**VEREINBARUNG ZUR DATENVERARBEITUNG UND DATENTRANSFER**

**Für unabhängige Verantwortliche / Auftragsverarbeiter (kombinierte Fassung)**

Diese Vereinbarung zur Datenverarbeitung und Datentransfer ("DPTA") tritt mit dem Datum der zuletzt geleisteten Unterschrift in diesem Dokument in Kraft und ergänzt die "Vereinbarung" zwischen **[COLLINS ENTITY NAME einfügen**] (nachfolgend "Käufer" oder "Collins") und dem Lieferanten sowie seinen Tochtergesellschaften und verbundenen Unternehmen (nachfolgend "Lieferant"). Sowohl der Käufer als auch der Lieferant werden in der Vereinbarung namentlich benannt.

Dieses DPTA regelt den Austausch personenbezogener Daten zwischen den Parteien und wird in die Vereinbarung zwischen den Parteien aufgenommen.

Großgeschriebene Begriffe in diesem DPTA haben die Bedeutung, die diesen Begriffen gemäß Absatz 1 (oder an anderen Stellen in diesem DPTA oder der Vereinbarung) zugeschrieben wird, und, sofern nicht anders definiert, ihre gewöhnliche und übliche Bedeutung.

1. Für dieses Dokument gelten **die folgenden** Definitionen:
   1. "Vereinbarung" bezieht sich auf alle Vereinbarungen oder Bestellungen (einschließlich, aber nicht beschränkt auf Leistungsbeschreibungen oder Aufträge) zusammen mit allen vorherigen Änderungen, Modifikationen, Überarbeitungen und/oder damit verbundenen Datenverarbeitungsvereinbarungen, mit denen der Lieferant Geschäftsaktivitäten durchführt und/oder Dienstleistungen für Collins erbringt.
   2. "Geschäftstätigkeiten" und/oder "Dienstleistungen" bezeichnen die Dienstleistungen und Arbeiten, die im Rahmen einer Vereinbarung erbracht werden, die diesem DPTA unterliegt.
   3. "Datenschutzgesetze" bezeichnet geltende nationale, bundesstaatliche, staatliche und örtliche Gesetze in Bezug auf den Datenschutz, den Schutz personenbezogener Informationen oder Daten und die grenzüberschreitende Übermittlung personenbezogener Informationen oder Daten, einschließlich, aber nicht beschränkt auf (a) den California Consumer Privacy Act ("CCPA") (und Vorschriften zur Umsetzung, Überarbeitung oder Ersetzung des CCPA); (b) die EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) ("DSGVO"); (c) der Data Protection Act von 2018 (die "britische DSGVO"); und (d) nationale Rechtsvorschriften, die zur Umsetzung, Überarbeitung oder Ersetzung des Vorstehenden, erlassen werden.
   4. "Personenbezogene Daten" sind alle Informationen oder Daten, die von Collins oder dem Lieferanten oder ihren Agenten, Vertretern oder Subunternehmern im Zusammenhang mit den Geschäftsaktivitäten zur Verfügung gestellt werden und die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen oder, im Falle eines Widerspruchs zu geltendem Recht, den Datenschutzgesetzen unterliegen.
   5. Die Begriffe "Verantwortlicher", "betroffene Person", "Auftragsverarbeiter" und "Verarbeitung" (einschließlich grammatikalischer Abweichungen) haben die in der DSGVO vorgesehene Bedeutung.
2. In Bezug auf die Geschäftsaktivitäten wird Collins als Verantwortlicher für die zur Verfügung gestellten personenbezogenen Daten von Collins handeln, die sich in seinem Besitz, in seiner Verwahrung oder unter seiner Kontrolle befinden, und der Lieferant wird als unabhängiger Verantwortlicher und/oder Auftragsverarbeiter der personenbezogenen Daten von Collins handeln.
3. Soweit die Parteien jeweils als **unabhängige Verantwortliche** handeln, muss jede Partei:
4. alle geltenden Datenschutzgesetze in Bezug auf die von der anderen Partei bereitgestellten personenbezogenen Daten einhalten;
