

1. Für diese Bestimmung gelten folgende Definitionen:
  - a. "Datenschutzgesetze" sind anwendbare Gesetze auf nationaler, Bundes-, Landes- oder Regionalebene in Bezug auf den Datenschutz, den Schutz personenbezogener Informationen oder Daten und die grenzüberschreitende Übermittlung personenbezogener Informationen oder Daten, einschließlich und ohne Einschränkung des Health Insurance Portability and Accountability Act ("HIPAA") von 1996, der Gesetze und Verordnungen der Mitgliedstaaten der Europäischen Union gemäß der EU-Richtlinie 95/46/EG (die "EU-Richtlinie"), der Datenschutz-Grundverordnung ("DSGVO") sowie aller EU-Gesetze oder Verordnungen, die erlassen werden können, um die EU- Richtlinie oder die DSGVO zu ersetzen.
  - b. "Personenbezogene Daten von Carrier beziehen sich auf alle Informationen und Daten, die im Rahmen dieser Vereinbarung an einen Lieferanten oder dessen Mitarbeiter, Vertreter oder Vertragsnehmer übermittelt werden, sowie auf jede Freigabe und dazugehörige Transaktionen, die mit einer identifizierten oder identifizierbaren natürlichen Person in Beziehung stehen, oder die bei einem Verstoß gegen geltendes Recht Datenschutzgesetzen unterliegen.
  - c. „Lieferant“ bezeichnet, soweit dies in einem etwaigen zugehörigen Hauptvertrag nicht anders oder genauer geregelt ist, den Vertragspartner von Carrier oder der Tochtergesellschaft von Carrier, die eine Leistung oder Ware bezieht von diesem Vertragspartner.
  - d. Carrier bezeichnet die Carrier Global Corporation, Palm Beach Gardens, FL, 33418, United States, Webseite: [www.carrier.com](http://www.carrier.com), nachfolgend „Carrier“; sowie all deren Tochtergesellschaften. Die nachfolgenden Pflichten des Lieferanten können generell durch ein Nachkommen gegenüber derjenigen Tochtergesellschaft von Carrier, die konkret im Rahmen eines eventuellen Hauptvertrages eine Leistung oder Ware vom Lieferanten bezieht, nachgekommen werden, sofern sich nicht aus der Natur der nachfolgend geregelten Pflicht etwas anderes ergibt.
2. Für den Lieferanten gilt folgendes:
  - a. Er muss alle geltenden Datenschutzgesetze einhalten.
  - b. Er darf personenbezogene Daten von Carrier nur sammeln, abrufen, nutzen oder teilen und diese Daten nur dann an autorisierte Dritte weitergeben, wenn hierdurch Verpflichtungen erfüllt werden, die sich aus dem Vertrag oder den unter diesem Vertrag veröffentlichten Freigaben ergeben, wenn dies mit den Carrier-Anweisungen übereinstimmt, oder wenn gesetzliche Verpflichtungen eingehalten werden müssen. Der Lieferant wird keine sekundäre oder anderweitige Nutzung (z. B. zum Zwecke des Data Mining) personenbezogener Daten von Carrier vornehmen, außer (i) wenn dies von Carrier ausdrücklich schriftlich im Zusammenhang mit der Nutzung der Services durch Carrier genehmigt wurde, oder (ii) wenn gesetzliche Bestimmungen eingehalten werden müssen.
  - c. Der Lieferant wird Carrier unverzüglich schriftlich benachrichtigen, wenn er der Ansicht ist, dass die Erhebung oder Verarbeitung personenbezogener Daten von Carrier gemäß dieser DPTA gegen Datenschutzgesetze verstößt.
  - d. Er darf keine personenbezogenen Daten von Carrier an Dritte weitergeben, übermitteln, offenlegen oder zugänglich machen, es sei denn, um Dienstleistungen im Rahmen des Vertrags zu erbringen, oder um gesetzliche Bestimmungen einzuhalten. Wenn der Lieferant personenbezogene Daten von Carrier an Dritte weitergibt, übermittelt, offenlegt oder Zugriff auf diese gewährt, gilt folgendes:

