# NACHTRAG ZUR DATENVERARBEITUNG VON COMMAND ALKON INCORPORATED

Aktualisiert: 25.07.24

**Dieser Zusatz zur Datenverarbeitung (“ DPA „) ist Teil des** *Rahmenlizenz- und Dienstleistungsvertrags* **(“ Agreement „) zwischen: (i) dem Kunden (im Master License and Services Agreement identifiziert) und seinen EWR-Tochtergesellschaften („Kunde“); und (ii) Command Alkon Incorporated und seinen verbundenen Unternehmen (“ Unternehmen „) nur dann, wenn es die Allgemeine Datenschutzverordnung („GDPR“) oder andere geltende Datenschutzvorschriften vorschreiben** Gesetzgebung.

Dieser Nachtrag ersetzt alle vorherigen Vereinbarungen zwischen den Parteien in Bezug auf den Gegenstand dieser Vereinbarung, d. h. Datenschutz und Sicherheit, wie sie für die Datenschutzgesetze gelten.

In Anbetracht der hier dargelegten gegenseitigen Verpflichtungen vereinbaren die Parteien hiermit, dass die unten aufgeführten Bedingungen als Ergänzung zur Vereinbarung hinzugefügt werden.

## 1. Definitionen

„**Personenbezogene Kundendaten**“ sind personenbezogene Daten, die vom Unternehmen im Namen des Kunden bei der Bereitstellung der Produkte und/oder Dienstleistungen verarbeitet werden.

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

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

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

„**Datenschutzgesetze**“ bezeichnet alle geltenden Gesetze und Vorschriften in Bezug auf die Verarbeitung personenbezogener Daten und den Datenschutz, die in den jeweiligen Jurisdiktionen existieren können, einschließlich, sofern zutreffend, der Allgemeinen Datenschutzverordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („GDPR“) (und jeder Änderung oder Ersetzung derselben), das Schweizer Bundesgesetz über Datenschutz („FADP“) (und jede Änderung oder Ersetzung) ), die EU-DSGVO in ihrer geänderten und in britisches Recht gemäß dem UK European Union (Withdrawal) Act 2018 und den anwendbaren sekundären Gesetzen, die unter diesem Gesetz erlassen wurden („UK GDPR“) (und jede Änderung oder Ersetzung davon), das brasilianische Allgemeine Datenschutzgesetz (das „LGPD“) (und jede Änderung oder

Ersetzung), das brasilianische Allgemeine Datenschutzgesetz (das „LGPD“) (und jede Änderung oder Ersetzung dazu), der Privacy Act 1988 (Cth) von Australien, in der jeweils gültigen Fassung („Australian Privacy Law“) (und jede Änderung oder Ersetzung dazu), USA Datenschutzgesetze der Bundesstaaten (einschließlich des CCPA und CPRA von Kalifornien) in ihrer erlassenen oder geänderten Fassung oder jedes andere geltende Datenschutzgesetz, das eine Datenschutzvereinbarung erfordert. Wo die DSGVO ausdrücklich erwähnt wird, gelten dieselben Anforderungen für alle anderen entsprechenden Anforderungen des geltenden Datenschutzrechts.

„**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 für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität der betroffenen Person spezifisch sind.

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

„**Sicherheitsverletzung**“ bedeutet eine bestätigte Sicherheitsverletzung, die zu einer versehentlichen oder unrechtmäßigen Zerstörung, Verlust, Änderung, unbefugter Offenlegung oder unberechtigtem Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Kundendaten führt.

„**Standardvertragsklauseln**“ bezeichnet die standardmäßigen Vertragsanforderungen, die im geltenden Datenschutzrecht festgelegt sind (EU-Standardvertragsklauseln, Mustervertragsklauseln des RIPD Latin American Data Protection Board, ASEAN-Modellvertragsklauseln usw.).

