CARRIER DATENSCHUTZBESTIMMUNGEN EINKAUF

1. Für diese Bestimmung gelten folgende Definitionen:

   a) **„Datenschutzgesetze“** bezeichnet Gesetze auf nationaler, Bundes-, Landes- und regionaler Ebene, die auf die Verarbeitung personenbezogener Daten durch den Lieferanten im Rahmen der Erfüllung des Vertrags anwendbar sind. Datenschutzgesetze umfassen die DSGVO (Datenschutz Grundverordnung) sowie alle vergleichbaren Gesetze weltweit, darunter (i) das Bundesgesetz über den Datenschutz in der Schweiz, (ii) das Datenschutzgesetz (DSG) in Österreich, (iii) das Bundesdatenschutzgesetz (BDSG) in Deutschland.

   b) **„Personenbezogene Daten“** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen („betroffene Person“), die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Klarstellung: Der Begriff „personenbezogene Daten“ umfasst ohne Einschränkung alle Informationen, die gemäß den Datenschutzgesetzen als personenbezogene Daten gelten.

   c) **„Datenschutzverletzung“** bezeichnet jeden tatsächlichen oder begründet mutmaßlichen Vorfall, der zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder Abfrage übermittelter, gespeicherter oder anderweitig verarbeiteter personenbezogener Daten führt.

   d) **„SVKs“** bezeichnet die **„EWR-Standardvertragsklauseln“**, d. h. die Standardvertragsklauseln, die durch Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021 genehmigt wurden.

2. Der Lieferant verpflichtet sich:

   a) alle geltenden Datenschutzgesetze einzuhalten;

   b) personenbezogene Daten, die im Rahmen der Erfüllung des Vertrags und anschließend verarbeitet werden, weder zu verkaufen noch gegen andere Wertgegenstände einzutauschen;

   c) im Rahmen der Erfüllung des Vertrags keine personenbezogenen Daten für andere Zwecke als die Bereitstellung der Produkte oder Dienstleistungen zu verarbeiten und diese personenbezogenen Daten nicht an Dritte weiterzugeben, es sei denn, dies wird von Carrier verlangt oder ist gesetzlich vorgeschrieben, z. B. im Rahmen von behördlichen Anordnungen, Vorladungen, Durchsuchungsbefehlen oder anderen rechtlichen, behördlichen, administrativen oder staatlichen Verfahren, die die Offenlegung personenbezogener Daten erfordern. Der Lieferant muss wirtschaftlich und rechtlich zumutbare Anstrengungen unternehmen, um die Art und den Umfang der erforderlichen Offenlegung personenbezogener Daten auf das Mindestmaß zu beschränken, das erforderlich ist, um geltendem Recht zu entsprechen. Sofern mit geltendem Recht vereinbar, hat der Lieferant Carrier im Voraus schriftlich über derartige Aufforderungen zur Offenlegung zu informieren, sodass Carrier die Möglichkeit hat, rechtliche, behördliche, administrative oder anderweitige behördliche Verfahren anzufechten, und mit Carrier zusammenzuarbeiten, um den Umfang der Offenlegung auf das gesetzlich unbedingt erforderliche Maß zu beschränken;

   d) Carrier unverzüglich zu informieren, wenn nach Ansicht des Lieferanten die Erhebung oder Verarbeitung der personenbezogenen Daten von Carrier gemäß der vorliegenden Erklärung gegen Datenschutzgesetze verstößt;

   e) Carrier unverzüglich schriftlich über (neue) Datenschutzgesetze zu informieren, die (i) die Lieferung von Waren oder die Erbringung von Dienstleistungen durch den Lieferanten beeinträchtigen können, (ii) die Ergänzung spezifischer Vertragsbestimmungen vorschreiben

oder anderweitig eine Änderung der vorliegenden Erklärung erfordern oder (iii) die Carrier oder dem Lieferanten Verpflichtungen auferlegen, die von der vorliegenden Erklärung abweichen;

f) sofern der Lieferant einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Namen von Carrier) beauftragt, darf dies ausschließlich im Rahmen eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen die gleichen oder gleichwertige Datenschutzverpflichtungen auferlegt wie dem Lieferanten gemäß der vorliegenden Erklärung auferlegt sind. Der Lieferant stellt sicher, dass der Unterauftragsverarbeiter die Verpflichtungen einhält, denen der Lieferant gemäß der vorliegenden Erklärung und den geltenden Datenschutzgesetzen unterliegt. Der Lieferant bleibt in vollem Umfang verantwortlich und haftet für Handlungen und Unterlassungen von Unterauftragsverarbeitern oder sonstigen Subunternehmern, die personenbezogene Daten von Carrier im Auftrag des Lieferanten verarbeiten, in derselben Weise und in demselben Umfang, in dem er für eigene Handlungen und Unterlassungen in Bezug auf diese personenbezogenen Daten von Carrier haftbar ist. Der Lieferant muss Carrier über jede Nichterfüllung seiner vertraglichen Verpflichtungen durch Unterauftragsverarbeiter informieren;