5. den betroffenen Personen, deren personenbezogene Daten die jeweilige Partei im Rahmen der Geschäftsaktivitäten verarbeitet, eine angemessene Datenschutzerklärung und/oder Einwilligung zukommen lassen. Jede Partei ist dafür verantwortlich, eine Datenschutzerklärung bezüglich der Verarbeitung bereitzustellen, für die sie verantwortlich ist. Wenn Collins personenbezogene Daten zur Verfügung stellt und der Lieferant die Daten anonymisiert und nur anonym verarbeitet, vereinbaren die Parteien, dass Collins für die Bereitstellung der Datenschutzerklärung oder Einwilligung verantwortlich ist.
6. die an sie gestellten Anfragen von betroffenen Personen, die auf Auskunft, Zugriff, Berichtigung, Löschung oder Widerspruch gegen die Verarbeitung personenbezogener Daten von Collins im Rahmen der Geschäftsaktivitäten abzielen, bearbeiten. Obwohl jede Partei für die Bearbeitung der Anfragen, die sie erhält, verantwortlich ist, erkennen die Parteien an, dass es Umstände geben kann, die eine Zusammenarbeit erfordern, z. B. wenn eine Partei über eine Datenbank, ein System oder eine andere Technologie verfügt, die den Zugriff, die Berichtigung, die Löschung oder den Widerspruch, den die betroffene Person begehrt, eindeutig ermöglicht. Unter diesen Umständen vereinbaren die Parteien, die andere Partei schriftlich zu benachrichtigen und angemessene kommerzielle Anstrengungen zu unternehmen, um zusammenzuarbeiten; und
7. die Informationen, Unterstützung und Zusammenarbeit bereitstellen, die die andere Partei oder ihre verbundenen Unternehmen von Zeit zu Zeit vernünftigerweise verlangen können, um die Einhaltung der Datenschutzgesetze zu gewährleisten.
8. Soweit **der Lieferant als Auftragsverarbeiter tätig wird**, muss der Lieferant:
9. personenbezogene Daten von Collins lediglich zur Durchführung der Geschäftsaktivitäten (einschließlich der Auditierung von Geschäftsaktivitäten) oder zur Erfüllung gesetzlicher Verpflichtungen erheben, darauf zugreifen, verwenden oder weitergeben oder personenbezogene Daten von Collins nur an autorisierte Dritte übermitteln. Der Lieferant wird die personenbezogenen Daten von Collins nicht zu sekundären neuen Zwecken oder anderweitig verwenden (z. B. zum Zwecke des Data Mining), es sei denn, (a) dies ist ausdrücklich schriftlich durch die Vereinbarung oder anderweitig von Collins genehmigt oder (b) gesetzlich vorgeschrieben;
10. personenbezogene Daten von Collins nicht an Dritte weitegeben, übermitteln, offenlegen oder Zugang diesen zu gewähren, es sei denn, dies dient der Erleichterung oder Unterstützung der Geschäftsaktivitäten oder ist gesetzlich vorgeschrieben. Wenn eine der Parteien personenbezogene Daten von Collins an Dritte weitergibt, überträgt, offenlegt oder Zugang zu diesen gewährt, muss sie:
11. für die Handlungen und Unterlassungen von Unterauftragnehmern oder anderen Dritten, die (im Sinne der geltenden Datenschutzgesetze) personenbezogene Daten von Collins auf die gleiche Weise und im gleichen Umfang einstehen wie sie für ihre eigenen Handlungen und Unterlassungen in Bezug auf diese personenbezogenen Daten von Collins verantwortlich sind;
12. sicherstellen, dass dieser Dritte an eine schriftliche Vereinbarung gebunden ist, die dieselben oder gleichwertige Verpflichtungen und Schutzmaßnahmen wie die in diesem Abschnitt dargelegten enthält; und
13. nur insoweit personenbezogene Daten an Dritte weitergeben, übertragen, offenlegen oder Zugang gewähren als ein solches Verhalten mit geltendem Recht vereinbar ist;

Dieser Abschnitt 4(b) betrifft nicht die Weitergabe an oder die Übertragung, Offenlegung oder Gewährung des Zugangs zu einer oder mehreren staatlichen Stellen gemäß einer gesetzlichen Verpflichtung. Ein solches Vorgehen muss in einer Weise erfolgen, die darauf abzielt, die Weitergabe personenbezogener Daten von Collins zu schützen und einzuschränken, soweit dies vernünftigerweise und rechtlich zulässig ist.

