmen gesetzlicher Verpflichtungen dazu gezwungen ist, unternimmt es angemessene und rechtmäßige Anstrengungen, um ein solches Verbot oder eine solche Pflicht anzufechten. Wenn das Unternehmen gezwungen ist, die persönlichen Daten des Kunden vorzulegen, wird das Unternehmen die persönlichen Daten des Kunden nur in dem Maße offenlegen, wie es gesetzlich vorgeschrieben erforderlich ist, um dies in Übereinstimmung mit den geltenden gesetzlichen Verfahren zu tun.

9.5 Übermittlungspriorität. Für den Fall, dass Dienstleistungen von mehr als einem Übermittlungsmechanismus abgedeckt werden, unterliegt die Übermittlung der personenbezogenen Daten des Kunden einem einzigen Übermittlungsmechanismus gemäß der folgenden Priorität: (i) EU-Standardvertragsklauseln (sofern dies nach geltendem Datenschutzrecht erforderlich ist); (ii) Selbstzertifizierung nach dem Privacy Shield (sollte diese wieder eingeführt werden).

10. Vertragsdauer und Kündigung

Vertragsdauer des DVZ. Dieser DVZ tritt an dem Tag in Kraft, an dem er von allen Parteien unterschrieben ist, und bleibt ungeachtet des Ablaufs der Laufzeit eines gekauften Abonnements bis zur Löschung aller personenbezogenen Daten des Kunden, wie in diesem DVZ beschrieben, in Kraft und erlischt nach besagter Löschung automatisch.

11. Nichteinhaltung; Rechtsbehelfe; Parteien

11.1 Haftungsbeschränkung. Die Haftung des Unternehmens für Verstöße gegen seine Verpflichtungen aus diesem DVZ unterliegt der Haftungsbeschränkung im Vertrag.

11.2 Parteien dieses DVZ. Keine der Bestimmungen des DVZ verleiht anderen Personen oder Einrichtungen als den Parteien dieses DVZ irgendwelche Vorteile oder Rechte.

12. Allgemeine Bedingungen

Geltendes Recht und Gerichtsbarkeit

12.1 Dieser DVZ wird ein Jahr nach dem Ausstellungsdatum und danach nach drei Jahren, gegebenenfalls auch früher, überprüft.

12.2 Sofern nicht durch die Standardvertragsklauseln vorgeschrieben:

12.2.1 die Parteien dieses Zusatzes unterwerfen sich hiermit der im Vertrag festgelegten Gerichtsbarkeit in Bezug auf alle Streitigkeiten oder Ansprüche, die sich aus diesem Zusatz ergeben, einschließlich Streitigkeiten über dessen Bestehen, Gültigkeit oder Kündigung; und

12.2.2 dieser Zusatz und alle außervertraglichen oder sonstigen Verpflichtungen, die sich aus oder im Zusammenhang mit ihm ergeben, unterliegen den Gesetzen des Landes oder Gebiets, das zu diesem Zweck im Vertrag festgelegt wurde.

Prioritätsfolge

12.3 Im Falle eines Widerspruchs oder einer Unstimmigkeit zwischen diesem Zusatz und den Standardvertragsklauseln, wenn die Standardvertragsklauseln erforderlich sind, haben die Standardvertragsklauseln Vorrang.

12.4 Vorbehaltlich Abschnitt 12.2 sind im Falle von Widersprüchen zwischen den Bestimmungen dieses Zusatzes und anderen Verträgen zwischen den Parteien, einschließlich des Vertrags und einschließlich (sofern nicht ausdrücklich schriftlich und im Namen der Parteien unterzeichnet anders vereinbart) Verträgen, die nach dem Datum dieses Zusatzes abgeschlossen wurden oder angeblich abgeschlossen wurden, die Bestimmungen dieses Zusatzes maßgebend.

Änderungen der Datenschutzgesetze

12.5 Der Kunde ist berechtigt:

12.5.1 durch schriftliche Mitteilung an das Unternehmen mit einer Frist von mindestens dreißig (30) Kalendertagen von Zeit zu Zeit Änderungen der Standardvertragsklauseln vorschlagen, die aufgrund einer Änderung oder einer Entscheidung einer zuständigen Behörde im Rahmen dieses Datenschutzgesetzes erforderlich sind; und

12.5.2 sonstige Änderungen dieses Zusatzes vorzuschlagen, die der Kunde angemessener Weise für erforderlich hält, um die Anforderungen eines Datenschutzgesetzes zu erfüllen.

