SIEMENS

Data Privacy Terms

April 2021

Dieser Vertrag zu Auftragsverarbeitung („**Data Privacy Terms**“ oder „**DPT**“) wird zwischen der in der Vereinbarung genannten Siemens Gesellschaft („**Siemens**") und dem in der Vereinbarung genannten Kunden ("**Kunde**") vereinbart.

1. Anwendungsbereich und Einhaltung Anwendbaren Datenschutzrechts

1.1. Diese DPT regeln die Verarbeitung Personenbezogener Daten im Rahmen der Erbringung des Angebots durch Siemens, soweit Siemens als Auftragsverarbeiter des Kunden tätig wird. In der Vereinbarung wird das Angebot teilweise als „Leistung“, „Service-Leistungen“ oder ähnlich definiert. Die DPT sind Bestandteil der Vereinbarung. Im Falle von Widersprüchen, gehen die DPT Exhibits den DPT vor, die DPT haben Vorrang vor den Regelungen der Vereinbarung.

1.2. Die DPT regeln die datenschutzrechtlichen Rechte und Pflichten des Kunden und von Siemens im Rahmen der Erbringung des Angebots durch Siemens als Auftragsverarbeiter. Im Übrigen bleiben sonstige Rechte und Pflichten der Parteien unberührt und richten sich ausschließlich nach den übrigen Bestimmungen der Vereinbarung.

1.3 Bei der Erbringung des Angebots ist Siemens verpflichtet, das unmittelbar für Auftragsverarbeiter geltende Anwendbare Datenschutzrecht, einschließlich der Bestimmungen zur Meldung von Datenschutzverstößen, einzuhalten. Diese Verpflichtung umfasst nicht die Einhaltung von Datenschutzbestimmungen, die ausschließlich auf den Kunden oder die Branche des Kunden anwendbar sind und nicht allgemein für Auftragsverarbeiter gelten. Der Kunde ist verpflichtet, alle für die Nutzung des Angebots durch den Kunden geltenden rechtlichen Anforderungen, insbesondere das Anwendbare Datenschutzrecht, einzuhalten und sicherzustellen, dass Siemens und Unterauftragsverarbeiter das Angebot gemäß dieser DPT erbringen dürfen.

2. Beschreibung der von Siemens erbrachten Datenverarbeitungstätigkeiten

Eine Beschreibung der von Siemens erbrachten Datenverarbeitungstätigkeiten, insbesondere eine Beschreibung des Gegenstands der Verarbeitung, Art und Zweck der Verarbeitung, Kategorien von Personenbezogenen Daten und Kategorien von Betroffenen Personen, ist in den DPT Exhibits enthalten.

3. Weisungen

Siemens verarbeitet Personenbezogene Daten ausschließlich entsprechend der dokumentierten Weisungen des Kunden. Die Parteien sind einig, dass die Vereinbarung (einschließlich dieser DPT) die abschließenden Weisungen des Kunden in Bezug auf die Verarbeitung von Personenbezogenen Daten durch Siemens als Auftragsverarbeiter darstellen. Ergänzende oder abweichende Weisungen, sind schriftlich zwischen den Parteien zu vereinbaren.

4. Technische und organisatorische Maßnahmen

4.1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft Siemens geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau umzusetzen. Die von Siemens getroffenen technischen und organisatorischen Maßnahmen sind in den DPT Exhibits beschrieben. Der Kunde ist sich bewusst, dass die technischen und organisatorischen Maßnahmen der technischen Weiterentwicklung unterliegen. Siemens hat deshalb das Recht, angemessene Alternativmaßnahmen zu treffen, soweit dabei das vermittelte Schutzniveau nicht abgesenkt wird.

4.2. Die in den DPT Exhibits beschriebenen Maßnahmen gelten für die Datenverarbeitungssysteme und Anlagen von Siemens und von Unterauftragsverarbeitern. Der Kunde ist für die Umsetzung und Aufrechterhaltung angemessener technischer und organisatorischer Maßnahmen für von ihm bereitgestellte oder kontrollierte Anlagen und Systeme verantwortlich (z. B. die Umsetzung von Maßnahmen zu physischen und systemtechnischen Zugangskontrollen zu Räumlichkeiten, Vermögenswerten und IT-Systemen des Kunden oder die Konfiguration des Angebots nach den individuellen Anforderungen des Kunden).

5. Vertraulichkeit der Verarbeitung

Siemens verpflichtet Mitarbeiter, die mit der Verarbeitung personenbezogener Daten betraut sind, (i) auf die Vertraulichkeit der Datenverarbeitung, (ii) personenbezogene Daten ausschließlich entsprechend der Bestimmungen dieser DPT oder dokumentierter Weisungen des Kunden zu verarbeiten und (iii) an Datenschutz- und Sicherheitsschulungen teilzunehmen.

6. Unterauftragsverarbeiter

6.1. Der Kunde stimmt hiermit dem Einsatz von Unterauftragsverarbeitern durch Siemens zu. Die derzeit von Siemens eingesetzten Unterauftragsverarbeiter sind in den DPT Exhibits benannt.