g) angemessene Maßnahmen zu ergreifen, um die Zuverlässigkeit der Mitarbeiter, Bevollmächtigten, Vertreter, Unterauftragnehmer, Mitarbeiter von Unterauftragnehmern oder anderer vom Lieferanten eingesetzter Personen („Personal des Lieferanten“) zu gewährleisten, die Zugang zu den von Carrier zur Verfügung gestellten personenbezogenen Daten haben, indem er unter anderem (i) sicherstellt, dass das gesamte Personal des Lieferanten durch vertragliche oder gesetzliche Vertraulichkeitsverpflichtungen zu Gunsten von Carrier (die denen des Vertrags entsprechen) zur Wahrung der Vertraulichkeit personenbezogener Daten verpflichtet ist, (ii) sicherstellt, dass das Personal des Lieferanten die Bestimmungen der vorliegenden Erklärung einhält, und (iii) sicherstellt, dass das gesamte Personal des Lieferanten eine angemessene Datenschutzschulung absolviert hat und die notwendigen Anweisungen erhalten hat, um personenbezogene Daten gemäß der vorliegenden Erklärung zu verarbeiten. In jedem Fall hat der Lieferant den Zugang zu den personenbezogenen Daten auf das Personal des Lieferanten zu beschränken, für das der Zugang unbedingt erforderlich ist. Der Lieferant hat die Liste des Personals des Lieferanten, das Zugang zu den personenbezogenen Daten hat, regelmäßig zu überprüfen und den Zugang unverzüglich zu entziehen, wenn er nicht mehr erforderlich ist;

h) Carrier dabei zu unterstützen, die Einhaltung der folgenden Verpflichtungen sicherzustellen, wobei die Art der Verarbeitung personenbezogener Daten und die dem Lieferanten zur Verfügung stehenden Informationen zu berücksichtigen sind. Die Verpflichtung zur: i) Durchführung einer „Datenschutz-Folgenabschätzung“ (Data Protection Impact Assessment, (D)PIA); ii) Durchführung einer Datentransfer-Folgenabschätzung (Transfer Impact Assessment, „TIA“); iii) Rücksprache mit den zuständigen Behörden vor der Verarbeitung, wenn eine (D)PIA ergibt, dass die Verarbeitung ein hohes Risiko birgt, wenn Carrier keine Maßnahmen zur Risikominderung ergreift; iv) Sicherstellung, dass die personenbezogenen Daten richtig und aktuell sind, indem er Carrier unverzüglich informiert, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind; v) Erfüllung der Verpflichtungen gemäß Artikel 32 DSGVO und den Artikeln 33, 36 bis 38 DSGVO; vi) Bereitstellung eines Datenschutzhinweises an die betroffenen Personen, mit denen der Lieferant direkten Kontakt hat, es sei denn, Lieferant und Carrier vereinbaren schriftlich, dass die Verpflichtung zum Datenschutzhinweis ausschließlich in der Verantwortung von Carrier liegt; vii) unverzüglichen Benachrichtigung von Carrier, wenn der Lieferant eine Anfrage einer zuständigen Behörde in Bezug auf personenbezogene Daten oder eine Beschwerde einer Person über die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung von Waren und/oder Dienstleistungen erhält. Der Lieferant arbeitet mit Carrier und gegebenenfalls mit den zuständigen Behörden zusammen, um Carrier die Beantwortung der Korrespondenz oder der Beschwerde zu ermöglichen; viii) die Verpflichtung, (a) Carrier unverzüglich zu benachrichtigen, wenn der Lieferant ein rechtsverbindliches Ersuchen einer Strafverfolgungsbehörde um Offenlegung personenbezogener Daten erhält, sofern dies nicht anderweitig untersagt ist, (b) ein solches Ersuchen um Daten zu prüfen und Ersuchen, die nicht notwendig und verhältnismäßig sind, angemessen einzuschränken und abzulehnen und (c) von Carrier geforderte angemessene Unterstützung zu leisten;