- e. Der Lieferant ist in der gleichen Weise und im gleichen Umfang verantwortlich für die Handlungen und Unterlassungen aller Vertragsnehmer oder anderer Dritter, die (im Sinne der geltenden Datenschutzgesetze) personenbezogene Daten von Carrier im Namen des Lieferanten verarbeiten, wie er für seine eigenen Handlungen und Unterlassungen in Bezug auf solche personenbezogenen Daten von Carrier verantwortlich ist.
- f. Der Lieferant muss sicherstellen, dass solche Dritte an eine schriftliche Vereinbarung gebunden sind, die die gleichen oder gleichwertige Verpflichtungen und Schutzmaßnahmen wie die in diesem Abschnitt aufgeführten enthält.
- g. Er darf die Daten außerdem nur insoweit weitergeben, übermitteln, offenlegen oder Zugriff auf sie gewähren, wie ein solches Verhalten geltendem Recht entspricht.
- h. Er muss kommerziell zumutbare Maßnahmen ergreifen, um die Zuverlässigkeit der Mitarbeiter, Vertreter, Vertragsnehmer, Mitarbeiter der Vertragsnehmer oder sonstiger vom Lieferanten eingesetzten Personen (zusammenfassend "Lieferantenpersonal") mit Zugriff auf die personenbezogenen Daten von Carrier sicherzustellen. Er muss außerdem sicherstellen, dass das Lieferantenpersonal verpflichtet ist, die Vertraulichkeit der personenbezogenen Daten von Carrier zu wahren, z. B. durch eine Vertraulichkeitsvereinbarung oder durch Anwendung einschlägiger Gesetze oder Vorschriften.
- i. Er muss Informationen, Unterstützung und Zusammenarbeit bereitstellen, wenn dazu ein begründeter Bedarf von Carrier oder teilnehmenden Carrier-Websites besteht, etwa, um von Zeit zu Zeit die Einhaltung der Datenschutzgesetze durch den Lieferanten zu überprüfen.
- j. Er muss auf Anfrage von Carrier erlauben, dass Carrier externe Auditoren beauftragt, um die Einhaltung der Verpflichtungen des Lieferanten und Dritter im Rahmen dieser Vereinbarung zu überprüfen. Zusätzlich muss der Lieferant Carrier auf Anfrage Auditberichte zur Verfügung stellen, die gemäß ISO 27001, ISO 29100, SSAE 16 (oder SAS 70), SOC 2 ODER ISAE 3402 erstellt wurden und personenbezogene Daten von Carrier abdecken.
- k. Er muss Carrier ermöglichen, Personen zu benachrichtigen, deren personenbezogene Daten von Carrier mit dem Lieferanten geteilt werden.
- l. Er muss verhältnismäßige und angemessene technische, physische und administrative Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten von Carrier treffen. Diese Maßnahmen umfassen angemessene Einschränkungen für den physischen Zugang zu Speicherorten, die personenbezogene Daten von Carrier enthalten, z. B. die Speicherung solcher Datensätze in gesperrten Einrichtungen, Lagerbereichen oder Containern. Der Lieferant muss die ergriffenen Maßnahmen regelmäßig neu bewerten, um sicherzustellen, dass sie nach wie vor verhältnismäßig und angemessen sind.
- m. Der Lieferant muss Carrier kommerziell zumutbare Unterstützung bei folgendem leisten:
  - i. Löschen personenbezogener Daten von Carrier auf Anfrage der natürlichen oder juristischen Person;
  - ii. Ermöglichen des Ausstiegs von Einzelpersonen;