1. wirtschaftlich angemessene Schritte unternehmen, um die Zuverlässigkeit seiner Mitarbeiter, Agenten, Vertreter, Unterauftragnehmer, Mitarbeiter von Subunternehmern oder anderer eingesetzter Personen, die Zugriff auf die personenbezogenen Daten von Collins haben (zusammen "Personal"), zu gewährleisten;

sicherstellen, dass dieser Zugriff auf einer Basis des „Wissen-Müssens“ erfolgt, einschließlich der Erstellung von Vertraulichkeitsvereinbarungen; und

sicherstellen, dass das Personal verpflichtet ist, die Vertraulichkeit der personenbezogenen Daten von Collins zu wahren, z. B. durch eine Vertraulichkeitsvereinbarung oder durch Anwendung der Unternehmensrichtlinie, der einschlägigen Gesetze oder Vorschriften;

1. angemessene und geeignete technische, physische und administrative Sicherheitsvorkehrungen zum Schutz der personenbezogenen Daten von Collins treffen. Diese Maßnahmen umfassen angemessene Beschränkungen des physischen Zugangs zu allen Orten, an denen personenbezogene Daten von Collins gespeichert werden, wie beispielsweise die Aufbewahrung von Unterlagen in verschlossenen Einrichtungen, Lagerräumen oder Behältern. Der Lieferant muss die getroffenen Maßnahmen regelmäßig neu bewerten, um sicherzustellen, dass sie weiterhin angemessen und geeignet sind;
2. Collins wirtschaftlich angemessen zu unterstützen bei: (i) Löschung personenbezogener Daten von Collins auf Anfrage einer betroffenen Person oder eines gesetzlichen Vertreters, falls zutreffend; und (ii) Bearbeitung von Anfragen von betroffenen Personen, die sich gegebenenfalls gegen die Nutzung ihrer Daten entscheiden möchten;
3. Personenbezogene Daten von Collins nur so lange wie erforderlich aufzubewahren und danach die personenbezogenen Daten von Collins zu löschen, es sei denn, es ist gesetzlich vorgeschrieben, die Daten aufzubewahren;
4. Collins unverzüglich schriftlich zu benachrichtigen, wenn der Lieferant über Folgendes Kenntnis erlangt:

(i) Beschwerden oder Behauptungen, die auf einen Verstoß gegen die Datenschutzgesetze in Bezug auf die personenbezogenen Daten von Collins hinweisen;

(ii) Anfragen oder Beschwerden von einer oder mehreren betroffenen Personen im Hinblick auf die Verarbeitung personenbezogener Daten; und

(iii) jede behördliche Anfrage, Vorladung, Durchsuchungsbefehl oder andere rechtliche, regulatorische, administrative oder staatliche Verfahren, die personenbezogene Daten von Collins (zusammenfassend als "Datenschutzangelegenheiten" bezeichnet) zum Gegenstand haben. Wenn der Lieferant von einer Datenschutzangelegenheit erfährt, muss er Collins nicht nur schriftlich benachrichtigen, sondern auch angemessene Unterstützung leisten, einschließlich der Zusammenarbeit mit Collins bei der Untersuchung der Datenschutzangelegenheit, der Bereitstellung relevanter Informationen für Collins, der Unterstützung bei der Vorbereitung einer Antwort, der Implementierung eines Rechtsbehelfs und/oder der Zusammenarbeit bei der Durchführung und Abwehr von Ansprüchen, Gerichts- oder behördliche Verfahren. Der Lieferant unternimmt wirtschaftlich und rechtlich vertretbare Anstrengungen, um die Art und den Umfang einer erforderlichen Offenlegung auf das Mindestmaß an personenbezogenen Daten von Collins zu beschränken, das zur Einhaltung der geltenden Gesetze erforderlich ist. Sofern dies nicht durch geltendes Recht anderweitig geregelt, informiert der Lieferant Collins im Voraus schriftlich über alle Datenschutzangelegenheiten, damit Collins rechtliche, behördliche, administrative oder andere staatliche Verfahren anzufechten kann; und

1. Der Lieferant wird Collins unverzüglich und möglichst innerhalb von achtundvierzig (48) Stunden schriftlich über jeden ihm zur Kenntnis gelangenden Vorfall der versehentlichen oder rechtswidrigen Zerstörung oder eines ungewollten Verlusts, einer Änderung, einer unbefugten oder versehentlichen Offenlegung oder des Zugriffs auf von Collins zugänglich gemachten personenbezogene Daten informieren (eine "Sicherheitsverletzung").

Der Lieferant hat alle zumutbaren Maßnahmen zu ergreifen, um die Sicherheitsverletzung einzudämmen und zu beheben, soweit dies möglich ist; er stellt Collins Informationen über die Untersuchung und Behebung der Sicherheitsverletzung zur Verfügung, sofern dies nicht gesetzlich eingeschränkt ist;