6.2. Siemens ist berechtigt, bestehende Unterauftragsverarbeiter jederzeit auszutauschen oder neue Unterauftragsverarbeiter einzusetzen. Wenn und soweit nach Anwendbarem Datenschutzrecht erforderlich, erfolgt der Einsatz neuer Unterauftragsverarbeiter nur mit Zustimmung des Kunden. Die Zustimmung erfolgt nach folgendem Verfahren: (i) Siemens benachrichtigt den Kunden mindestens 30 Tage vor dem Einsatz und Zugriff des neuen Unterauftragsverarbeiter auf Personenbezogene Daten des Kunden; (ii) widerspricht der Kunde binnen dieses Zeitraums nicht schriftlich und unter Angabe eines wichtigen Grundes, gilt die Zustimmung zum Einsatz des neuen Unterauftragsverarbeiters als erteilt; (iii) widerspricht der Kunde gegenüber Siemens aus wichtigem Grund, wird Siemens im Rahmen des Zumutbaren (a) Änderungen an den Konfigurationen und/oder des Angebots vorschlagen, die eine Inanspruchnahme des Angebots ohne den neuen Unterauftragsverarbeiter möglich machen oder (b) andere Maßnahmen vorschlagen, die geeignet sind, die in dem Widerspruch des Kunden geltend gemachten Gründe auszuräumen; (iv) genügen die vorgeschlagenen Änderungen oder Maßnahmen aus Sicht des

Kunden nicht, um die im Widerspruch geltend gemachten Gründe auszuräumen, ist der Kunde berechtigt, den betroffenen Teil des Angebots innerhalb einer Frist von 14 Tagen nach Zugang der Antwort von Siemens auf den Widerspruch des Kunden schriftlich zu kündigen. Kündigt der Kunde den betroffenen Teil des Angebots nicht innerhalb der 14 tägigen Frist, gilt die Zustimmung des Kunden zum Einsatz des Unterauftragsverarbeiters als erteilt.

6.3. Siemens verpflichtet sich, mit jedem eingesetzten Unterauftragsverarbeiter eine Vereinbarung zu treffen, die dem Unterauftragsverarbeiter im Wesentlichen entsprechende Verpflichtungen auferlegt, wie sie nach diesen DPT für Siemens gelten. Siemens ist für Handlungen und Unterlassungen der eingesetzten Unterauftragsverarbeiter in gleicher Weise wie für eigene Handlungen und Unterlassungen verantwortlich.

7. Auftragsverarbeiter außerhalb des EWR

7.1. Betrifft eine Übermittlung an Auftragsverarbeiter außerhalb des EWR Personenbezogene Daten eines Verantwortlichen mit Sitz im EWR, der Schweiz oder des Vereinigten Königreichs, ist Siemens verpflichtet, die in den DPT Exhibits bezeichneten Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus umzusetzen. Siemens ist berechtigt, die in den DPT Exhibits bezeichneten Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus durch alternative Maßnahmen zu ersetzen. In diesem Fall gilt der Mitteilung- und Zustimmungsmechanismus in Ziffer 6.2 entsprechend.

7.2. Die folgenden Bestimmungen finden Anwendung, wenn und soweit die Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus auf den EU-Standartvertragsklauseln beruhen:

(i) Hat die Siemens-Gesellschaft, mit der die Vereinbarung abgeschlossen wird, ihren Sitz außerhalb des EWR und außerhalb eines Landes mit Angemessenheitsbeschluss, schließen Siemens und der Kunde hiermit die EU-Standardvertragsklauseln ab. Der Kunde schließt die EU-Standardvertragsklauseln im eigenen Namen sowie im Namen der Weiteren Verantwortlichen ab. Die DPT Exhibits „DOT Exhibits - Beschreibung der Auftragsverarbeitungsmaßnahmen“ und „DPT Exhibits - Technische und organisatorische Maßnahmen“ werden als Anlagen 1 und 2 Bestandteil der EU-Standardvertragsklauseln.

(ii) Siemens schließt mit Unterauftragsverarbeitern, die ihren Sitz außerhalb des EWR und außerhalb eines Landes mit Angemessenheitsbeschluss haben, EU-Standardvertragsklauseln ab, die die durch den Unterauftragsverarbeiter erbrachten Verarbeitungstätigkeiten erfassen. Der Kunde und Weitere Verantwortliche werden in die EU-Standardvertragsklauseln werden wie folgt Partei der EU-Standardvertragsklauseln: (a) die EU-Standardvertragsklauseln enthalten das Recht des Kunden und der Weiteren Verantwortlichen, den EU-Standardvertragsklauseln durch einseitige Erklärung beizutreten, d.h. die EU-Standardvertragsklauseln sind mit Abgabe der Beitrittserklärung unabhängig eines Zugangs bei Siemens und dem Unterauftragsverarbeiter für den Kunden, Weitere Verantwortliche und den jeweiligen Unterauftragsverarbeiter verbindlich ("**Beitrittsmechanismus**"); oder (b) Siemens schließt die EU-Standardvertragsklauseln mit dem Unterauftragsverarbeiter im Namen des Kunden und Weiterer Verantwortlicher ab ("**Vollmachtsmechanismus**"). Der Vollmachtsmechanismus findet Anwendung, wenn und soweit dies in den DPT Exhibits für einen Unterauftragsverarbeiter angegeben ist.

7.3. Wenn und soweit die Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus auf den BCR beruhen, verpflichtet Siemens den Unterauftragsverarbeiter vertraglich, die BCR bei der Verarbeitung Personenbezogener Daten im Rahmen dieser DPT einzuhalten.

7.4. Zusätzliche Maßnahmen: Zusätzlich zu den Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveau, bestätigt Siemens hiermit, dass, nach der Kenntnis von Siemens, weder Siemens noch eingesetzte Unterauftragsverarbeiters Gesetzen unterliegen, die die Befolgung der Anweisungen des Kunden und die Einhaltung der vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten der DPT und der Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus auswirken, dem Kunden unmittelbar nach Kenntnis mitteilen wird, und der Kunde dann berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten.