**„Drittanbieter“** bedeutet eine andere Partei als Kunde oder Unternehmen.

Die Begriffe „**Verantwortlicher**“, „**Auftragsverarbeiter**“ und „**Aufsichtsbehörde**“, wie sie in dieser DPA verwendet werden, werden die Bedeutungen haben, die ihnen im geltenden Datenschutzgesetz zugewiesen werden.

Alle anderen nicht definierten, aber großgeschriebenen Begriffe haben die in der Vereinbarung oder dem geltenden Datenschutzgesetz festgelegte Bedeutung.

## 2. Verarbeitung personenbezogener Kundendaten

2.1 Zweck der Verarbeitung. Der Zweck der Datenverarbeitung im Rahmen dieser Datenschutzvereinbarung ist die Bereitstellung der Produkte und/oder Dienstleistungen gemäß der Vereinbarung. Anhang 1 beschreibt den Gegenstand und die Einzelheiten der Verarbeitung personenbezogener Kundendaten.

2.2 Verantwortlichkeiten des Prozessors und des Controllers. Die Parteien erkennen an und stimmen zu, dass: (a) das Unternehmen ein Verarbeiter personenbezogener

Kundendaten gemäß den Datenschutzgesetzen ist; (b) der Kunde gemäß den Datenschutzgesetzen für die Verarbeitung personenbezogener Kundendaten verantwortlich ist; (c) der Kunde ist dafür verantwortlich, alle erforderlichen Genehmigungen und Genehmigungen für die Eingabe, Verwendung, Bereitstellung, Speicherung und Verarbeitung personenbezogener Kundendaten einzuholen, damit das Unternehmen die Produkte und/oder Dienstleistungen bereitstellen kann; und (d) jede Partei wird die geltenden Verpflichtungen einhalten dazu gemäß den Datenschutzgesetzen in Bezug auf die Verarbeitung von Personenbezogene Daten des Kunden.

2.3 US-Datenschutzgesetze. Für die Zwecke der US-Datenschutzgesetze (einschließlich des CCPA) umfasst „Verantwortlicher“ „Unternehmen“, „Auftragsverarbeiter“ umfasst „Dienstleister“, „Datensubjekt“ umfasst „Verbraucher“ und „personenbezogene Daten“ umfasst „personenbezogene Daten“. Das Unternehmen ist ein Dienstleister und der Kunde ist ein Unternehmen.

2.4 Anweisungen für den Kunden. Der Kunde weist das Unternehmen an, personenbezogene Kundendaten zu verarbeiten: (a) gemäß der Vereinbarung und allen geltenden Ergänzungen; (b) soweit anderweitig erforderlich, um dem Kunden die Produkte und/oder Dienstleistungen zur Verfügung zu stellen; (c) soweit dies zur Einhaltung geltender Gesetze oder Vorschriften erforderlich ist; und (d) um andere angemessene schriftliche Anweisungen des Kunden zu befolgen, sofern diese Anweisungen mit den Bedingungen der Vereinbarung übereinstimmen. Der Kunde wird sicherstellen, dass seine Anweisungen zur Verarbeitung personenbezogener Kundendaten den Datenschutzgesetzen entsprechen. Im Verhältnis der Parteien trägt der Kunde die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Kundendaten und die Art und Weise, wie der Kunde die personenbezogenen Daten des Kunden erhalten hat.

2.5 Einhaltung der Kundenanweisungen durch das Unternehmen. Das Unternehmen verarbeitet personenbezogene Daten von Kunden nur gemäß den Anweisungen des Kunden und behandelt personenbezogene Daten des Kunden als vertrauliche Informationen. Falls das Unternehmen glaubt oder davon Kenntnis erlangt, dass Anweisungen des Kunden gegen Datenschutzgesetze verstoßen, wird das Unternehmen den Kunden innerhalb einer angemessenen Frist informieren. Das Unternehmen kann personenbezogene Daten von Kunden auf andere Weise als auf schriftliche Anweisung des Kunden verarbeiten, wenn dies nach geltendem Recht, dem das Unternehmen unterliegt, erforderlich ist. In dieser Situation muss das Unternehmen den Kunden über diese Anforderung informieren, bevor das Unternehmen die personenbezogenen Daten des Kunden verarbeitet, sofern dies nicht nach geltendem Recht verboten ist.