Der Lieferant wird nicht ohne vorherige schriftliche Genehmigung von Collins und nicht ohne vorherige schriftliche Zustimmung zum Inhalt, Medium und Zeitpunkt der Benachrichtigung über die Sicherheitsverletzung (falls zutreffend) eine Benachrichtigung, Ankündigung oder Veröffentlichung vornehmen oder anderweitig die Verbreitung von Mitteilungen oder Informationen über eine Sicherheitsverletzung („Benachrichtigung über die Sicherheitsverletzung“) veranlassen, es sei denn, dies ist gesetzlich oder durch Gerichtsbeschluss vorgeschrieben; und selbst wenn dies gesetzlich oder per Gerichtsbeschluss erforderlich ist, alle angemessenen Anstrengungen zu unternehmen, um sich vor der Bereitstellung einer Benachrichtigung über die Sicherheitsverletzung mit Collins abzustimmen. Wenn die Sicherheitsverletzung (a) Daten in den Netzwerken oder Systemen des Lieferanten betrifft oder (b) auf das Verschulden des Lieferanten zurückzuführen ist, trägt dieser auf Verlangen von Collins die Kosten der Behebung, benachrichtigt die betroffenen Personen und stellt, soweit zutreffend, Diebstahlüberwachungsdienste bereit.

1. Sollten die Datenschutzgesetze geändert werden, werden die Parteien zusammenarbeiten, um alle erforderlichen Änderungen an diesem DPTA vorzunehmen. Die Parteien werden wirtschaftlich vertretbare Anstrengungen unternehmen, um jeden Dritten zu veranlassen, diese oder vergleichbare Änderungen vorzunehmen.
2. Datentransfers / Datenübermittlung

Wenn die Vereinbarung die Bereitstellung von Geschäftsaktivitäten beinhaltet, bei denen der Lieferant personenbezogene Daten von Collins aus einem Land des Europäischen Wirtschaftsraums, des Vereinigten Königreichs oder der Schweiz (zusammen "EWR/UK/CH") in Länder außerhalb des EWR/UK/CH überträgt, für die kein Angemessenheitsbeschluss vorliegt, vereinbaren Collins und der Lieferant, dass die von der Europäischen Kommission im Beschluss 2021/914/EU angenommenen Standardvertragsklauseln (nachfolgend die "SCCs") durch Verweis aufgenommen werden, als ob sie hierin enthalten wären.

Darüber hinaus unterliegen Übermittlungen aus dem Vereinigten Königreich an Orte außerhalb des Vereinigten Königreichs, für die keine Angemessenheitsentscheidung vorliegt, ebenfalls den verbindlichen Klauseln des genehmigten Nachtrags, d. h. dem Muster-Nachtrag B.1.0, der vom Information Commissioner's Office herausgegeben und dem Parlament gemäß § 119A des Data Protection Act 2018 am 2. Februar 2022 vorgelegt wurde, da sie gemäß Abschnitt 18 dieser verbindlichen Klauseln überarbeitet wurde, die durch Verweis in diesen Text aufgenommen wurden, als wären sie hierin enthalten (nachfolgend „Verbindliche Klauseln des Vereinigten Königreichs“).

In Ergänzung des Vorstehenden vereinbaren Collins und der Lieferant Folgendes:

* 1. Die Parteien vereinbaren, dass der Lieferant entweder als unabhängiger Verantwortlicher und/oder Auftragsverarbeiter handelt, wobei in diesem Fall entweder ***"Modul Eins***" und/oder "***Modul Zwei***" Anwendung finden.
  2. In Bezug auf **Klausel 9(a) [Einsatz von Unterauftragsverarbeitern]** gilt Option 2 [allgemeine schriftliche Genehmigung], und die Benachrichtigung muss mindestens 30 Tage im Voraus erfolgen. Wenn der Lieferant jedoch einen Unterauftragsverarbeiter einsetzt, der seine Geschäftstätigkeit einstellt, oder wenn eine andere Notsituation vorliegt, muss der Lieferant: (i) so früh wie möglich darüber informieren; (ii) wirtschaftlich angemessene Anstrengungen unternehmen, um sicherzustellen, dass der Unterauftragsverarbeiter kein Wettbewerber von Collins ist; und (iii) Collins danach 30 Tage Zeit geben, um Einspruch zu erheben und, falls Collins Einwände erhebt, einen alternativen Unterauftragsverarbeiter benennen. Collins erklärt sich bereit, sämtliche Einwände nach Treu und Glauben zu erheben. Der Lieferant kann seine Mitteilung über Unterauftragsverarbeiter bereitstellen, indem er eine Liste auf einer Website veröffentlicht, die Collins schriftlich mitgeteilt wird, oder indem er eine schriftliche Liste an Collins sendet, oder gemäß anderweitiger schriftlicher Vereinbarung der Parteien.
  3. In Bezug auf **Klausel 17** (Option 2) **[Anwendbares Recht]** vereinbaren die Parteien, dass - mit Ausnahme von Transfers aus dem Vereinigten Königreich, die dem Recht von England und Wales unterliegen -, das **Belgische Recht** Anwendung findet, wenn der jeweilige EU-Mitgliedstaat keine Sonderrechte für Dritte vorsieht.
  4. In Bezug auf **Klausel 18 [Wahl des Gerichtsstands und der Gerichtsbarkeit]** werden Streitigkeiten vor den Gerichten des EU-Mitgliedstaats entschieden, in dem der betreffende Datenexporteur ansässig ist. Wenn es mehrere relevante Datenexporteure gibt, vereinbaren die Parteien die Zuständigkeit und den Gerichtsstand der Belgischen Gerichte, mit Ausnahme von Streitigkeiten, die sich ausschließlich aus einem Transfer aus dem Vereinigten Königreich ergeben und für die die Parteien Zuständigkeit und Gerichtsstand der Gerichte von England und Wales vereinbaren.
  5. Die Anhänge I und II der SCCs sind als Anlage 1A bzw. 1B beigefügt. Anhang III ist nicht anwendbar.
  6. Im Falle eines Widerspruchs zwischen den SCCs (in der jeweils durch die Verbindlichen Klauseln des Vereinigten Königreichs geänderten Fassung) und dieser Vereinbarung oder einer Leistungsbeschreibung oder einer Bestellung im Rahmen dieser Vereinbarung haben die SCCs Vorrang.
  7. Wenn die Standardvertragsklauseln durch Gesetze oder Vorschriften (z. B. durch Maßnahmen der Europäischen Union) geändert werden, vereinbaren die Parteien, dass die geänderte Version, soweit gesetzlich zulässig, automatisch in Kraft tritt und Anlage 1 ersetzt.

1. Wenn die Vereinbarung das Erheben oder Verarbeiten personenbezogener Daten von Personen in Kalifornien beinhaltet, dann vereinbaren die Parteien, dass der Lieferant ein "Service Provider" entsprechend der Definition dieses Begriffs im kalifornischen Consumer Privacy Act, Cal, Civ. Code §§ 1798.100 ff. und der Durchführungsbestimmungen (der "CCPA") ist und dass er personenbezogene Daten weder verkauft noch gegen etwas von Wert eintauscht. Wenn die Vereinbarung nicht die Erhebung oder Verarbeitung von Collins personenbezogenen Informationen betroffener Personen in Kalifornien beinhaltet, findet dieser Abschnitt 7 keine Anwendung.
2. Dieses DPTA stellt die gesamte Vereinbarung zwischen den Parteien in Bezug auf den hierin behandelten Gegenstand dar und ersetzt alle sich widersprechenden Bedingungen. Widersprüchliche Datenschutz- und Datentransferbedingungen sind für die Parteien im Rahmen der Vereinbarung nicht bindend, es sei denn, dies erfolgt durch ein schriftliches Dokument, das (a) ausdrücklich auf dieses DPTA verweist und (b) von den bevollmächtigten Vertretern beider Parteien unterzeichnet wird.
3. Alle Mitteilungen, die im Rahmen dieses DPTA oder eines der Anlagen (einschließlich Anhängen) bereitgestellt werden, sind an folgende Adresse zu senden:

|  |  |
| --- | --- |
| Für Collins:  Mit einer Kopie an: | Wie in der Vereinbarung festgelegt  Wie in Anlage 1 dieses DPTA festgelegt |
| Für den Lieferanten: | Wie in der Vereinbarung festgelegt |

ZUM URKUNDLICHEN NACHWEIS stimmen die Parteien den oben genannten Bedingungen zu und haben dieses DPTA entsprechend unterzeichnet.

**Collins: [COLLINS ENTITY NAME EINFÜGEN**]

|  |  |
| --- | --- |
| Anschrift (vollständig ausgeschrieben): | [einfügen] |
| Name (vollständig ausgeschrieben): | [einfügen] |
| Titel: | [einfügen] |
| Datum: | [einfügen] |
| Unterschrift: |  |

Lieferant: **[NAME DER LIEFERANTENEINHEIT EINFÜGEN]**

|  |  |
| --- | --- |
| Anschrift (vollständig ausgeschrieben): | [einfügen] |
| Name (vollständig ausgeschrieben): | [einfügen] |
| Titel: | [einfügen] |
| Datum: | [einfügen] |
| Unterschrift: |  |

***Anlage 1A: ANHANG I***

**Anhang I der Standardvertragsklauseln**

Für die Zwecke dieses Anhangs I werden "personenbezogene Daten" als personenbezogene Daten des Käufers definiert.