8. Maßnahmen zum Schutz vor Herausgabeanordnungen Dritter

Erhält Siemens eine Anordnung eines Dritten zur Herausgabe der Personenbezogenen Daten, verpflichtet sich Siemens (i) zumutbare Maßnahmen zu ergreifen, dass der Dritte das Herausgabeverlangen direkt gegenüber dem Kunden ausübt, (ii) den Kunden unverzüglich zu informieren, es sei denn die Information des Kunden ist rechtlich untersagt; ist die Information des Kunden rechtlich untersagt, verfügbare Rechtsmittel gegen das Verbot zu ergreifen, um so viele Informationen wie möglich zeitnah an den Kunden geben zu können und (iii) verfügbare Rechtsmittel zu ergreifen, mit denen die Rechtmäßigkeit der Anordnung nach dem für den anfragenden Dritten geltenden Rechts bestritten oder ein Konflikt mit dem Recht des EWRs oder dem Recht eines EWR Mitgliedsstaats geltend gemacht werden kann.

9. Verletzung des Schutzes Personenbezogener Daten

9.1. Siemens unterrichtet den Kunden unverzüglich nach Bekanntwerden einer Verletzung des Schutzes Personenbezogener Daten. Unter Berücksichtigung der Art der Verarbeitung und der Siemens zur Verfügung stehenden Informationen hat die Unterrichtung folgende Angaben zu enthalten: (i) die Art der Verletzung des Schutzes Personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der Betroffenen Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen Personenbezogenen Datensätze, (ii) einen Kontakt, über den weitere Informationen eingeholt werden können, (iii) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes Personenbezogener Daten und (iv) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes Personenbezogener Daten. Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann Siemens diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

9.2. Siemens verpflichtet sich, (i) den Kunden im bei der Erfüllung seiner Pflichten nach Anwendbarem Datenschutzrecht bei Verletzungen des Schutzes Personenbezogener Daten in

angemessener Weise zu unterstützen, und (ii) entsprechende und angemessene Abhilfemaßnahmen umzusetzen.

10. **Rechte betroffener Personen und weitere Unterstützungsleistungen durch Siemens**

10.1. Soweit gesetzlich zulässig, benachrichtigt Siemens den Kunden unverzüglich, wenn Siemens eine Aufforderung eines Betroffenen zur Ausübung seiner Betroffenenrechte (wie z.B. das Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung) erhält.

10.2. Unter Berücksichtigung der Art der Verarbeitung und der Siemens zur Verfügung stehenden Informationen wird Siemens (i) den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachzukommen; (ii) nach eigenem Ermessen entweder (a) dem Kunden die Möglichkeit zur Berichtigung oder Löschung Personenbezogener Daten über die Funktionalitäten des Angebots zur Verfügung stellen oder (b) Personenbezogene Daten auf Anweisung des Kunden berichtigen oder löschen; und (iii) den Kunden in angemessener Weise bei der Erfüllung seiner weiteren Pflichten nach Anwendbarem Datenschutzrecht unterstützen. Die weitergehende Unterstützung gemäß Ziffer (iii) bedarf einer gesonderten Vereinbarung zwischen den Parteien.

11. **Kontrollrechte**

11.1. Soweit dem Kunden nach Anwendbarem Datenschutzrecht ein Kontrollrecht zusteht, ist der Kunde berechtigt, die Einhaltung der datenschutzrechtlichen Verpflichtungen durch Siemens und Unterauftragsverarbeiter einmal jährlich nach Maßgabe der nachfolgenden Ziffern 11.2 bis 11.4 zu überprüfen, soweit nicht zusätzliche Kontrollen nach Anwendbarem Datenschutzrecht erforderlich sind. Solche Kontrollen beschränken sich auf die Informations- und Datenverarbeitungssysteme, die für die Erbringung des Angebots relevant sind.

11.2. Siemens und Unterauftragsverarbeiter können (interne oder externe) Auditoren beauftragen, Audits durchzuführen, um die Einhaltung der datenschutzrechtlichen Pflichten zu prüfen. In diesem Fall wird jeweils ein Prüfbericht („**Auditreport**“) erstellt. Auf Verlangen des Kunden stellt Siemens die entsprechenden Auditreports für die betroffenen Angebote zur Verfügung. Der Kunde stimmt zu, dass die Kontrollrechte des Kunden durch die übermittelten Auditreports erfüllt werden.

11.3. Soweit nach Anwendbarem Datenschutzrecht erforderlich, gewährt Siemens zusätzliche Kontrollen, insbesondere Vor-Ort-Kontrollen, in den Einrichtungen und Räumlichkeiten von Siemens durch den Kunden oder ein unabhängiges, akkreditiertes Drittunternehmen, während der regulären Geschäftszeiten und nach angemessener Vorankündigung gegenüber Siemens geprüft werden können. Die Kosten der Kontrollen nach diesem Absatz trägt der Kunde.

11.4. Alle Auditreports und im Rahmen eines Audits zur Verfügung gestellte Informationen und Dokumente sind vertrauliche Informationen von Siemens und dürfen nur an Weitere Verantwortliche weitergegeben werden, wenn der Kunde diesen Vertraulichkeitspflichten auferlegt, die den Vertraulichkeitspflichten der Vereinbarung entsprechen. Sofern sich Auditreports auf Unterauftragsverarbeiter beziehen, können die Auditreports gegebenenfalls nur zur Verfügung gestellt werden, wenn sich der Kunde und Weitere Verantwortliche direkt gegenüber dem Unterauftragsverarbeiter zur Vertraulichkeit verpflichtet.

12. **Single Point of Contact und Haftung**

12.1. Der Kunde dient als einziger Ansprechpartner für Siemens; auch in Bezug auf Weitere Verantwortliche im Rahmen der DPT.

12.2. Wenn und soweit die DPT oder eine der in Ziffer 7 genannten Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus (wie die EU-Standardvertragsklauseln) Verantwortlichen Rechte einräumt, verpflichtet sich der Kunde, diese Rechte im Namen und im Auftrag des jeweiligen Verantwortlichen gegenüber Siemens geltend zu machen, es sei denn eine direkte Geltendmachung durch den Verantwortlichen ist nach Anwendbarem Datenschutzrecht zwingend erforderlich Siemens und Unterauftragsverarbeiter sind berechtigt, direkt von Weiteren Verantwortlichen gestellte Anfragen, Anweisungen oder Ansprüche abzulehnen.