2.6 CCPA-Bearbeitung. Soweit die Verarbeitung personenbezogener Daten durch das Unternehmen dem CCPA unterliegt, bestätigt das Unternehmen, dass es: (a) personenbezogene Kundendaten nicht anders als in der Vereinbarung vorgesehen aufbewahren, verwenden oder weitergeben wird, soweit dies zur Bereitstellung der Produkte und/oder Dienstleistungen, zur Entwicklung oder Verbesserung der Qualität der Produkte und/oder Dienstleistungen, zur Aufdeckung von Sicherheitsvorfällen, zum Schutz vor betrügerischen oder illegalen Aktivitäten, zur Beauftragung von

Unterauftragsverarbeitern gemäß dieser DPA erforderlich ist oder wie anderweitig erlaubt von der CCPA; oder (b) persönliche Kundendaten verkaufen oder weitergeben.

## 3. Unterauftragsverarbeiter

3.1 Ernennung von Unterauftragsverarbeitern. Der Kunde erteilt dem Unternehmen hiermit die allgemeine schriftliche Genehmigung, dritte Unterauftragsverarbeiter mit der Erbringung von eingeschränkten oder ergänzenden Dienstleistungen im Zusammenhang mit der Bereitstellung von Produkten und/oder Dienstleistungen zu beauftragen. Auf der Website des Unternehmens sind Unterauftragsverarbeiter aufgeführt, die derzeit vom Unternehmen mit der Durchführung bestimmter Verarbeitungsaktivitäten im Zusammenhang mit personenbezogenen Kundendaten beauftragt werden (https://commandalkon.com/sub-processor-list/), und das Unternehmen wird die Liste der Unterauftragsverarbeiter aktualisieren, bevor neue Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungen beauftragt werden. 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 Einwand innerhalb von dreißig (30) Tagen nach einer Aktualisierung mitteilt, und die Parteien werden nach bestem Wissen und Gewissen daran arbeiten, den Einwand zu lösen. Der Kunde stimmt hiermit der Unterverarbeitung durch aktuelle Unterauftragsverarbeiter zu, die auf der Website des Unternehmens aufgeführt sind.

3.2 Sicherheit von Unterauftragsverarbeitern. Wenn das Unternehmen seine Verpflichtungen weitervergibt, darf es dies nur durch eine schriftliche Vereinbarung mit dem Unterauftragsverarbeiter tun, die vertragliche Verpflichtungen auferlegt, die den Verpflichtungen, die dem Unternehmen im Rahmen dieses Zusatzes auferlegt wurden, mindestens gleichwertig sind. Die Parteien vereinbaren, dass Kopien der Vereinbarungen mit autorisierten Unterauftragsverarbeitern, die gemäß den geltenden Standardvertragsklauseln bereitgestellt werden müssen, nur auf schriftliche Anfrage des Kunden zur Verfügung gestellt werden.

3.3 Haftung. Wenn der Unterauftragsverarbeiter seinen Datenschutzverpflichtungen aus einer solchen schriftlichen Vereinbarung nicht nachkommt, haftet das Unternehmen gegenüber dem Kunden weiterhin in vollem Umfang für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters aus dieser Vereinbarung.