1. **LISTE DER PARTEIEN**

**A-1. Auswahl der Module**

|  |  |
| --- | --- |
| Prüfen Sie, welche Option(en) zutrifft | |
| X | **MODUL EINS:** **Übermittlung von Verantwortlichen an Verantwortliche** |
| X | **MODUL ZWEI:** **Übermittlung von Verantwortlichen an Auftragsverarbeiter** |
|  | **MODUL DREI:** **Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter** |
|  | **MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche** |

**A-2. Datenexporteur(e): Käufer oder Collins**

|  |  |
| --- | --- |
| Firmenname | Collins Aerospace juristische Person, die über das DPTA referenziert wurde |
| Firmenadresse | per Referenz im DPTA festgelegt |
| Unternehmensrolle (Verantwortlicher oder Auftragsverarbeiter oder beides) | Verantwortlicher / Controller |
| Name der Kontaktperson | Siehe unten |
| Ansprechpartner Position/Titel | Chief Privacy Officer |
| E-Mail-Adresse und/oder Telefonnummer des Ansprechpartners | RTX Corporation  10 Farm Springs Straße  Farmington, CT 06032 USA  [Privacy.compliance@rtx.com](mailto:Privacy.compliance@rtx.com)  + (011) 781-522-3000 |
| Beschreibung der Tätigkeiten, die für die von diesem Unternehmen übermittelten Daten relevant sind | Die in der Vereinbarung beschriebenen Dienstleistungen: Im Rahmen der Inanspruchnahme der Dienstleistungen muss der Datenexporteur personenbezogene Daten gemäß Abschnitt B unten weitergeben. |
| Name der unterzeichnenden Person (muss nicht der Kontakt sein) | per Referenz im DPTA festgelegt |
| Titel der unterzeichnenden Person | per Referenz im DPTA festgelegt |
| Unterschrift | per Referenz im DPTA festgelegt |
| Datum der Unterschrift | per Referenz im DPTA festgelegt |

**A-3. Datenimporteur(e): Lieferant**

|  |  |
| --- | --- |
| Firmenname | Der Name der juristischen Person des Lieferanten, der durch Referenz aus dem DPTA aufgenommen wird |
| Firmenadresse | per Referenz im DPTA festgelegt |
| Unternehmensrolle (Verantwortlicher oder Auftragsverarbeiter oder beides) | Verantwortlicher / Auftragsverarbeiter |
| Name der Kontaktperson | per Referenz in der Vereinbarung festgelegt |
| Ansprechpartner Position/Titel | per Referenz in der Vereinbarung festgelegt |
| E-Mail-Adresse und/oder Telefonnummer des Ansprechpartners | per Referenz in der Vereinbarung festgelegt |
| Beschreibung der Tätigkeiten, die für die von diesem Unternehmen übermittelten Daten relevant sind | Erbringung der Dienstleistungen, wie in der Vereinbarung geregelt |
| Name der unterzeichnenden Person (muss nicht der Kontakt sein) | per Referenz im DPTA festgelegt |
| Titel der unterzeichnenden Person | per Referenz im DPTA festgelegt |
| Unterschrift | per Referenz im DPTA festgelegt |
| Datum der Unterschrift | per Referenz im DPTA festgelegt |

1. **BESCHREIBUNG DER ÜBERMITTLUNG**

**B-1. Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden**

Die übermittelten personenbezogenen Daten betreffen die folgenden Kategorien von Betroffenen:

* Mitarbeiter, Auftragnehmer, Kunden, Endbenutzer, Bewerber und Investoren
* Mitarbeiter der Geschäftspartner von Collins, wie Lieferanten, Dienstleister und Kunden
* Dritte, über deren personenbezogene Daten Collins aus rechtlichen Gründen verfügen kann, z. B. Parteien in Rechtsstreitigkeiten

**B-2. Kategorien der übermittelten personenbezogenen Daten**

Die übermittelten personenbezogenen Daten betreffen folgende Datenkategorien:

Alle personenbezogenen Daten, die erforderlich sind, damit der Datenimporteur die Dienstleistungen gemäß der Vereinbarung erbringen kann.

**B-3. Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie zum Beispiel strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Führung von Aufzeichnungen über den Zugriff auf die Daten, Beschränkungen für die Weiterübermittlung oder zusätzliche Sicherheitsmaßnahmen.**

Die übermittelten personenbezogenen Daten betreffen die folgenden besonderen Kategorien von Daten:

Keine, es sei denn, dies ist gesetzlich vorgeschrieben, um die in der Vereinbarung festgelegten Dienstleistungen zu erbringen.