12.3. Wenn und soweit die DPT oder eine Maßnahme zur Sicherstellung eines Angemessenen Datenschutzniveaus Informationspflichten gegenüber weiteren Verantwortlichen vorsehen, gilt - vorbehaltlich entgegenstehender Bestimmungen des Anwendbaren Datenschutzrechts - die Information durch Siemens und Unterauftragsverarbeiter als erteilt, wenn dem Kunden die entsprechende Information mitgeteilt wird.

12.4. Unbeschadet gesetzlicher Rechte der Betroffenen Personen gelten die in der Vereinbarung enthaltenen Haftungsbeschränkungen auch für die (aggregierte) Haftung von Siemens und Unterauftragsverarbeitern gegenüber dem Kunden und Weiteren Verantwortlichen.

12.5. Der Kunde ist verpflichtet sicherzustellen, dass sich Siemens und Unterauftragsverarbeiter gegenüber Weiteren Verantwortlichen auf die Ziffern 12.1 bis 12.4 berufen können.

13. **Mitteilungen**

13.1. Für Mitteilungen nach den DPT finden die Regelungen der Vereinbarung Anwendung.

13.2. Siemens hat das Recht, den Einsatz von Unterauftragsverarbeiter nach Ziffer 6 wie folgt mitzuteilen: aktuelle Unterauftragsverarbeiter werden auf www.siemens.com/dpt veröffentlicht und Siemens stellt dem Kunden einen Mechanismus zur Verfügung, mit dem der Kunde über jeden neuen Unterauftragsverarbeiter informiert wird. Der Kunde ist verpflichtet, einen geeigneten Kontakt auf www.siemens.com/dpt zu registrieren und die angegebenen Kontaktinformationen aktuell zu halten.

14. **Laufzeit und Vertragsende**

Diese DPT haben dieselbe Laufzeit wie die Vereinbarung. Vorbehaltlich abweichender Vereinbarungen zwischen den Parteien, wird Siemens mit Beendigung dieser DPT alle Personenbezogenen Daten, welche Siemens von dem Kunden zur Verfügung gestellt wurden, oder welche im Zusammenhang mit der Erbringung des Angebots erhoben wurden, löschen.

SIEMENS

15. **Sprachen**

Soweit Siemens Übersetzungen der englischen Sprachversion der DPT oder der Exhibits anbietet, geht im Falle eines Widerspruchs, die englische Sprachversion der DPT oder der Exhibits vor.

16. **Länderspezifische Regelungen**

16.1. **Russische Föderation.** Soweit Siemens Personenbezogene Daten im Rahmen des Datenschutzgesetzes Nr. 152 FZ Verarbeitet, (i) ist der Kunde für die erstmalige Erhebung, Erfassung, Systematisierung, Speicherung, Aktualisierung, Änderung, Übermittlung, Extraktion und sonstige Verarbeitung (zusammenfassend „**Erstverarbeitung**“) dieser Personenbezogenen Daten verantwortlich; und (ii) versichert der Kunde hiermit, dass die Erstverarbeitung im Einklang mit den anwendbaren Gesetzen zur Verarbeitung und zum Schutz dieser Informationen erfolgt und (iii) holt der Kunde die Einwilligung der Betroffenen Person zur Übermittlung (einschließlich internationaler Übermittlung) und Verarbeitung ihrer Personenbezogenen Daten durch Siemens und Unterauftragsverarbeiter ein.

16.2. **USA.** Soweit Siemens Personenbezogene Daten von Einwohnern der USA Verarbeitet, gilt zusätzlich das Folgende: Siemens Verarbeitet Personenbezogene Daten im Auftrag des Kunden und wird die Personenbezogenen Daten nicht für andere als die in den DPT festgelegten und nach in den USA geltendem Datenschutzrecht („**US-Datenschutzrecht**“) zulässigen Zwecke speichern, nutzen oder offenlegen, auch nicht im Rahmen der Ausnahmeregelung zum "Verkauf" von Personenbezogenen Daten. Es erfolgt kein „Verkauf“ der Personenbezogenen Daten im Sinne des US-Datenschutzrechts. Durch diese Bestimmungen bleiben die datenschutzrechtlichen Pflichten von Siemens gegenüber dem Kunden gemäß dieser DPT, dieser Vereinbarung oder einer sonstigen Abrede zwischen Siemens und dem Kunden unberührt. Siemens bestätigt hiermit, dass Siemens die vorgenannten Beschränkungen anerkennt und einhält.

17. **Begriffsbestimmungen**

17.1. „**Anwendbares Datenschutzrecht**“ bezeichnet alle anwendbaren Gesetze, die sich auf die Verarbeitung Personenbezogener Daten nach dieser Vereinbarung beziehen.

17.2. „**Auftragsverarbeiter**” bezeichnet jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

17.3. „**BCR**“, „**Binding Corporate Rules for Processors**“ oder **„Verbindliche Interne Datenschutzvorschriften für Auftragsverarbeiter**“ bezeichnet verbindliche interne Datenschutzvorschriften für Auftragsverarbeiter, die im Sinne von Artikel 47 Verordnung (EU) 2016/679 (Datenschutzgrundverordnung) genehmigt wurden.

17.4. „**Besondere Kategorien Personenbezogener Daten“** sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

17.5. „**Betroffene Person**“ bezeichnet eine identifizierte oder identifizierbare natürliche Person.

17.6. „**Data Privacy Terms**“ oder „**DPT**“ bezeichnen diese Vertragsklauseln zur Auftragsverarbeitung.