## 4. Verantwortlichkeiten im Bereich Sicherheit

4.1 Unternehmenssicherheit. Das Unternehmen wird angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Kundendaten („**Informationssicherheitsprogramm**“) ergreifen und dabei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, den Kontext und die Zwecke der Verarbeitung sowie das Risiko unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Das Unternehmen reguliert sich selbst 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 enthalten, die der Kunde nutzen kann und die sich auf die Sicherheit der personenbezogenen Kundendaten auswirken, die durch die Nutzung der Produkte und/oder Dienstleistungen durch den Kunden verarbeitet werden. Der Kunde ist dafür verantwortlich, die Informationen, die das Unternehmen zur Datensicherheit zur Verfügung stellt, zu überprüfen und unabhängig zu entscheiden, ob die Produkte und/oder Dienstleistungen den Anforderungen und rechtlichen Verpflichtungen des Kunden entsprechen, einschließlich seiner Verpflichtungen nach geltendem Datenschutzrecht. Der Kunde ist weiterhin dafür verantwortlich, die Produkte und/oder Dienstleistungen ordnungsgemäß zu konfigurieren und die vom Unternehmen zur Verfügung gestellten Funktionen und Funktionen zu nutzen, um angesichts der Art der personenbezogenen Kundendaten, die aufgrund 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 die Speicherung aller Kopien der personenbezogenen Kundendaten außerhalb der Systeme des Unternehmens oder der Unterauftragsverarbeiter des Unternehmens, einschließlich, aber nicht beschränkt auf die Sicherung der Zugangsdaten, Systeme und Geräte zur Kontoauthentifizierung und gegebenenfalls die Aufbewahrung von Kopien seiner personenbezogenen Kundendaten.

4.3 Mitarbeiter des Unternehmens. Das Unternehmen stellt sicher, dass sein Personal, das mit der Verarbeitung personenbezogener Kundendaten befasst ist, über den vertraulichen Charakter der personenbezogenen Kundendaten informiert wird, eine angemessene Schulung in Bezug auf seine Aufgaben erhalten hat und Vertraulichkeitspflichten unterliegt, wobei diese Verpflichtungen auch nach Beendigung der Zusammenarbeit dieser Person mit dem Unternehmen bestehen.

4.4 Sicherheitstests. Das Unternehmen wird die Wirksamkeit des Informationssicherheitsprogramms zur Gewährleistung der sicheren Verarbeitung personenbezogener Kundendaten testen, bewerten und bewerten. 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 Maßnahmen ergreifen, um mit dem Kunden zusammenzuarbeiten und ihn bei der Durchführung von Folgenabschätzungen und damit verbundenen Konsultationen mit Aufsichtsbehörden zu unterstützen, falls der Kunde gemäß Datenschutzgesetzen verpflichtet ist, solche Folgenabschätzungen durchzuführen.

## 5. Rechte der betroffenen Person

5.1 Unterstützung bei den Verpflichtungen des Kunden. Soweit der Kunde bei der Nutzung oder beim Empfang der Produkte und/oder Dienstleistungen nicht in der Lage ist, personenbezogene Daten des Kunden zu korrigieren, zu ändern, einzuschränken, zu sperren oder zu löschen, wie es die Datenschutzgesetze vorschreiben, wird das Unternehmen angemessenen Anfragen des Kunden zur Erleichterung solcher Maßnahmen umgehend nachkommen, soweit das Unternehmen

dazu gesetzlich berechtigt und in der Lage ist. Sofern gesetzlich zulässig, ist der Kunde für alle Kosten verantwortlich, die sich aus der Bereitstellung solcher Unterstützung durch das Unternehmen ergeben.

5.2 Mitteilungspflichten. Das Unternehmen muss, soweit gesetzlich zulässig, den Kunden umgehend benachrichtigen, wenn es eine Anfrage von einer betroffenen Person auf Zugang, Korrektur, Ergänzung, Löschung oder Widerspruch gegen die Verarbeitung personenbezogener Kundendaten in Bezug auf diese Person erhält. Das Unternehmen wird ohne die vorherige schriftliche Zustimmung des Kunden keine solche Anfrage einer betroffenen Person in Bezug auf personenbezogene Daten von Kunden beantworten, es sei denn, um zu bestätigen, dass sich die Anfrage auf den Kunden bezieht. Darüber hinaus muss das Unternehmen, soweit gesetzlich zulässig, den Kunden umgehend benachrichtigen, wenn es von Strafverfolgungsbehörden, einer zuständigen Behörde oder einer zuständigen Datenschutzbehörde einen Antrag auf Offenlegung oder Korrespondenz, Mitteilung oder andere Mitteilung in Bezug auf personenbezogene Kundendaten erhält. Das Unternehmen bietet dem Kunden angemessene Zusammenarbeit und Unterstützung bei der Bearbeitung einer solchen Anfrage, soweit dies gesetzlich zulässig ist und soweit 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 sich aus der Bereitstellung solcher Unterstützung durch das Unternehmen ergeben.