- n. Ermöglichen des Löschens personenbezogener Daten durch Carrier, die älter als ein Jahr oder eine andere von den Parteien schriftlich vereinbarte Frist sind, es sei denn, dass die Daten nach geltendem Recht anderweitig gespeichert werden müssen; und
- o. Carrier umgehend schriftlich darauf hinweisen, wenn er von folgendem Kenntnis erhält: (i) Beschwerden oder Anschuldigungen bezüglich eines Verstoßes gegen Datenschutzgesetze im Zusammenhang mit den personenbezogenen Daten von Carrier, (ii) Anfragen einzelner oder mehrerer Personen, auf die personenbezogenen Daten von Carrier zuzugreifen, diese zu korrigieren oder sie zu löschen, (iii) Untersuchungen oder Beschwerden einzelner oder mehrerer Personen in Bezug auf das Erfassen, Verarbeiten oder Übermitteln der personenbezogenen Daten von Carrier oder (iv) allen behördlichen Anfragen, Vorladungen, Durchsuchungsbefehlen oder anderen gesetzlichen, behördlichen, administrativen oder staatlichen Vorgängen, die die Suche nach personenbezogenen Daten von Carrier betreffen (zusammenfassend "Datenschutzangelegenheiten"). Wenn der Lieferant von einer solchen Beschwerde, Anfrage, Anschuldigung oder Nachforschung erfährt, muss der Lieferant Carrier unterstützen und mit Carrier bei der Untersuchung der Angelegenheit kooperieren, einschließlich und ohne Einschränkung der Bereitstellung der relevanten Informationen für Carrier, der Vorbereitung einer Antwort, der Umsetzung von Rechtsbehelfen und/oder der Mitwirkung bei der Durchführung und Verteidigung von Ansprüchen, Gerichts- oder Behördenverfahren. Carrier ist für die Kommunikation mit Einzelpersonen in Bezug auf ihre personenbezogenen Daten von Carrier im Zusammenhang mit solchen Datenschutzangelegenheiten verantwortlich, es sei denn, Carrier ermächtigt den Lieferanten, dies in seinem Namen zu tun. Der Lieferant muss kommerziell und rechtlich zumutbare Anstrengungen unternehmen, um die Art und den Umfang der erforderlichen Offenlegung personenbezogener Daten von Carrier auf das Mindestmaß zu beschränken, das erforderlich ist, um geltendem Recht zu entsprechen. Sofern dies nicht durch anwendbares Recht verhindert wird, muss der Lieferant Carrier vorab schriftlich über solche Datenschutzangelegenheiten informieren, sodass Carrier die Gelegenheit hat, rechtliche, behördliche, administrative oder andere staatliche Vorgänge anzufechten.
3. Der Lieferant muss Carrier baldmöglichst und keinesfalls später als 48 Stunden nach deren Auftreten oder Bekanntwerden schriftlich auf jegliche tatsächlichen, vermuteten oder angedrohten Vorfälle im Zusammenhang mit versehentlicher oder rechtswidriger Zerstörung oder unbeabsichtigtem Verlust, Veränderung, nicht autorisiertem oder unbeabsichtigtem Offenlegen von bzw. Zugriff auf personenbezogene Daten von Carrier ("Sicherheitsverstoß") hinweisen. Anschließend muss er angemessene Maßnahmen ergreifen, um den Sicherheitsverstoß einzudämmen oder zu beheben. Sofern dies nicht gesetzlichen Einschränkungen unterliegt, muss er Carrier Informationen zur Untersuchung und Behebung des Sicherheitsverstoßes bereitstellen. Ohne vorherige schriftliche Zustimmung und Genehmigung des Inhalts, der Medien und des Zeitpunkts durch Carrier darf er keine Bekanntmachung, Ankündigung, Veröffentlichung oder anderweitige Verbreitung jeglicher Hinweise oder Informationen über einen Sicherheitsverstoß ("Verstoßmeldung") vornehmen, sofern er hierzu nicht gesetzlich oder per Gerichtsbeschluss verpflichtet ist. Selbst wenn er gesetzlich oder per Gerichtsbeschluss verpflichtet ist, muss er angemessene Anstrengungen unternehmen, um sich vor dem Einreichen einer Verstoßmeldung mit Carrier zu koordinieren. Wenn der Sicherheitsverstoß Datenelemente umfasst, die zu Identitätsdiebstahl führen können, und in den Netzwerken oder Systemen des Lieferanten stattfindet oder vom Lieferanten verschuldet wurde, übernimmt der Lieferant auf Anfrage von Carrier die Kosten für die Beseitigung der Mängel (einschließlich, falls angemessen und erforderlich, ein Call-Center). Er muss den betroffenen Personen für ein Jahr oder einen längeren Zeitraum Kreditüberwachung oder andere kommerziell zumutbare Dienstleistungen zur Minderung der durch den Identitätsdiebstahl verursachten Schäden bereitstellen, entsprechend gesetzlicher oder behördlicher Vorschriften.