17.7. „**DPT Exhibits**“ bezeichnet sämtliche Vertragsunterlagen, die den Umfang, die Art und den Zweck der Verarbeitung, die Arten der Verarbeiteten Personenbezogenen Daten, die Kategorien der betroffenen Personen, die eingesetzten Unterauftragsverarbeiter und die technischen und organisatorischen Maßnahmen beschreiben sowie auf die in dieser Vereinbarung und/oder diesen DPT verwiesen wird.

17.8. „**EU-Standardvertragsklauseln**” bezeichnen die Standardvertragsklauseln für die Übermittlung Personenbezogener Daten an Auftragsverarbeiter in Drittländern gemäß Kommissionsentscheidung 2010/87/EU vom 5. Februar 2010 oder entsprechende Nachfolgeentscheidungen der EU-Kommission. Die zum Zeitpunkt des Inkrafttretens dieser Vereinbarung gültigen Standardvertragsklauseln sind als Annex diesen DPT beigefügt.

17.9. „**EWR**“ bezeichnet den Europäischen Wirtschaftsraum.

17.10. „**Land mit Angemessenheitsbeschluss vorliegt**“ bezeichnet ein Land außerhalb des EWR, für das die Europäische Kommission entschieden hat, dass das Land ein angemessenes Schutzniveau in Bezug auf Personenbezogene Daten gewährleistet.

17.11. **„Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus**“ bezeichnet (i) einen Angemessenheitsbeschluss der Europäischen Kommission oder (ii) angemessene Garantien im Sinne von Artikel 46 der Datenschutzgrundverordnung (EU) 2016/679.

17.12. „**Personenbezogene Daten“** sind Informationen, sich auf eine identifizierte oder identifizierbare Person Betroffene Person beziehen, insbesondere Namen, E-Mail-Adressen, Postanschriften, Kennnummer, Standortdaten, Online-Kennung oder ein oder mehrere besondere Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Personenbezogene Daten im Sinne der DPT sind nur solche Personenbezogenen Daten, die vom Kunden oder Weiteren Verantwortlichen in das Angebot eingegeben werden oder auf die Siemens im Zusammenhang mit der Erbringung des Angebots zugreift.

17.13. „**Übermittlung an Auftragsverarbeiter außerhalb des EWR**“ bezeichnet (i) die Verarbeitung Personenbezogener Daten außerhalb des EWR oder außerhalb eines Landes mit Angemessenheitsbeschluss, oder (ii) Zugriff auf Personenbezogene Daten durch Siemens oder einen Unterauftragsverarbeiter von außerhalb des EWR oder von außerhalb eines Landes mit Angemessenheitsbeschluss.

17.14. „**Unterauftragsverarbeiter**” bezeichnet jeden weiteren Auftragsverarbeiter, welcher durch Siemens zur Erbringung des Angebots beauftragt wird und Zugang zu Personenbezogenen Daten hat.

17.15. „**Verantwortlicher**" bezeichnet jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Personenbezogenen Daten entscheiden.

17.16. „**Verarbeiten**" oder „**Verarbeitung**" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten wie Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten oder eine andere Form von Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung.

17.17. „**Vereinbarung**" bezeichnet den kommerziellen Vertrag über die Erbringung der des Angebots zwischen Siemens und dem Kunden.

17.18. „**Verletzung des Schutzes Personenbezogener Daten**" bezeichnet eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von, beziehungsweise zum, unbefugten Zugang zu Personenbezogenen Daten führt, die im Rahmen dieser DPT Verarbeitet werden.

17.19. „**Angebot"** bezeichnet die von Siemens im Rahmen der Vereinbarung erbrachten Auftragsverarbeitungstätigkeiten. In der Vereinbarung wird das Angebot teilweise als „Leistung", „Service-Leistungen" oder ähnlich definiert.

17.20. „**Weitere Verantwortliche**" bezeichnet sämtliche Dritte (z.B. verbundene Unternehmen des Kunden), welche nach dieser Vereinbarung zum Empfang des Angebots berechtigt sind.

DPT Exhibits – Beschreibung der Auftragsverarbeitungsmaßnahmen

Diese Anlage spezifiziert den Gegenstand der Verarbeitung, die Art und den Zweck der Verarbeitung, die Art der Personenbezogenen Daten und die Kategorien der Betroffenen Personen. Die Parteien können weitere Einzelheiten in dieser Vereinbarung regeln, wenn und soweit dies für einen bestimmte Vertragsgegenständliche Leistung erforderlich ist.

Gegenstand, Art und Zweck der Verarbeitung

Siemens und Unterauftragsverarbeiter Verarbeiten Personenbezogene Daten, um das Angebot zu erbringen, einschließlich:

- über das Internet zugängliche oder ähnliche Dienste, die von Siemens bereitgestellt und gehostet werden ("**Cloud-Dienste**"); oder
- Administrations-, Management-, Installations-, Konfigurations-, Migrations-, Wartungs- und Supportleistungen oder sonstige Leistungen, die einen (Fern-)Zugriff auf die in den Cloud Services oder auf den IT-Systemen des Kunden gespeicherten Personenbezogenen Daten erfordern ("**Support-Leistungen**").

Betroffene Personen

Die Verarbeiteten Personenbezogenen Daten betreffen die folgenden Kategorien Betroffener Personen:

- Arbeitnehmer;
- Vertragspartner;
- Lieferanten;
- Geschäftspartner; und
- andere Personen, deren Personenbezogene Daten im Rahmen des Angebots gespeichert und/oder im Zusammenhang mit der Bereitstellung des Angebots Verarbeitet werden.