## 6. Verletzung personenbezogener Daten

6.1 Mitteilungspflichten. Falls das Unternehmen von einer verifizierten Sicherheitsverletzung im Zusammenhang mit personenbezogenen Kundendaten Kenntnis erlangt, wird das Unternehmen den Kunden unverzüglich und in jedem Fall nicht später als zweiundsiebzig (72) Stunden nach der Bestätigung über die Sicherheitsverletzung informieren. Die Verpflichtungen in diesem Abschnitt 6 gelten nicht für Vorfälle, die von Kunden oder Mitarbeitern 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 auf Firewalls oder Netzwerksysteme.

6.2 Art der Benachrichtigung. Benachrichtigungen über Sicherheitsverletzungen, falls vorhanden, werden per E-Mail oder Telefon an den Ansprechpartner des Kunden zugestellt. Es liegt in der alleinigen Verantwortung des Kunden, dafür zu sorgen, dass die Kontaktinformationen in den Supportsystemen des Unternehmens jederzeit korrekt sind. Der Kunde ist allein verantwortlich für die Einhaltung der für den Kunden geltenden Meldepflichten bei Verstößen und für die Erfüllung aller Meldepflichten gegenüber Dritten im Zusammenhang mit Sicherheitsverstößen gegen personenbezogene Daten.

6.3 Inhalt der Benachrichtigung. Wenn eine Benachrichtigung erforderlich ist, muss eine solche Benachrichtigung mindestens:

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

6.3.2 den Namen und die Kontaktdaten des jeweiligen Ansprechpartners des Unternehmens mitteilen, 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 wurden oder ergriffen werden sollen, um die Sicherheitsverletzung zu beheben.

## 7. Löschung oder Rückgabe personenbezogener Kundendaten

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

7.2 Falls Kunde und Unternehmen Standardvertragsklauseln abgeschlossen haben, die eine schriftliche Bestätigung der Löschung erfordern (wie die Klauseln 8.5 und 16 der EU-SCCs), vereinbaren die Parteien, dass eine schriftliche Bestätigung nur auf schriftlichen Antrag des Kunden ausgestellt wird.

7.3 Definition von Löschen. Zur Klarstellung: „**Löschen**" bedeutet, persönliche Kundendaten zu entfernen oder zu löschen, sodass sie nicht wiederhergestellt oder rekonstruiert werden können.

7.4 Aufzeichnungen. Das Unternehmen kann personenbezogene Daten von Kunden in dem Umfang aufbewahren, wie es die geltenden Gesetze erfordern oder wie es der Zeitplan für die Aufbewahrung von Dokumenten des Unternehmens vorschreibt, vorausgesetzt, dass das Unternehmen die Vertraulichkeit all dieser personenbezogenen Kundendaten gewährleistet.

## 8. Prüfungsrechte

8.1 Prüfungsrechte. Nicht mehr als einmal pro Jahr darf der Kunde einen einvernehmlich vereinbarten Dritten mit der Prüfung des Unternehmens beauftragen, ausschließlich zum Zwecke der Erfüllung seiner Prüfanforderungen gemäß Artikel 28, Abschnitt 3 (h) der DSGVO. 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 müssen an privacy@commandalkon.com gesendet werden. Der Wirtschaftsprüfer muss vor der Durchführung des Audits eine für das Unternehmen akzeptable schriftliche Vertraulichkeitsvereinbarung abschließen. Das