12.6 Wenn der Kunde eine Mitteilung gemäß Abschnitt 12.5 vorlegt, erörtern die Parteien unverzüglich die vorgeschlagenen Änderungen und verhandeln nach Treu und Glauben mit dem Ziel, diese oder alternative Änderungen zu vereinbaren und umzusetzen, um die in der Mitteilung des Kunden genannten Anforderungen so bald wie möglich zu erfüllen.

Abtrennung

12.7 Sollte eine Bestimmung dieses Zusatzes ungültig oder nicht durchsetzbar sein, so bleibt der Rest dieses Zusatzes gültig und in Kraft. Die ungültige oder nicht durchsetzbare Bestimmung wird entweder: (i) so geändert werden, dass ihre Gültigkeit und Durchsetzbarkeit gewährleistet ist, wobei die Absichten der Parteien so weit wie möglich beibehalten werden, oder, falls dies nicht möglich ist, (ii) so ausgelegt werden, als ob der ungültige oder nicht durchsetzbare Teil nie darin enthalten gewesen wäre.

ANHANG I ZU DEN STANDARDVERTRAGSKLAUSELN

A. LISTE DER PARTEIEN

Datenexporteur(e)[1]: [*Identität und Kontaktdaten des Datenexporteurs / der Datenexporteure und ggf. seines/deren Datenschutzbeauftragten und/oder Vertreter(s) in der Europäischen Union*]

Name:

Anschrift:

Name, Position und Kontaktdetails der Kontaktperson:

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten relevant sind:

Unterschrift und Datum:

Rolle: Verantwortlicher

Datenimporteur(e): [*Identität und Kontaktdaten des/der Datenimporteure(s), einschließlich einer Kontaktperson, die für den Datenschutz zuständig ist*]

Name: Command Alkon Incorporated

Anschrift: 1800 Industrial Park Drive, Suite 400, Birmingham, Alabama 35243 USA

Name, Position und Kontaktdetails der Kontaktperson: David R. Burkholder, Stellvertretender Syndikus und leitender Datenschutzbeauftragter, dburkholder@commandalkon.com, 1-205-263-5524 App. 2837

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten relevant sind:

Leitender Datenschutzbeauftragter für die Einhaltung der Vorschriften

Unterschrift und Datum:

Rolle: Auftragsverarbeiter

B. BESCHREIBUNG DER ÜBERMITTLUNG

[1] Wenn dieser Abschnitt nicht ausgefüllt ist, ist der Datenexporteur die in der zugehörigen Hauptlizenz- und Dienstleistungsvereinbarung und den zugehörigen Dokumenten genannte Stelle.

Kategorien von betroffenen Personen, deren personenbezogene Daten übermittelt werden

Mitarbeiter des Kunden; Kunden des Kunden; Mitarbeiter von mit dem Kunden verbundenen Unternehmen.

Kategorien der übertragenen personenbezogenen Daten

Kontaktinformationen; Website-, Produkt- und Service-Interaktionsinformationen; Adressen; Geburtsdatum; Geburtsort; E-Mail-Adressen; Namen; Geschlecht; Titel; Telefonnummern; Führerscheinnummer; Unterschrift; Mitarbeiternummer; Geostandortinformationen; Lohnsatz; Benutzername; Passwort; Leistungsinformationen; Qualifikationen und Einschränkungen.

Übermittlung sensibler Daten (falls zutreffend) und Anwendung von Beschränkungen oder Schutzmaßnahmen, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie z. B. strikte Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnung des Zugangs zu den Daten, Beschränkungen für die Weitergabe oder zusätzliche Sicherheitsmaßnahmen

Es werden keine sensiblen Daten im Sinne der Datenschutz-Grundverordnung übermittelt.

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden)

Kontinuierliche Übermittlung von Daten, da das Produkt/die Plattform von den Endnutzern verwendet wird.

Art der Verarbeitung

Soweit für die Bereitstellung des Produkts/der Dienstleistung im Rahmen des Vertrags erforderlich und gemäß den Anweisungen des Exporteurs.

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Soweit für die Bereitstellung des Produkts/der Dienstleistung oder zur Unterstützung des Produkts/der Dienstleistung erforderlich.

Zeitraum, für den die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien, nach denen dieser Zeitraum bestimmt wird

Solange, wie dies für die Bereitstellung des Produkts/der Dienstleistung und im Zusammenhang mit der Richtlinie und dem Zeitplan für die Vorratsdatenspeicherung des Unternehmens erforderlich ist, oder wie durch geltende Gesetze oder Vorschriften vorgeschrieben.