Kategorien von Daten

Die Verarbeiteten Personenbezogenen Daten betreffen folgende Datenkategorien:

- Kontakt- und Benutzerinformationen, insbesondere Name, Telefonnummer, E-Mail-Adresse, Zeitzone und Adressdaten;
- Systemzugriffs-, Nutzungs-, Autorisierungs- und Betriebsdaten sowie Systemprotokolldateien, die Personenbezogene Daten oder andere anwendungsspezifische Daten enthalten, die Benutzer im Rahmen des Angebots hochladen; und
- ggf. weitere Personenbezogene Daten, die der Kunde und Weitere Verantwortliche durch das Hochladen oder Verbinden mit dem Angebot oder in sonstiger Weise im Zusammenhang mit dem Angebot zur Verfügung stellen.

Besondere Datenkategorien (falls zutreffend)

Das Angebot sind nicht für die Verarbeitung Besonderer Kategorien Personenbezogener Daten bestimmt und der Kunde sowie Weitere Verantwortliche übermitteln weder direkt noch indirekt solche sensiblen Personenbezogenen Daten an Siemens.

DPT Exhibits – Liste genehmigter Unterauftragsverarbeiter

Ein Verzeichnis der von uns bei der Erbringung des Angebots eingesetzten Unterauftragsverarbeiter ist unter www.siemens.com/DPT abrufbar oder in der jeweiligen Vereinbarung enthalten.

DPT Exhibits – Technische und organisatorische Maßnahmen

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen (TOMs), die von Siemens und Unterauftragsverarbeitern zum Schutz ihrer IT-Systeme und Anlagen umgesetzt werden. Einige Angebote können durch andere oder zusätzliche TOMs geschützt sein, die in der jeweiligen Vereinbarung festgelegt sind.

Szenario 1: TOMs, die für Cloud-Dienste gelten.

Szenario 2: TOMs, die für Support-Leistungen gelten, welche über von Siemens bereitgestellte und kontrollierte Fernzugriffstools erbracht werden.

Szenario 3: TOMs, die für Support-Leistungen gelten, welche über vom Kunden bereitgestellte und kontrollierte Fernzugriffstools erbracht werden.

#	Maßnahmen	Szenario		
		1	2	3
1.	Physische Sicherheitsmaßnahmen und Zutrittskontrollen			
	Siemens trifft geeignete Maßnahmen, um zu verhindern, dass Unbefugte Zugriff auf die Datenverarbeitungsanlagen (namentlich Datenbank- und Applikationsserver sowie zugehörige Hardware) erhalten. Dazu werden die folgenden Maßnahmen ergriffen:			
	a) Einrichtung von Sicherheitsbereichen;	X	X	-
	b) Sicherung und Einschränkung der Zugangswege;	X	X	-
	c) Sicherung der dezentralen Datenverarbeitungsanlagen und Personalcomputer;	X	X	X
	d) Festlegung von Zugriffsberechtigungen für Mitarbeiter und Dritte, einschließlich der entsprechenden Dokumentation;	X	X	-
	e) Protokollierung, Überwachung und Nachverfolgung aller Zugriffe auf das Rechenzentrum, in dem Personenbezogene Daten gehostet werden;	X	-	-
	f) Sicherung des Rechenzentrums, in dem Personenbezogene Daten gehostet werden, durch Zugangskontrollen und andere geeignete Sicherheitsmaßnahmen; und	X	-	-
	g) Wartung und Inspektion in IT-Bereichen und Rechenzentren nur durch autorisiertes Personal	X	X	-
2.	Zugriffskontrolle (IT-Systeme und/oder IT-Anwendungen)			
	2.1 Siemens implementiert ein Autorisierungs- und Authentifizierungs-Framework, das unter anderem die folgenden Elemente umfasst:			
	a) Rollenbasierte Zugriffskontrollen;	X	X	X
	b) Verfahren zum Erstellen, Ändern und Löschen von Accounts;	X	X	X
	c) Schutz des Zugriffs auf IT-Systeme und IT-Anwendungen durch Authentifizierungsmechanismen;	X	X	X
	d) Nutzung geeigneter Authentifizierungsmethoden, basierend auf den Eigenschaften und technischen Möglichkeiten des IT-Systems oder der IT-Anwendung;	X	X	X