Audit muss während der regulären Geschäftszeiten gemäß den Richtlinien des Unternehmens durchgeführt werden und darf die Geschäftsaktivitäten des Unternehmens nicht unangemessen beeinträchtigen. Jegliche Audits erfolgen auf alleinige Kosten und Kosten des Kunden. Das Unternehmen wird mit jedem Kunden oder jeder zuständigen Regulierungs- oder Aufsichtsbehörde zusammenarbeiten, um zu überprüfen, ob das Unternehmen seinen Verpflichtungen gemäß dieser DPA nachkommt, indem es, vorbehaltlich der Geheimhaltungspflichten, Prüfberichte Dritter, sofern verfügbar, 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. Unter Berücksichtigung der Art der Verarbeitung und der dem Unternehmen zur Verfügung stehenden Informationen wird das Unternehmen dem Kunden eine angemessene und angemessene Zusammenarbeit und Unterstützung in Bezug auf die in den Artikeln 32-36 der DSGVO 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 Unterauftragsverarbeiter Einrichtungen unterhält oder personenbezogene Daten anderweitig verarbeitet, speichern und verarbeiten kann. Solche Übertragungen unterliegen zunächst der Data Privacy Framework-Zertifizierung des Unternehmens oder, alternativ, den Standardvertragsklauseln des Unternehmens zwischen verbundenen Unternehmen. Das Unternehmen wird keine personenbezogenen Kundendaten von einer Gerichtsbarkeit in eine andere übertragen oder deren Übertragung veranlassen, es sei denn, dies entspricht geltendem Recht und wird nicht dazu führen, dass der Kunde gegen ein Datenschutzgesetz verstößt.

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 Zwei der Standardvertragsklauseln und wird hiermit aufgenommen. 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 entweder direkt oder durch Weiterleitung an jedes Land oder jeden Empfänger außerhalb des Vereinigten Königreichs übertragen werden, das von der zuständigen britischen Aufsichtsbehörde oder Regierungsbehörde für das Vereinigte Königreich nicht als ausreichend anerkannt ist Schutzniveau für 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 die Datenübertragungen ausschließlich dem FADP oder sowohl dem FADP als auch der EU-DSGVO unterliegen: (a) Der Begriff „Mitgliedstaat“ darf nicht so ausgelegt werden, dass Datensubjekte in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) einzuklagen gemäß Klausel 18 (c) der Standardvertragsklauseln; (b) soweit Die den Standardvertragsklauseln zugrunde liegenden Datenübertragungen unterliegen ausschließlich dem FADP, Verweise auf die EU-DSGVO sind als Verweise auf das FADP zu verstehen; und (c) soweit die Datenübertragungen, die den Standardvertragsklauseln zugrunde liegen, sowohl dem FADP als auch der EU-DSGVO unterliegen, sind die Verweise auf die EU-DSGVO als Verweise auf das FADP zu verstehen, sofern die Datenübertragungen dem FADP unterliegen.

9.5 Zusätzliche Maßnahmen. In Ergänzung zu den Standardvertragsklauseln wird das Unternehmen, wenn das Unternehmen erfährt, dass eine Regierungsbehörde (einschließlich Strafverfolgungsbehörden) Zugang zu oder eine Kopie einiger oder aller vom Unternehmen verarbeiteten personenbezogenen Kundendaten erhalten möchte, ob auf freiwilliger oder obligatorischer Basis, für Zwecke der nationalen Sicherheitsnachrichtendienste, dann wird das Unternehmen, sofern nicht gesetzlich verboten oder aufgrund einer zwingenden gesetzlichen Verpflichtung, die etwas anderes erfordert,: 1) den Kunden, für den die personenbezogenen Daten gelten, unverzüglich informieren; 2) informieren die zuständige Regierungsbehörde, die wurde nicht befugt, die personenbezogenen Daten des Kunden weiterzugeben, und muss, sofern nicht gesetzlich verboten, den Kunden, für den die personenbezogenen Daten des Kunden gelten, unverzüglich informieren; 3) die Regierungsbehörde darüber informieren, dass sie alle Anfragen oder Anfragen direkt an den Kunden richten sollte, für den die personenbezogenen Daten des Kunden gelten; und 4) keinen Zugriff auf die personenbezogenen Kundendaten gewähren, bis der Kunde, für den die personenbezogenen Daten gelten, schriftlich autorisiert hat oder bis er gesetzlich dazu verpflichtet ist. Wenn das Unternehmen rechtlich dazu gezwungen ist, wird das Unternehmen angemessene und rechtmäßige Anstrengungen unternehmen, um ein solches Verbot oder einen solchen Zwang anzufechten. Wenn das Unternehmen gezwungen ist, die personenbezogenen Daten des Kunden herauszugeben, wird das Unternehmen die personenbezogenen Daten des Kunden nur in dem Umfang weitergeben, in dem dies gemäß dem geltenden rechtmäßigen Verfahren gesetzlich vorgeschrieben ist.