**B-4. Die Häufigkeit der Übertragung (z. B., ob die Daten einmalig oder kontinuierlich übertragen werden).**

Die Häufigkeit wird je nach Bedarf festgelegt, um die Arbeit im Rahmen des Abkommens zu unterstützen.

**B-5. Art der Verarbeitung**

Die Art der erbrachten Dienstleistungen ist in der Vereinbarung festgelegt. Der Datenimporteur verarbeitet personenbezogene Daten nur zum Zwecke der Erbringung dieser Dienste.

**B-6. Zweck(e) der Datenübermittlung und weitere Verarbeitung**

Die Datenimporteure sind Dienstleister für Collins. Sie werden die Daten nur verarbeiten, um die Dienstleistungen im Rahmen der Vereinbarung zu erbringen.

**B-7. Der Zeitraum, für den die personenbezogenen Daten aufbewahrt werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieses Zeitraums**

Personenbezogene Daten werden nur so lange aufbewahrt, wie es für die Erbringung der Dienstleistungen gemäß dem Vertrag und/oder einer gemäß dem Vertrag ausgeführten Leistungsbeschreibung oder einer gemäß dem Vertrag erteilten Bestellung erforderlich ist.

**B-8. Bei Übermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben**

Alle Übertragungen an Unterauftragsverarbeiter erfolgen im Einklang mit den Bestimmungen der Standardvertragsklauseln, dem Abschnitt "Datenschutz" der Allgemeinen Geschäftsbedingungen und diesem Anhang I.

1. **ZUSTÄNDIGE AUFSICHTSBEHÖRDE**

*Benennen Sie die zuständige(n) Aufsichtsbehörde(n) gemäß Klausel 13 (Aufsicht) der SCCs:*

Mitgliedstaat, in dem der betreffende Datenexporteur niedergelassen ist, der für die Zwecke des Abkommens als das Recht des Geschäftssitzes des für die Datenverarbeitung Verantwortlichen gilt.

***Anlage 1B: ANHANG II***

**TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH TECHNISCHER UND ORGANISATORISCHER**

**MASSNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN**

**X MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche**

**X MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter**

**MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter**

Der Datenimporteur verpflichtet sich, physische, technische und organisatorische Sicherheitsmaßnahmen zu ergreifen und aufrechtzuerhalten, um die Sicherheit der im Zusammenhang mit der Vereinbarung und den darin vorgesehenen Verarbeitungsvorgängen erzeugten, erhobenen, empfangenen oder anderweitig erhaltenen personenbezogenen Daten aufrechtzuerhalten und zu schützen, wobei diese Maßnahmen für die Verarbeitung personenbezogener Daten in Übereinstimmung mit den einschlägigen Datenschutzgesetzen der Europäischen Union erforderlich sind.

Die technischen und organisatorischen Sicherheitsmaßnahmen des Datenimporteurs umfassen mindestens die folgenden (die von Zeit zu Zeit aktualisiert werden können).

**Interne Kontrollen und Systeme**

Der Datenimporteur muss strenge interne Kontrollen gemäß den Richtlinien ISO 27001 und ISO 20000 einhalten. Der Datenimporteur implementiert Sicherheitsregeln in Form von verbindlichen Richtlinien und Verfahren für Mitarbeiter und alle Subunternehmer oder Vertreter, die Zugriff auf personenbezogene Daten von Collins – als Teil der Raytheon Technologies, Inc. Konzerns (RTX) - haben.

Diese Richtlinien und Verfahren umfassen:

- Maßnahmen, Standards, Verfahren, Regeln und Normen, um das angemessene Sicherheitsniveau zu gewährleisten;

- die Bedeutung und Wichtigkeit personenbezogener Daten und die Notwendigkeit, sie sicher, vertraulich und nur mit dem „Wissen-Müssen“-Prinzip zugänglich zu machen;

- Funktionen, Pflichten und Zugriffsrechte des Personals;

- die Verfahren für die Meldung, Verwaltung und Reaktion auf Sicherheitsvorfälle im Zusammenhang mit personenbezogenen Daten; und

- die Verfahren zum Erstellen von Sicherungskopien und zum Wiederherstellen personenbezogener Daten.

**Sicherheit**

Der Zugriff auf personenbezogene Daten durch den Datenimporteur wird durch den Zugriff und die von den Collins bzw. RTX geregelten Verfahren gewährt.

Im Folgenden werden die wichtigsten Sicherheitsverpflichtungen zusammengefasst (und im Falle von Streitigkeiten oder Widersprüchen haben die vereinbarten umfassenderen Sicherheitsverpflichtungen Vorrang):

**Funktionen und Pflichten des Personals in Bezug auf Dateien:**

Die Funktionen und Pflichten jedes Nutzers oder Profils von Nutzern, die Zugang zu den personenbezogenen Daten und zu den Informationssystemen haben, müssen in einem Sicherheitsdokument schriftlich klar und deutlich definiert werden.

**Aufzeichnung von Vorfällen:**

Es wird ein Verfahren für die Meldung und das Management von Sicherheitsvorfällen, die personenbezogene Daten betreffen, und ein Register zur Erfassung des Vorfalls eingerichtet wird, in dem die Art des Vorfalls, der Zeitpunkt, zu dem er aufgetreten ist oder gegebenenfalls festgestellt wurde, die Person, die die Meldung vorgenommen hat, an wen sie weitergegeben wurde, die sich daraus ergebenden Auswirkungen und die angewandten Korrekturmaßnahmen erfasst werden.

**Identifizierung und Authentifizierung:**

Der Datenimporteur ergreift die Maßnahmen, die die korrekte Identifizierung und Authentifizierung der Nutzer gewährleisten. Der Datenimporteur muss einen Mechanismus einrichten, der die eindeutige und personalisierte Identifizierung jedes Benutzers, der versucht, auf das Informationssystem zuzugreifen, sowie die Überprüfung seiner Berechtigung ermöglicht. In dem Sicherheitsdokument ist die Häufigkeit anzugeben, mit der die Passwörter geändert werden, wobei die Häufigkeit unter keinen Umständen geringer als die jährliche sein darf. Während ihrer Gültigkeitsdauer müssen Passwörter in unlesbarer Form gespeichert werden.

**Sicherungskopien und Wiederherstellung:**

In dem Sicherheitsdokument wird verlangt und der Datenimporteur stellt sicher, dass: (1) Backups mindestens wöchentlich erstellt werden; und (2) Datenwiederherstellungsverfahren implementiert werden, die eine Rekonstruktion in den ursprünglichen Zustand zum Zeitpunkt des Verlusts oder der Zerstörung ermöglichen, soweit dies technisch möglich ist.

**Sicherheitsbeauftragter:**

In dem Sicherheitsdokument sind ein oder mehrere Sicherheitsbeauftragte zu benennen, die für die Umsetzung und Überwachung der Einhaltung der Anforderungen des Sicherheitsdokuments zuständig sind. Diese Ernennung kann allgemein für alle Dateisysteme oder die Verarbeitung personenbezogener Daten oder spezifisch sein, abhängig von den verwendeten Informationssystemen, die im Sicherheitsdokument deutlich festgehalten werden.

**Audit:**

Das Sicherheitsdokument muss vorsehen und der Datenimporteur muss sicherstellen, dass mindestens alle zwei Jahre eine interne oder externe Prüfung durchgeführt wird, um die Einhaltung der im Sicherheitsdokument enthaltenen Sicherheitsmaßnahmen zu verifizieren.

**Verwaltung von Medien und Dokumenten:**

Das Sicherheitsdokument verlangt, und der Datenimporteur stellt sicher, dass ein Registrierungs- oder Inventarsystem für die Eingabe von Datenträgern, die Daten enthalten, eingerichtet wird, das direkt oder indirekt die Identifizierung der Art des Dokuments oder der Datenträger sowie des Datums und der Uhrzeit, des Ausstellers und der Anzahl der bei der Übermittlung enthaltenen Dokumente oder Medien, die Art der darin enthaltenen Informationen, die Art der Übertragungsmethode und die für den Empfang verantwortliche Person ermöglicht.

**Identifizierung und Authentifizierung:**

Das Sicherheitsdokument schreibt vor, und der Datenimporteur muss einen Mechanismus einrichten, um den unbefugten Zugriff auf die Daten zu beschränken, einschließlich der Aktualisierung des Sicherheitsdokuments auf der Grundlage neuer oder neu identifizierter Risiken.

**Physische Zugangskontrolle:**

Das Sicherheitsdokument schreibt vor und der Datenimporteur muss sicherstellen, dass nur das autorisierte Personal Zugang zu den Orten hat, in denen sich die physische Ausrüstung befindet, die die Informationssysteme unterstützt.

**Protokoll der Wiederherstellung von Vorfällen:**

Das Register enthält die Verfahren für die Wiederherstellung von Daten unter Angabe der Person, die den Vorgang durchgeführt hat, der wiederhergestellten Daten und gegebenenfalls der Daten, die im Rahmen des Wiederherstellungsprozesses manuell erfasst werden mussten.