i) Carrier zu gestatten, angemessene Maßnahmen zu ergreifen, um die Einhaltung seiner Verpflichtungen gemäß der vorliegenden Erklärung zu prüfen, einschließlich der Kontrolle der Datenverarbeitungseinrichtungen, -verfahren und -unterlagen des Lieferanten sowie der Ermöglichung von und Mitwirkung an Audits. Vertragsbestimmungen, die für Audits jeglicher Art gelten, gelten auch für Audits im Zusammenhang mit der Einhaltung der Datenschutzgesetze oder der Verpflichtungen des Lieferanten gemäß der vorliegenden Erklärung. Unbeschadet des Vorstehenden hat der Lieferant Audits und Inspektionen, die von Carrier oder von einem von ihm beauftragten Prüfer durchgeführt werden, zuzulassen, dabei mit Carrier zusammenzuarbeiten und dazu beizutragen, und zwar in einer Weise, die (i) der Art und Intensität der mit der Verarbeitung personenbezogener Daten im Rahmen des Vertrags verbundenen Risiken und (ii) dem Grad der Dringlichkeit und der Schwere des tatsächlichen oder vermuteten potenziellen Verstoßes gegen die Verpflichtungen der Parteien gemäß den Datenschutzgesetzen angemessen ist. Im Allgemeinen muss Carrier den Lieferanten mindestens 30 Tage vor der Durchführung solcher Audits benachrichtigen, es sei denn, ein früheres Audit/eine frühere Inspektion ist nach den geltenden Datenschutzgesetzen erforderlich oder wird von den zuständigen Behörden angeordnet;

j) Carrier nach der ersten Aufforderung sämtliche gemäß ISO 27001, ISO 29100, SSAE 16 (oder SAS 70), SSAE 18, SOC 2 oder ISAE 3402 erstellten Audit-Berichte zur Verfügung zu stellen, die sich auf personenbezogene Daten von Carrier beziehen;

k) angemessene technische, physische, organisatorische, administrative und vertragliche Maßnahmen zu ergreifen und aufrechtzuerhalten (einschließlich der Verwendung von Verschlüsselung, Beschränkungen des physischen Zugangs zu allen Orten, an denen von Carrier bereitgestellte personenbezogene Daten gespeichert werden, z. B. die Aufbewahrung solcher Aufzeichnungen in verschlossenen Einrichtungen, Lagerbereichen oder Behältern, Backup- und Disaster-Recovery-Systemen und aller weiteren Maßnahmen, die gemäß den geltenden Datenschutzgesetzen erforderlich oder vorgeschrieben sind, sowie, ohne Einschränkung, aller Sicherheitsmaßnahmen), um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, um die unbefugte oder unrechtmäßige Verarbeitung personenbezogener Daten sowie den versehentlichen oder unrechtmäßigen Verlust, die Zerstörung, die Veränderung, die Offenlegung, das Abrufen, die Speicherung oder die Beschädigung personenbezogener Daten zu vermeiden. Der Lieferant muss diese technischen, physischen, organisatorischen und administrativen Sicherheitsmaßnahmen regelmäßig testen und neu bewerten, um sicherzustellen, dass diese wie gehabt angemessen und wirksam sind.

3. Erhält der Lieferant Kenntnis von einem tatsächlichen oder mutmaßlichen Vorfall, Ereignis, Risiko oder Einbruch, der bzw. das allein oder in Kombination mit anderen Umständen zu einer Datenschutzverletzung im Sinne der obigen Definition führen, diese nach sich ziehen oder anderweitig herbeiführen kann (im Folgenden als „Vorfall“ bezeichnet), ist der Lieferant dazu verpflichtet:

(i) alle angemessenen Vorkehrungen und Maßnahmen zu ergreifen, die erforderlich sind, um den Vorfall einzudämmen und zu beheben, soweit dies möglich ist;

(ii) Carrier zu unterstützen und Carrier alle verfügbaren Informationen bezüglich der Untersuchung, Behebung und Analyse des Vorfalls zur Verfügung zu stellen, es sei denn, dies ist nach geltendem Recht ausdrücklich untersagt;

(iii) sobald Kenntnis von einem solchen Vorfall erlangt wurde, Carrier über alle verfügbaren Einzelheiten in Bezug auf diesen Vorfall zu informieren, weitere Untersuchungen durchzuführen und Carrier alle zusätzlichen Einzelheiten, Informationen oder Schlussfolgerungen zur Verfügung zu stellen, die dem Lieferanten im Laufe der Untersuchung des Vorfalls zugänglich werden;

(iv) falls erforderlich, zusammen mit der Erstmeldung eine ausführliche Erklärung darüber abzugeben, warum eine umfassende Meldung der Datenschutzverletzung nicht früher erfolgen konnte, damit Carrier in Übereinstimmung mit den Datenschutzgesetzen mit der zuständigen Aufsichtsbehörde zusammenarbeiten kann (falls erforderlich, wiederholt);

(v) sicherzustellen, dass Carrier über alle Informationen verfügt, die erforderlich sind, um den zuständigen Behörden einen solchen Vorfall gemäß den Datenschutzgesetzen zu melden,

darunter die Kategorien und die ungefähre Anzahl der betroffenen Personen, die Kategorien und die ungefähre Anzahl der betroffenen Datensätze, der Name und die Kontaktdaten der Kontaktstelle, bei der weitere Informationen zum Vorfall eingeholt werden können, die wahrscheinlichen Folgen eines solchen Vorfalls und die vom Anbieter ergriffenen oder vorgeschlagenen Maßnahmen, um die potenziellen nachteiligen Auswirkungen zu mildern;