Bei Übermittlungen an (Unter-)Verarbeiter ebenfalls Gegenstand, Art und Dauer der Verarbeitung angeben

Für den Support, der für die Bereitstellung des Produkts/der Dienstleistung erforderlich ist (z. B. Cloud-Speicherdienste) und für den Zeitraum, der für die Bereitstellung des Produkts/der Dienstleistung erforderlich ist.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Benennung der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13

Datenschutzbehörde der Niederlande.

ANHANG II ZU DEN STANDARDVERTRAGSKLAUSELN

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

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

Maßnahmen zur Pseudonymisierung und Verschlüsselung von personenbezogenen Daten **Verschlüsselung bei der Übertragung und im Speicher ist implementiert.**

Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und -dienste **Command Alkon richtet sich nach dem Sicherheitsrahmen NIST 800-171 sowie den AWS CIS-Benchmarks v1.2 und AWS Foundational Best Practices v1.0**

Maßnahmen zur Gewährleistung der Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen **Command Alkon führt regelmäßig geplante Backups durch und verwendet eine hochverfügbare Architektur.**

Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten **Regelmäßige automatisierte Schwachstellentests; jährliche Penetrationstests; jährliche Datenschutz- und Sicherheitsaudits**

Maßnahmen zur Benutzeridentifikation und -autorisierung **Multi-Faktor-Authentifizierung; komplexes Passwortprogramm; Berechtigungsbeschränkungen; Protokollierung**

Maßnahmen zum Schutz der Daten bei der Übermittlung **Verschlüsselung bei der Übertragung**

Maßnahmen zum Schutz der Daten während der Aufbewahrung **Verschlüsselung im Speicher; logische Zugangskontrollen; Redundanz durch Backup und Ausfallsicherung**

Maßnahmen zur Gewährleistung der physischen Sicherheit der Orte, an denen personenbezogene Daten verarbeitet werden **Schlüsselkarten/Codes; Besucherregistrierung; Sicherheitsvideo; Sicherheitsbeauftragte; Sicherheits-/Datensicherheitsschulung**

Maßnahmen zur Gewährleistung der Ereignisprotokollierung **Protokollierung vorhanden und überwacht; die Protokollierung wird an einen Third Party Management (TPM)-Dienstleister weitergeleitet; Ereigniswarnungen sind aktiviert**

Maßnahmen zur Aufrechterhaltung der Systemkonfiguration, einschließlich der Standardkonfiguration **Alle Konfigurationszustände und -änderungen werden nachverfolgt; Änderungsmanagementprogramm implementiert**

Maßnahmen zur internen IT und IT- Security Governance und -Verwaltung **Sicherheits- und Datenschutzrichtlinien und -verfahren; Leitender Beauftragter für die Sicherheit von Informationen; dediziertes Team für sicherheitsbezogene Betriebsverfahren (SecOps-Team); Leitender Datenschutzbeauftragter; Sicherheits-/Datenschutzschulungen**

Maßnahmen zur Zertifizierung/Absicherung von Prozessen und Produkten **NIST 800-171; CIS AWS Benchmark v1.2; AWS Foundational Best Practices v1.0**

Maßnahmen zur Gewährleistung der Datenminimierung **Es werden nur Daten verarbeitet, die vom Endbenutzer/Kunden/Verantwortlichen eingegeben wurden.**

Maßnahmen zur Gewährleistung der Datenqualität **Die verarbeiteten Daten werden von den Endnutzern eingegeben und gepflegt.**

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung **Die Vorratsdatenspeicherung wird durch vertragliche Verpflichtungen sowie durch die Richtlinie und den Zeitplan für die Vorratsdatenspeicherung geregelt.**

Maßnahmen zur Gewährleistung der Nachweis-Führung **Die Nachweis-Führung wird durch eine überwachte Protokollierung gewährleistet; die Protokollierung wird an einen TPM-Dienstleister weitergeleitet; Ereigniswarnungen sind aktiviert.**

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung von Daten **Die Datenübertragbarkeit wird von Fall zu Fall gehandhabt, und die Löschung von Daten wird durch vertragliche Verpflichtungen und Benachrichtigungs- und Bestätigungsverfahren gewährleistet.**

Bei Übermittlungen an (Unter-)Auftragsverarbeiter, auch Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der (Unter-)Auftragsverarbeiter ergreifen muss, um den für die Verarbeitung Verantwortlichen und - bei Übermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter - den Datenexporteur unterstützen zu können

Unterauftragsverarbeiter, die personenbezogene Daten verarbeiten, unterliegen vertraglichen Beschränkungen und Datenverarbeitungszusätzen, die gegebenenfalls die Einhaltung der Standardvertragsklauseln vorschreiben.