9.6 Gesetz zur Überwachung ausländischer Nachrichtendienste. Das Unternehmen hat bisher keine Richtlinie gemäß Abschnitt 702 des U.S. Foreign Intelligence Surveillance Act, kodifiziert in 50 U.S.C. §1881a („FISA Section 702“), erhalten. Kein Gericht hat festgestellt, dass Unternehmen die Art von Unternehmen ist, die für ein Verfahren gemäß FISA Abschnitt 702 in Frage kommen. Das Unternehmen gehört nicht zu den Anbietern, die gemäß FISA-Abschnitt 702, wie in der *Schrems II-Entscheidung* beschrieben, einer vorgelagerten Sammlung („Sammelabholung“) unterliegen können.

9.7 Rangfolge der Übertragung. Für den Fall, dass Dienstleistungen durch mehr als einen Übertragungsmechanismus abgedeckt sind, unterliegt die Übertragung der personenbezogenen Daten des Kunden einem einzigen Übertragungsmechanismus

gemäß der folgenden Rangfolge: (i) Zertifizierung des Unternehmens nach dem Datenschutzrahmen; (ii) geltende Standardvertragsklauseln (sofern nach geltendem Datenschutzrecht erforderlich).

## 10. Laufzeit und Kündigung

Laufzeit der Datenschutzbehörde. Diese Datenschutzvereinbarung tritt an dem Tag in Kraft, an dem die Vereinbarung vollständig ausgeführt wird, und bleibt, ungeachtet des Ablaufs der Laufzeit eines gekauften Abonnements, bis alle personenbezogenen Kundendaten, wie in dieser DPA beschrieben, gelöscht werden, und erlischt automatisch nach deren Löschung.

## 11. Nichteinhaltung; Rechtsbehelfe; Parteien

11.1 Haftungsbeschränkung. Die Haftung des Unternehmens für die Verletzung seiner Verpflichtungen aus dieser DPA unterliegt der Haftungsbeschränkung in der Vereinbarung.

11.2 Parteien dieser Datenschutzbehörde. Nichts in der DPA verleiht irgendwelchen anderen Personen oder Organisationen als den Parteien dieser DPA irgendwelche Vorteile oder Rechte.

## 12. Allgemeine Geschäftsbedingungen

*Geltendes Recht und Gerichtsbarkeit*

12.1 Diese Datenschutzvereinbarung wird ein Jahr nach dem Ausstellungsdatum und dann drei Jahre danach, oder gegebenenfalls früher, überprüft.

12.2 Sofern nicht durch die Standardvertragsklauseln vorgeschrieben:

12.2.1 Die Parteien dieses Zusatzes unterwerfen sich hiermit der in der Vereinbarung 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, die zu diesem Zweck in der Vereinbarung festgelegt sind.

*Reihenfolge der Rangfolge*

12.3 Im Falle eines Konflikts oder einer Inkonsistenz zwischen diesem Addendum 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 dieses Zusatzes, haben im Fall von Widersprüchen zwischen den Bestimmungen dieses Zusatzes und allen anderen Vereinbarungen zwischen den Parteien, einschließlich der Vereinbarung

und einschließlich (sofern nicht ausdrücklich schriftlich etwas anderes vereinbart, im Namen der Parteien unterzeichnet) Vereinbarungen, die nach dem Datum dieses Zusatzes abgeschlossen wurden oder angeblich geschlossen werden sollen, die Bestimmungen dieses Zusatzes Vorrang.