(vi) auf eigene Kosten unverzüglich eine vollständige Untersuchung der Umstände des Vorfalls einzuleiten und Carrier so schnell wie möglich sämtliche Berichte und Aufzeichnungen über die Untersuchung zur Verfügung zu stellen;

(vii) auf Kosten des Lieferanten umfassend bei der Untersuchung mit Carrier zusammenzuarbeiten und jede von Carrier geforderte Unterstützung zu leisten, damit Carrier den Vorfall untersuchen und die Datenschutzverletzung ggf. gemäß den Datenschutzgesetzen der zuständigen Behörde melden kann;

(viii) keine Benachrichtigung, Ankündigung oder Veröffentlichung über einen Vorfall (eine „Meldung von Datenschutzverletzungen“) vorzunehmen oder zu genehmigen – sofern nicht gesetzlich oder per gerichtlicher Anordnung vorgeschrieben –, ohne die vorherige schriftliche Zustimmung von Carrier zu Inhalt, Medien und Zeitpunkt der Meldung von Datenschutzverletzungen einzuholen. Ist der Lieferant gesetzlich oder durch Gerichtsbeschluss zur Übermittlung einer Meldung von Datenschutzverletzungen verpflichtet, unternimmt er alle angemessenen Anstrengungen zur Abstimmung mit Carrier, bevor er eine derartige Meldung von Datenschutzverletzungen übermittelt.

4. Nach Beendigung des Vertrags hat der Lieferant im Ermessen von Carrier sämtliche im Auftrag von Carrier verarbeiteten personenbezogenen Daten zu löschen und dies zu bescheinigen oder alle personenbezogenen Daten an Carrier zurückzugeben und vorhandene Kopien zu löschen, es sei denn, die Datenschutzgesetze verlangen die Aufbewahrung der personenbezogenen Daten. Bis zur Löschung oder Rückgabe der Daten hat der Lieferant weiterhin die Einhaltung der vorliegenden Erklärung zu gewährleisten. Ohne Anweisungen und soweit gesetzlich zulässig muss der Lieferant alle personenbezogenen Daten nach Beendigung oder Erfüllung des Vertragsverhältnisses und nach einer Frist von 30 Tagen, die es Carrier ermöglichen soll, die personenbezogenen Daten zurückzufordern, unverzüglich vernichten.

5. Gemäß den schriftlichen Anweisungen von Carrier hat der Lieferant Carrier die Möglichkeit einzuräumen, personenbezogene Daten von Carrier, die älter als ein Jahr (oder ein anderer von den Parteien schriftlich vereinbarter Zeitraum) sind, zu löschen, sofern die Daten nicht zur Erfüllung geltenden Rechts aufbewahrt werden müssen.

6. Die Parteien vereinbaren, dass die SVK durch Verweis Teil des vorliegenden Dokuments werden. Die SVK gelten für personenbezogene Daten, die aus dem Europäischen Wirtschaftsraum oder dem Vereinigten Königreich entweder direkt oder im Wege der Weiterübermittlung in ein Land oder an einen Empfänger außerhalb des Europäischen Wirtschaftsraums oder des Vereinigten Königreichs übermittelt werden, das bzw. der (a) nicht als Land anerkannt ist, das ein angemessenes Schutzniveau für personenbezogene Daten bietet, und (b) nicht durch ein anderes geeignetes Instrument zur Datenübermittlung abgedeckt ist. Wenn der Lieferant als für die Verarbeitung Verantwortlicher handelt, vereinbaren die Parteien, dass Modul 1 Anwendung findet; wenn der Lieferant als Auftragsverarbeiter handelt, vereinbaren die Parteien, dass Modul 2 Anwendung findet. Für Modul 2 gilt Option 2 von Klausel 9(a) und die Mitteilung muss mindestens 30 Tage im Voraus erfolgen. Für beide Module gilt Option 2 für Klausel 17 und der betreffende Datenexporteur ist der maßgebliche. Das deutsche Recht findet Anwendung, wenn das betreffende EU-Land keine Rechte von Drittbegünstigten zulässt. Für Klausel 18 gilt für beide Module, dass Streitigkeiten vor den Gerichten des EU-Landes des jeweiligen Datenexporteurs verhandelt werden müssen. Gibt es mehrere relevante Datenexporteure, vereinbaren die Parteien die Zuständigkeit und den Gerichtsstand der Gerichte in Deutschland. Im Falle eines Widerspruchs zwischen den SVK und dem Vertrag haben die SVK Vorrang.