#	Maßnahmen	Szenario		
		1	2	3
	e) Erfordernis einer angemessenen Authentifizierung für den Zugang zu IT-Systemen und IT-Anwendungen;	X	X	X
	f) Protokollierung sämtlicher Zugriffe auf Daten (insbesondere Personenbezogener Daten);	X	X	-
	g) Autorisierungs- und Protokollierungsmaßnahmen für ein- und ausgehende Netzwerkverbindungen zu IT-Systemen und IT-Anwendungen (insbesondere Firewalls zum Zulassen oder Verweigern eingehender Netzwerkverbindungen);	X	X	-
	h) Vergabe privilegierter Zugriffsrechte auf IT-Systeme, IT-Anwendungen und Netzwerkdienste nur an Personen, die diese zur Erfüllung ihrer Aufgaben benötigen (Least-Privilege-Prinzip)	X	X	X
	i) Dokumentation und laufende Aktualisierung der privilegierten Zugriffsrechte auf IT-Systeme und IT-Anwendungen;	X	X	X
	j) Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte auf IT-Systeme und -Anwendungen;	X	X	X
	k) Passwort-Policy mit Anforderungen an die Komplexität von Passwörtern, Mindestlänge und Ablauf nach angemessener Zeit, sowie keiner Wiederverwendung von kürzlich verwendeten Passwörtern;	X	X	X
	l) Technische Durchsetzung der Passwort-Policy durch IT-Systeme und IT-Anwendungen;	X	X	X
	m) Richtlinie zum Sperren des Benutzerterminals beim Verlassen des Arbeitsplatzes;	X	X	X
	n) Automatisches Time-Out des Benutzerterminals bei Nichtbenutzung;	X	X	X
	o) automatisches Sperren der Benutzeridentifikation bei mehrfacher Falscheingabe von Passwörtern mit Protokollierung der Ereignisse (Überwachung von Zugriffsversuchen);	X	X	X
	p) Entzug der Zugriffsrechte von Mitarbeitern und externem Personal auf IT-Systeme und IT-Anwendungen bei Beendigung des Arbeitsverhältnisses oder des Vertrages; und	X	X	X
	q) Verwendung von sicheren, dem Stand der Technik entsprechenden Authentifizierungszertifikaten.	X	X	-
	2.2 Siemens implementiert ein Rollen- und Berechtigungskonzept.	X	X	-
	2.3 IT-Systeme und IT-Anwendungen sperren sich automatisch oder beenden die Sitzung nach Überschreiten einer zuvor definierten, angemessenen Leerlaufzeit.	X	X	-
	2.4 Siemens unterhält Anmeldeverfahren an IT-Systemen mit Schutzmaßnahmen gegen verdächtige Anmeldeaktivitäten (z. B. gegen Brute-Force- und Password-Guessing-Angriffe).	X	X	X
3.	Verfügbarkeitskontrolle			
	3.1 Siemens definiert, dokumentiert und implementiert ein Datensicherungskonzept für IT-Systeme, das die folgenden technischen und organisatorischen Elemente umfasst:			
	a) Schutz der Backup-Speichermedien vor unberechtigtem Zugriff und vor Umweltbedrohungen (z. B. Hitze, Feuchtigkeit, Feuer);	X	-	-
	b) vordefinierte Backup-Intervalle; und	X	-	-

#	Maßnahmen	Szenario		
		1	2	3
	c) regelmäßiges Testen der Wiederherstellung von Daten aus Backups entsprechend der Sensibilität des IT-Systems oder der IT-Anwendung.	X	-	-
	3.2 Siemens speichert Backups an einem anderen physischen Ort als dem Ort, an dem das laufende System gehostet wird.	X	-	-
	3.3 Siemens implementiert geeigneter und dem Stand der Technik entsprechender Anti-Malware-Lösungen zum Schutz der Systeme und Anwendungen vor Schadsoftware.	X	X	X
	3.4 IT-Systeme und IT-Anwendungen in Nicht-Produktionsumgebungen sind logisch oder physikalisch von IT-Systemen und IT-Anwendungen in Produktionsumgebungen getrennt.	X	-	-
	3.5 Rechenzentren, in denen Personenbezogene Daten gespeichert oder Verarbeitet werden, sind gegen Naturkatastrophen, physische Angriffe und Unfälle geschützt.	X	-	-
	3.6 Unterstützende Einrichtungen in IT-Bereichen und Rechenzentren, wie z. B. Kabel, Strom, Telekommunikationseinrichtungen, Wasserversorgung oder Klimaanlagen, sind vor Störungen und unbefugter Manipulation geschützt.	X	-	-
4.	Betriebssicherheit			
	4.1 Siemens unterhält und implementiert ein unternehmensweites ISO 27001 Information Security Framework, das regelmäßig überprüft und aktualisiert wird.	X	X	X
	4.2 Siemens protokolliert sicherheitsrelevante Ereignisse, wie z.B. Aktivitäten der Benutzerverwaltung (z.B. Anlegen, Löschen), fehlgeschlagene Anmeldungen, Änderungen an der Sicherheitskonfiguration des Systems auf IT-Systemen und IT-Applikationen.	X	X	X
	4.3 Siemens analysiert kontinuierlich die jeweiligen Protokolldaten der IT-Systeme und IT-Applikationen auf Anomalien, Unregelmäßigkeiten, Hinweise auf Kompromittierung und andere verdächtige Aktivitäten.	X	X	X
	4.4 Siemens scannt und testet IT-Systeme und IT-Anwendungen regelmäßig auf Sicherheitslücken.	X	X	X
	4.5 Siemens implementiert und unterhält einen Change-Management-Prozess für IT-Systeme und IT-Applikationen.	X	X	X
	4.6 Siemens unterhält einen Prozess zur Aktualisierung und Implementierung von Security Fixes und Updates der Hersteller auf den jeweiligen IT-Systemen und IT-Applikationen.	X	X	X
	4.7 Siemens löscht Daten unwiederbringlich oder vernichtet die Datenträger physisch, bevor ein IT-System entsorgt oder wiederverwendet wird.	X	X	X
5.	Übertragungssteuerung			
	5.1 Siemens überwacht kontinuierlich und systematisch IT-Systeme, IT-Anwendungen und relevante Netzwerkzonen, um bösartige und abnormale Netzwerkaktivitäten zu erkennen, durch:			
	a) Firewalls (z.B. Stateful Firewalls, Application Firewalls);	X	X	-
	b) Proxy-Server;	X	X	-
	c) Intrusion Detection Systems (IDS) und/oder Intrusion Prevention Systems (IPS);	X	X	-
	d) UR-Filterung; und	X	-	-
	e) Security Information and Event Management (SIEM) Systeme.	X	X	-