*Änderungen der Datenschutzgesetze*

12.5 Der Kunde kann:

12.5.1 indem Sie das Unternehmen von Zeit zu Zeit mindestens dreißig (30) Kalendertage schriftlich darüber informieren, welche Änderungen der Standardvertragsklauseln erforderlich sind, die aufgrund einer Änderung oder Entscheidung einer zuständigen Behörde gemäß diesem Datenschutzgesetz erforderlich sind; und

12.5.2 schlägt alle anderen Varianten dieses Zusatzes vor, die der Kunde vernünftigerweise für notwendig hält, um den Anforderungen aller Datenschutzgesetze gerecht zu werden.

12.6 Wenn der Kunde gemäß Abschnitt 12.5 eine Mitteilung macht, werden die Parteien die vorgeschlagenen Änderungen umgehend besprechen und in gutem Glauben verhandeln, um diese oder alternative Varianten, die auf die in der Mitteilung des Kunden genannten Anforderungen zugeschnitten sind, zu vereinbaren und umzusetzen, sobald dies vernünftigerweise praktikabel ist.

*Abfindung*

12.7 Sollte eine Bestimmung dieses Zusatzes ungültig oder nicht durchsetzbar sein, dann bleibt der Rest dieses Zusatzes gültig und in Kraft. 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 so genau wie möglich gewahrt 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 — Einzelheiten der Datenverarbeitung

**Datenexporteur (Controller):** Kunde, wie in der Vereinbarung angegeben.

**Datenimporteur (Auftragsverarbeiter):** Unternehmen, wie in der Vereinbarung angegeben.

**Gegenstand:** Gegenstand der Datenverarbeitung im Rahmen dieser Datenschutzvereinbarung sind die personenbezogenen Daten des Kunden.

**Dauer der Verarbeitung:** Die Laufzeit der Vereinbarung plus der Zeitraum, bis das Unternehmen alle personenbezogenen Kundendaten gemäß dieser Datenschutzvereinbarung löscht.

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

**Art der Verarbeitung:** Die Art der Datenverarbeitung dient der Bereitstellung der Produkte und/oder Dienstleistungen, wie in der Vereinbarung beschrieben.

**Kategorien von betroffenen Personen:** Kundenangestellte und Mitarbeiter von verbundenen Unternehmen, Kunden und Geschäftspartnern.

**Arten personenbezogener Daten:** Der Kunde kann bestimmte personenbezogene Kundendaten für die Produkte und/oder Dienstleistungen hochladen, einreichen oder auf andere Weise bereitstellen, deren Umfang in der Regel vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird und Kontaktinformationen, Informationen zur Website, Produkt- und Serviceinteraktion, Adressen, Geburtsdatum, Geburtsort, E-Mail-Adressen, Namen, Geschlecht, Titel, Telefonnummern, Führerscheinnummer, Unterschrift, Mitarbeiternummer, Standortinformationen, Gehaltssatz beinhalten kann; Nutzername; Passwort; Leistung Informationen; Qualifikationen und Einschränkungen; Geräteinformationen.

**Sensible Daten übertragen:** Keine.

**Häufigkeit der Übertragung:** Kontinuierlich, je nach Bedarf für die Bereitstellung der Produkte und/oder Dienstleistungen.

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

**Zuständige Aufsichtsbehörde:** Gemäß den geltenden Datenschutzgesetzen oder, in der Reihenfolge ihres Inkrafttretens, 1) gemäß den Bestimmungen der Vereinbarung oder 2) Datenschutzbehörde der Niederlande.

**Aufbewahrung:** Gemäß der Vereinbarung und dieser Datenschutzvereinbarung.

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