4. Der Lieferant muss die vorherige schriftliche Zustimmung aller natürlichen Personen einholen, von denen der Lieferant personenbezogene Daten von Carrier erhebt, wenn dies aufgrund anwendbarer Datenschutzgesetze oder gemäß den Anweisungen von Carrier erforderlich ist. Für den Fall, dass der Lieferant Carrier personenbezogene Daten zur Verfügung stellt, die durch Datenschutzgesetze geschützt sind, stellt der Lieferant sicher, dass diese personenbezogenen Daten im Einklang mit geltendem Recht bereitgestellt werden, einschließlich, falls erforderlich, der Einholung der Einwilligung oder Benachrichtigung.
5. Alle vom Lieferanten erhobenen personenbezogenen Daten von Carrier müssen auf Wunsch der teilnehmenden Carrier-Website zurückgegeben oder vernichtet werden, es sei denn: (i) solche personenbezogenen Daten von Carrier werden vom Lieferanten benötigt, um seinen Verpflichtungen aus diesem Vertrag oder gemäß geltendem Recht nachzukommen; oder (ii) die Rückgabe oder Vernichtung ist nach geltendem Recht verboten. Ohne gegenteilige Anweisungen und, soweit gesetzlich nicht verboten, muss der Verkäufer alle personenbezogenen Daten von Carrier nach der Beendigung oder dem Abschluss der Bestellung und nach einer Frist von 30 Tagen, die es Carrier ermöglichen soll, die personenbezogenen Daten zurückzufordern, unverzüglich vernichten.
6. Wenn die Datenschutzgesetze geändert werden, muss der Lieferant mit Carrier zusammenarbeiten, um erforderliche Änderungen an dieser DPTA vorzunehmen. Der Lieferant verpflichtet sich, jeden Dritten mit diesen oder vergleichbaren Änderungen zu beauftragen.
7. Wenn diese Vereinbarung und/oder Bestellung die Bereitstellung von Dienstleistungen beinhaltet, bei denen der Lieferant (i) als Verantwortlicher handelt (wie in der EU-Richtlinie definiert) und (ii) personenbezogene Daten des Käufers aus einem Land des Europäischen Wirtschaftsraums oder der Schweiz (zusammengefasst "EWR/CH") an einen Empfänger außerhalb des EWR/CH übermittelt, dann stimmen der Käufer und der Lieferant zu, dass die Bedingungen der Mustervertragsklauseln (auch als Standardvertragsklauseln bezeichnet), die von der Europäischen Kommission in der Entscheidung 2004/915/EC (im folgenden als "Auftragsverarbeitungsmusterklauseln" oder "Musterklauseln" bezeichnet) angenommen wurden, hierin durch Bezugnahme so enthalten sind, als wären sie dargelegt. Wenn diese Vereinbarung und/oder Bestellung die grenzüberschreitende Übermittlung personenbezogener Daten des Käufers aus einem Land des EWR/CH an einen Empfänger außerhalb des EWR/CH beinhaltet, der Lieferant jedoch nicht als Verantwortlicher handelt, stimmen der Käufer und der Lieferant zu, dass die Bedingungen der Mustervertragsklauseln (auch als Standardvertragsklauseln bezeichnet), die von der Europäischen Kommission in der Entscheidung 2010/87/EU (im folgenden als "Verarbeitermusterklauseln" oder "Musterklauseln" bezeichnet) angenommen wurden, hierin durch Bezugnahme so enthalten sind, als wären sie dargelegt. Ungeachtet des Vorstehenden stimmen Käufer und Lieferant folgendem zu:
  - a. Die Musterklauseln können als eigenständiges Dokument mit den Unterschriften zu dieser Vereinbarung und/oder Bestellung neu formatiert werden, oder die Parteien führen die Musterklauseln als separates eigenständiges Dokument aus. Die eigenständigen Musterklauseln können bei Aufsichtsbehörden eingereicht und/oder für andere gesetzlich zulässige Zwecke verwendet werden und haben dieselbe Auswirkung, als ob sie direkt unterzeichnet wären.
  - b. Wenn eine der Parteien versucht, die Musterklauseln bei einer Regulierungsbehörde zu registrieren, und die Regulierungsbehörde die Registrierung ablehnt, arbeiten die Parteien zusammen, um die Exponate der Musterklauseln den Anforderungen der Regulierungsbehörde entsprechend anzupassen.

- c. Wenn eine der Bedingungen der Musterklauseln mit den Bedingungen dieser Vereinbarung und/oder Bestellung kollidiert, haben die Musterklauseln Vorrang.
- d. Wenn der Lieferant Vertragsnehmer beschäftigt, die auf von den Musterklauseln abgedeckte personenbezogene Informationen des Käufers zugreifen, muss der Lieferant sicherstellen, dass Übermittlungen an den Vertragsnehmer in Übereinstimmung mit den Musterklauseln erfolgen.

Hamburg, Dezember 2020

Chubb Deutschland GmbH