#	Maßnahmen	Szenario		
		1	2	3
	5.2 Siemens dokumentiert und aktualisiert regelmäßig die Netzwerktopologien und deren Sicherheitsanforderungen.	X	X	-
	5.3 Siemens verwaltet IT-Systeme und IT-Anwendungen unter Verwendung von verschlüsselten Verbindungen, die dem Stand der Technik entsprechen.	X	X	-
	5.4 Siemens schützt die Integrität von Inhalten bei der Übertragung durch modernste Netzwerkprotokolle, wie z.B. TLS.	X	X	-
	5.5 Siemens verschlüsselt oder ermöglicht seinen Kunden die Verschlüsselung von Kundendaten, die über öffentliche Netze übertragen werden.	X	X	-
	5.6 Siemens nutzt sichere Key Management Systeme (KMS) zur Speicherung von geheimen Schlüsseln in der Cloud.	X	-	-
6.	Sicherheitstechnische Vorfälle			
	Siemens unterhält und implementiert einen Prozess zur Behandlung von sicherheitstechnischen Vorfällen, der unter anderem Folgendes umfasst:			
	a) Aufzeichnungen über Sicherheitsverstöße;	X	X	X
	b) Prozesse zur Benachrichtigung von Kunden; und	X	X	X
	c) ein Konzept für die Reaktion auf einen Vorfall, das Folgendes zum Zeitpunkt des Vorfalls regelt: (i) Rollen, Verantwortlichkeiten sowie Kommunikations- und Kontaktstrategien im Falle einer Kompromittierung, (ii) spezifische Verfahren für die Reaktion auf den Vorfall und (iii) die Absicherung und Behandlung aller kritischen Systemkomponenten.	X	X	X
7.	Asset Management, Systembeschaffung, Entwicklung und Wartung			
	7.1 Siemens implementiert einen angemessenen Security-Patching-Prozess, der Folgendes umfasst:			
	a) Überprüfung der Komponenten auf mögliche Schwachstellen (CVEs);	X	X	-
	b) Prioritätseinstufung der Fehlerbehebungen;	X	X	-
	c) rechtzeitige Implementierung des Fixes; und	X	X	-
	d) das Herunterladen von Patches aus vertrauenswürdigen Quellen.	X	X	-
	7.2 Siemens identifiziert und dokumentiert die Anforderungen an die Informationssicherheit vor der Entwicklung und Beschaffung neuer IT-Systeme und IT-Anwendungen sowie vor Verbesserungen an bestehenden IT-Systemen und IT-Anwendungen.	X	X	-
	7.3 Siemens implementiert einen formalen Prozess zur Kontrolle und Durchführung von Änderungen an entwickelten Anwendungen.	X	X	-
	7.4 Siemens konzipiert und integriert Sicherheitstests in den System Development Life Cycle von IT-Systemen und IT-Anwendungen.	X	X	-
8.	Personalsicherheit			

#	Maßnahmen	Szenario		
		1	2	3
	8.1 Siemens setzt im Bereich der Personalsicherheit folgende Maßnahmen um:			
	a) Verpflichtung von Mitarbeitern mit Zugang zu Personenbezogenen Daten zur Vertraulichkeit; und	X	X	X
	b) Regelmäßige Schulung von Mitarbeitern mit Zugang zu Personenbezogenen Daten hinsichtlich anwendbarer Datenschutzgesetze und -vorschriften.	X	X	X
	8.2 Siemens implementiert einen Offboarding-Prozess für Siemens-Mitarbeiter und externe Lieferanten.	X	X	X

DPT Exhibits – Übersicht zur DSGVO

In der folgenden Tabelle sind zur Veranschaulichung die relevanten Artikel der DSGVO und die entsprechenden Bestimmungen der DPT aufgeführt.

#	Norm der DSGVO	Ziffer der DPT	Titel
1.	Artikel 28 (1)	Ziffer 4 und DPT Exhibits	Technische und organisatorische Maßnahmen und DPT Exhibits - Technische und organisatorische Maßnahmen
2.	Artikel 28 (2), (3) (d) und (4)	Ziffer 6	Unterauftragsverarbeiter
3.	Artikel 28 (3) Satz 1	Ziffer 2 und DPT Exhibits	Beschreibung der Datenverarbeitung und DPT Exhibits – Beschreibung der Auftragsverarbeitungsmaßnahmen
4.	Artikel 28 (3) (a) und 29	Ziffer 3	Weisungen
5.	Artikel 28 (3) (b)	Ziffer 5	Vertraulichkeit der Verarbeitung
6.	Artikel 28 (3) (c) and 32	Ziffer 4 und DPT Exhibits	Technische und organisatorische Maßnahmen und DPT Exhibits - Technische und organisatorische Maßnahmen
7.	Artikel 28 (3) (e)	Ziffer 10.1	Rechte Betroffener Personen
8.	Artikel 28 (3) (f) and 32	Ziffer 10.2, Ziffer 4 und DPT Exhibits	Weitere Unterstützungsleistungen durch Siemens, Technische und organisatorische Maßnahmen und DPT Exhibits - Technische und organisatorische Maßnahmen
9.	Artikel 28 (3) (f) und 33 bis 34	Ziffer 9	Verletzung des Schutzes Personenbezogener Daten
10.	Artikel 28 (3) (f) und 35 bis 36	Ziffer 10.2	Weitere Unterstützungsleistungen durch Siemens
11.	Artikel 28 (3) (g)	Ziffer 14	Laufzeit und Vertragsende
12.	Artikel 28 (3) (h)	Ziffer 11	Kontrollrechte
13.	Artikel 46 (1) (b) und (c)	Ziffer 7 und EU Standardvertragsklauseln	Auftragsverarbeiter außerhalb des EWR und Annex – EU-Standardvertragsklauseln

Annex – EU-Standardvertragsklauseln

gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

Klausel 1
Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten“, „besondere Kategorien personenbezogener Daten“, „Verarbeitung“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“ und „Kontrollstelle“ entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (1);

b) der „Datenexporteur“ ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der „Datenimporteur“ ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der „Unterauftragsverarbeiter“ ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff „anwendbares Datenschutzrecht“ bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen“ sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2
Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3
Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4
Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs (2)

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii) jeden zufälligen oder unberechtigten Zugang und

   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7

Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder

b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8

Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

Klausel 10

Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11

Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss (3). Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine

solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: …

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen