SIEMENS

Data Privacy Agreement

November 2025

Dieser Vertrag zur Auftragsverarbeitung („**Data Privacy Agreement**“ oder „**DPA**“) wird zwischen der in der Vereinbarung genannten Siemens Gesellschaft („**Siemens**") und dem in der Vereinbarung genannten Kunden ("**Kunde**") geschlossen.

1. Anwendungsbereich und Einhaltung Anwendbaren Datenschutzrechts

1.1. Dieses DPA regeln die Verarbeitung Personenbezogener Daten im Rahmen der Erbringung der vereinbarten Leistungen durch Siemens, soweit Siemens als Auftragsverarbeiter des Kunden tätig wird. In den Vereinbarungen werden die vereinbarten Leistungen teilweise als „Leistung“, „Service-Leistung“ oder ähnlich definiert. Das DPA ist Bestandteil der jeweiligen Vereinbarung. Im Falle von Widersprüchen, geht die DPA Annexes dem DPA vor, das DPA hat Vorrang vor den Regelungen der Vereinbarung.

1.2. Das DPA regeln die datenschutzrelevanten Rechte und Pflichten des Kunden und Siemens im Rahmen der Erbringung der vereinbarten Leistungen 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 der vereinbarten Leistungen 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 anwendbar sind und nicht allgemein für Auftragsverarbeiter gelten. Der Kunde ist verpflichtet, alle für die Nutzung der vereinbarten Leistungen durch den Kunden geltenden rechtlichen Anforderungen, insbesondere das Anwendbare Datenschutzrecht, einzuhalten und sicherzustellen, dass Siemens und Unterauftragsverarbeiter die vereinbarten Leistungen gemäß dieses DPA 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 DPA Annexes enthalten.

3. Weisungen

Siemens verarbeitet Personenbezogene Daten ausschließlich entsprechend der dokumentierten Weisungen des Kunden. Die Parteien sind einig, dass die Vereinbarung (einschließlich dieses DPA) 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 DPA Annexes 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 DPA Annexes 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 der vereinbarten Leistungen 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 dieses DPA 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 DPA Annexes 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 der vereinbarten Leistungen vorschlagen, die eine Inanspruchnahme der vereinbarten Leistungen 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 der vereinbarten Leistungen 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 der vereinbarten Leistungen 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 diesem DPA für Siemens gelten. Siemens ist für Handlungen und Unterlassungen der eingesetzten Unterauftragsverarbeiter in gleicher Weise wie für eigene Handlungen und Unterlassungen verantwortlich.

7. Internationale Datentransfers

7.1. Drittlandtransfers. Betrifft ein Drittlandtransfer Personenbezogene Daten eines Verantwortlichen mit Sitz im EWR, der Schweiz oder des Vereinigten Königreichs, ist Siemens verpflichtet, die in den DPA Annexes bezeichneten Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus umzusetzen. Siemens ist berechtigt, die in den DPA Annexes bezeichneten Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus durch alternative Maßnahmen zu ersetzen. In diesem Fall gilt der Mitteilungs- und Zustimmungsmechanismus in Ziffer 6.2 entsprechend.

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

(i) Option 1 - Sitz von Siemens innerhalb des EWR. Hat die Siemens-Gesellschaft, mit der das DPA abgeschlossen wird, ihren Sitz innerhalb des EWR und innerhalb eines Landes mit Angemessenheitsbeschluss, findet diese Option 1 Anwendung und Siemens schließt Modul 3 der Standardvertragsklauseln EU und die relevanten Bestimmungen der Standardvertragsklauseln UK mit Unterauftragsverarbeitern ab. Siemens hat dabei sicherzustellen, dass die durch den Unterauftragsverarbeiter erbrachten Verarbeitungstätigkeiten durch die Standardvertragsklauseln erfasst werden.

(ii) Option 2 - Sitz von Siemens außerhalb des EWR. Hat die Siemens-Gesellschaft, mit der das DPA abgeschlossen wird, ihren Sitz außerhalb des EWR und außerhalb eines Landes mit Angemessenheitsbeschluss, findet diese Option 2 Anwendung und Siemens und der Kunde schließen hiermit Modul 2 und, wenn der Kunde selbst Auftragsverarbeiter für Weitere Verantwortliche ist, Modul 3 der Standardvertragsklauseln EU und die Standardvertragsklauseln UK ab. Zu diesem Zweck vereinbaren die Partien hiermit die Geltung der unter www.siemens.com/DPT/SCC abrufbaren Standardvertragsklauseln. Die DPA Annexes „DPA Annex - Beschreibung der Auftragsverarbeitungsmaßnahmen“, „DPA Annex - Technische und organisatorische Maßnahmen“ und „DPA Annex – Liste genehmigter Unterauftragsverarbeiter“ werden als Anhänge 1 bis 3 Bestandteil der Standardvertragsklauseln. 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 unter den Standardvertragsklauseln.

(iii) Schweiz. Unterliegt ein Drittlandtransfer dem Anwendbaren Datenschutzrecht der Schweiz und werden die Standardvertragsklauseln verwendet, ist jeder Verweis in den Standardvertragsklauseln EU auf die EU-Datenschutzgrundverordnung (EU) 2016/679 als Verweis auf das Anwendbare Datenschutzrecht in der Schweiz und Verweise auf die zuständige Aufsichtsbehörde als Verweise auf den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten zu verstehen. Die Parteien vereinbaren zudem, dass das anwendbare Recht für Zwecke von Klausel 17 der Standardvertragsklauseln das Recht der Schweiz ist. Für in der Schweiz ansässige betroffene Personen sind die Gerichte der Schweiz ein alternativer Gerichtsstand für Streitigkeiten.

7.3. BCR. 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 dieses DPA einzuhalten.

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, verpflichtet sich Siemens im Rahmen des zumutbaren verfügbare Rechtsmittel gegen das Verbot zu erheben, um so viele Informationen wie möglich zeitnah an den Kunden herausgeben zu können und (iii) im Rahmen des zumutbaren 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 und soweit der Betroffene hinreichend Angaben zur Identifizierung des Kunden macht, 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 unterstützen, 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 der jeweiligen Leistung 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.

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 oder nach einer Verletzung des Schutzes Personenbezogener Daten 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 der jeweiligen Leistung relevant sind.

11.2. Siemens ist berechtigt den Nachweis über die Einhaltung der Verpflichtungen aus dem DPA durch Vorlage (i) einschlägiger ISO 27001 Zertifizierungen oder vergleichbarer Standards oder (ii) anderer Zertifikate und Nachweise zur Einhaltung ("Zertifikate und Nachweise") erbringen. Der Kunde stimmt zu, dass die Kontrollrechte des Kunden durch die übermittelten Zertifikate und Nachweise erfüllt werden.

11.3. Soweit nach Anwendbarem Datenschutzrecht erforderlich, ermöglicht Siemens in angemessenem Umfang 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 geprüft werden können.

11.4. Alle Zertifikate und Nachweise 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 Zertifikate und Nachweise auf Unterauftragsverarbeiter beziehen, können die Zertifikate und Nachweise gegebenenfalls nur zur Verfügung gestellt werden, wenn sich der Kunde und Weitere Verantwortliche direkt gegenüber dem Unterauftragsverarbeiter zur Vertraulichkeit verpflichtet.

12. **Mitteilungen**

Für Mitteilungen nach dem DPA finden die Regelungen der Vereinbarung Anwendung.

13. **Laufzeit und Vertragsende**

Dieses DPA hat dieselbe Laufzeit wie die jeweilige Vereinbarung. Vorbehaltlich abweichender Vereinbarungen zwischen den Parteien, wird Siemens mit Beendigung dieses DPA alle Personenbezogenen Daten, welche Siemens von dem Kunden zur Verfügung gestellt wurden, oder welche im Zusammenhang mit der Erbringung der jeweiligen Leistung erhoben wurden, löschen.

14. **Sprachen**

Soweit Siemens Übersetzungen der englischen Sprachversion des DPA oder der DPA Annexes anbietet, geht im Falle eines Widerspruchs, die englische Sprachversion des DPA oder der DPA Annexes vor.

15. **Länderspezifische Regelungen**

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 der Vereinbarung oder dem DPA festgelegten und nach in den USA geltendem Datenschutzrecht („**US-Datenschutzrecht**“) zulässigen Zwecke speichern, nutzen oder offenlegen. Es erfolgt kein „Verkauf“ oder „Teilen“ der Personenbezogenen Daten im Sinne des US-Datenschutzrechts. Siemens wird personenbezogenen Daten nicht mit von Dritten zur Verfügung gestellten personenbezogenen Daten oder mit personenbezogenen Daten, die Siemens im Rahmen der eigenen Interaktion mit der betroffenen Person erhoben hat kombinieren, es sei denn, dies ist nach dem US-Datenschutzrecht oder der Vereinbarung gestattet. Durch diese Bestimmungen bleiben die datenschutzrechtlichen Pflichten von Siemens gegenüber dem Kunden gemäß dieses DPA, dieser Vereinbarung oder einer sonstigen Abrede zwischen Siemens und dem Kunden unberührt.

16. **Begriffsbestimmungen**

16.1. „**Vereinbarte Leistung(en)“** bezeichnet die von Siemens im Rahmen der jeweiligen Vereinbarung erbrachten Auftragsverarbeitungstätigkeiten. In der jeweiligen Vereinbarung wird die jeweilige Leistung teilweise als „Leistung“, „Service“ oder ähnlich definiert.

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

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

16.4. „**BCR**“, „**Binding Corporate Rules for Processors**“ oder **„Verbindliche Interne Datenschutzvorschriften für Auftragsverarbeiter**“ bezeichnet verbindliche interne

Datenschutzvorschriften für Auftragsverarbeiter, die durch die zuständigen Aufsichtsbehörden (i) in der Europäischen Union und (ii) im Vereinigten Königreich genehmigt wurden.

16.5. „**Besondere Kategorien Personenbezogener Daten“ oder „Sensible Personenbezogene 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.

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

16.7. „**Data Privacy Agreement**“ oder „**DPA**“ bezeichnen diese Vertragsklauseln zur Auftragsverarbeitung.

16.8. „**DPA Annexes**“ 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 diesem DPA verwiesen wird. Im Anwendungsbereich der Standardvertragsklauseln gelten die DPA Annexes als Anlagen I bis III der Standardvertragsklauseln und werden hiermit durch Bezugnahme zum Bestandteil der Standardvertragsklauseln.

16.9. „**Drittlandtransfer**“ 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.

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

16.11. „**Land mit Angemessenheitsbeschluss**“ bezeichnet ein Land, für das die Europäische Kommission entschieden hat, dass das Land ein angemessenes Schutzniveau in Bezug auf Personenbezogene Daten gewährleistet und für Personenbezogene Daten aus dem Vereinigten Königreich, ein Land, für das eine Angemessenheitsbeschluss im Vereinigten Königreich getroffen wurde.

16.12. **„Maßnahme(n) zur Sicherstellung eines angemessenen Datenschutzniveaus**“ bezeichnet die nach Anwendbarem Datenschutzrecht erforderlichen angemessene Garantien zum Schutz von Drittlandtransfers, wie Maßnahmen im Sinne von Artikel 46 der Datenschutzgrundverordnung (EU) 2016/679.

16.13. „**Personenbezogene Daten“** sind Informationen, die 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 Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Personenbezogene Daten im Sinne des DPA sind nur solche Personenbezogenen Daten, die vom Kunden oder Weiteren Verantwortlichen in die jeweilige Leistung eingegeben werden oder auf die Siemens im Zusammenhang mit der Erbringung der jeweiligen Leistung zugreift.

16.14. „**Standardvertragsklauseln**” bezeichnen die Standardvertragsklauseln EU und, bzgl. Personenbezogener Daten, die von Verantwortlichen aus dem Vereinigten Königreich stammen, die Standardvertragsklauseln UK.

16.15. „**Standardvertragsklauseln EU**” bezeichnen die Standardvertragsklauseln (EU) 2021/914.

16.16. „**Standardvertragsklauseln UK**” bezeichnen die Standarddatenschutzklauseln, die vom UK Information Commissioner Office nach dem Anwendbaren Datenschutzrecht im Vereinigten Königreich verabschiedet werden, einschließlich des International Data Transfer Agreements und der Standardvertragsklauseln EU erweitert um das UK International Data Transfer Addendum.

16.17. „**Unterauftragsverarbeiter**” bezeichnet jeden weiteren Auftragsverarbeiter, welcher durch Siemens zur Erbringung der jeweiligen Leistung beauftragt wird und Zugang zu Personenbezogenen Daten hat.

16.18. „**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.

16.19. „**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.

16.20. „**Vereinbarung**” bezeichnet den kommerziellen Vertrag über die Erbringung der jeweiligen Leistung zwischen Siemens und dem Kunden.

16.21. „**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 dieses DPA verarbeitet werden.

16.22. „**Weitere Verantwortliche**” bezeichnet sämtliche Dritte (z.B. verbundene Unternehmen des Kunden), welche nach der Vereinbarung zum Empfang der jeweiligen Leistung berechtigt sind.

Annex I zu dem DPA (und, soweit anwendbar, Anlage I zu den EU-Standardvertragsklausel)

Beschreibung der Auftragsverarbeitungsmaßnahmen

Diese Anlage spezifiziert den Gegenstand der Verarbeitung (einschließlich Art und den Zweck der Verarbeitung, Art der Personenbezogenen Daten und Kategorien der Betroffenen Personen). Die Parteien können weitere Einzelheiten in der Vereinbarung regeln, einschließlich in der unter https://www.hacon.de/record-of-processing abrufbaren Übersicht der produktspezifisch verarbeiteten personenbezogenen Daten.

A. LISTE DER PARTEIEN

Kunde (und, soweit die EU-Standardvertragsklauseln Anwendung finden, Datenexporteur):

Name, Anschrift, Funktion und Kontaktdaten der Kontaktperson: Name und Anschrift sowie Funktion und Kontaktdatensind in der Vereinbarung angegeben oder werden beim Aufsetzen der jeweiligen Leistung erhoben.

Rolle (Verantwortlicher/Auftragsverarbeiter): Der Kunde agiert als (i) Verantwortlicher für Verarbeitungstätigkeiten, die durch Siemens gegenüber dem Kunden erbracht werden und (ii) als Auftragsverarbeiter gemäß den Weisungen seiner Weiteren Verantwortlichen, für Verarbeitungstätigkeiten, die durch Siemens gegenüber Weiteren Verantwortlichen erbracht werden.

Dienstleister (und, soweit die EU-Standardvertragsklauseln Anwendung finden, Datenimporteur):

Name, Anschrift, Funktion und Kontaktdaten der Kontaktperson: Der Dienstleister / Datenimporteur ist die in der Vereinbarung angegebene Siemens Gesellschaft. Kontakt für Datenschutzanfragen privacy@hacon.de

Rolle (Verantwortlicher/Auftragsverarbeiter): Siemens agiert als Auftragsverarbeiter und verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Kunden und im Auftrag Weiterer Verantwortlicher.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren Personenbezogene Daten übermittelt/Verarbeitet werden

Die Verarbeiteten Personenbezogenen Daten betreffen die folgenden Kategorien Betroffener Personen:

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

Kategorien der übermittelten personenbezogenen Daten

Die Verarbeiteten Personenbezogenen Daten betreffen folgende Datenkategorien:

- Kontakt- und Benutzerinformationen, insbesondere Name, Telefonnummer, E-Mail-Adresse, Zeitzone und Adressdaten;
- Systemzugriffs-, Nutzungs- oder Autorisierungsdaten-, die Personenbezogene Daten enthalten oder sonstige anwendungsspezifische Inhalte, die Benutzer im Rahmen der jeweiligen Leistung hochladen; und
- ggf. weitere Personenbezogene Daten, die der Kunde und Weitere Verantwortliche durch das Hochladen oder Verbinden mit der jeweiligen Leistung oder in sonstiger Weise im Zusammenhang mit der jeweiligen Leistung zur Verfügung stellen.

Sensible Personenbezogene Daten (falls zutreffend)

Die jeweilige Leistung ist 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.

Häufigkeit der Übermittlung (z. B., ob die Daten einmalig oder kontinuierlich übermittelt werden)

- Wenn die jeweilige Leistung die Erbringung von Cloud-Diensten (wie unten definiert) erfasst, speichert Siemens die Personenbezogenen Daten kontinuierlich im Auftragt des Kunden.
- Wenn die jeweilige Leistung die Erbringung von Support-Leistungen (wie unten definiert) erfasst und keine abweichende Regelung in der Vereinbarung getroffen wird, hat Siemens jeweils nur bei der Leistungserbringung selbst Zugriff auf die Personenbezogenen Daten.

Art der Verarbeitung und Zweck der Datenübermittlung und Weiterverarbeitung
Siemens und Unterauftragsverarbeiter Verarbeiten Personenbezogene Daten, um die jeweilige Leistung 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 Personenbezogenen Daten erfordern ("**Support-Leistungen**").

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
Personenbezogene Daten werden für die Dauer der Vereinbarung gespeichert. Der Kunde hat entweder die Möglichkeit zur Berichtigung oder Löschung Personenbezogener Daten über die Funktionalitäten der jeweiligen Leistung, oder (b) Personenbezogene Daten werden auf Anweisung des Kunden durch Siemens berichtigt oder gelöscht.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.
Gegenstand, Art und Dauer der Verarbeitung werden je Unterauftragsverarbeiter in ANNEX III beschrieben

C. **Wenn die Standardvertragsklauseln Anwendung finden: ZUSTÄNDIGE AUFSICHTSBEHÖRDE**
Wenn der Kunde der Datenexporteur gemäß Modul 2 oder Modul 3 ist, ist die zuständige Aufsichtsbehörde, die nach Klausel 13 der Standardvertragsklauseln EU für den Kunden zuständige Aufsichtsbehörde. Eine Liste der Aufsichtsbehörden in der Europäischen Union hier https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm abrufbar.

Annex II zum DPA (und, soweit anwendbar, Anlage II zu den EU-Standardvertragsklausel)

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 der jeweiligen Leistungen 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
		X	X	-
	f) Autorisierungs- und Protokollierungsmaßnahmen für Netzwerkverbindungen zu IT-Systemen und IT-Anwendungen (insbesondere Firewalls zum Zulassen oder Verweigern eingehender Netzwerkverbindungen);	X	X	-
	g) 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
	h) Dokumentation und laufende Aktualisierung der privilegierten Zugriffsrechte auf IT-Systeme und IT-Anwendungen;	X	X	X
	i) Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte auf IT-Systeme und -Anwendungen;	X	X	X
	j) Passwort-Policy mit Anforderungen an die Komplexität von Passwörtern, Mindestlänge, sowie keiner Wiederverwendung von kürzlich verwendeten Passwörtern;	X	X	X
	k) Technische Durchsetzung der Passwort-Policy durch IT-Systeme und IT-Anwendungen;	X	X	X
	l) Richtlinie zum Sperren des Benutzerterminals beim Verlassen des Arbeitsplatzes;	X	X	X
	m) Automatisches Time-Out des Benutzerterminals bei Nichtbenutzung;	X	X	X
	n) automatisches Sperren der Benutzeridentifikation bei mehrfacher Falscheingabe von Passwörtern mit Protokollierung der Ereignisse (Überwachung von Zugriffsversuchen);	X	X	X
	o) Unverzüglicher 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
	p) Verwendung von sicheren und branchenüblichen 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	-	-
	c) 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	-	-

#	Maßnahmen	Szenario		
		1	2	3
	3.3 Siemens implementiert geeignete und branchenübliche 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 Information Security Framework basierend auf ISO 27001 Anforderungen, das regelmäßig überprüft und aktualisiert wird.	X	X	X
	4.2 Siemens definiert und protokolliert sicherheitsrelevante Ereignisse.	X	X	X
	4.3 Siemens analysiert kontinuierlich die jeweiligen Protokolldaten der IT-Systeme und Ereignisse auf Anomalien, Unregelmäßigkeiten, Hinweise auf Kompromittierung und andere verdächtige Aktivitäten.	X	X	X
	4.4 Siemens scannt 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. Das kann die folgenden Maßnahmen umfassen:			
	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	-
	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 branchenüblichen verschlüsselten Verbindungen, die dem Stand der Technik entsprechen.	X	X	-
	5.4 Siemens schützt die Integrität von Inhalten bei der Übertragung durch branchenübliche Netzwerkprotokolle, wie z.B. TLS.	X	X	-

#	Maßnahmen	Szenario		
		1	2	3
	5.5 Siemens verschlüsselt oder ermöglicht seinen Kunden die Verschlüsselung von Kundendaten.	X	X	-
	5.6 Siemens nutzt Schlüsselmanagementsysteme 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			
	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

#	Maßnahmen	Szenario		
		1	2	3

Annex III zum DPA (und, soweit anwendbar, Anlage III zu den EU-Standardvertragsklausel)

Liste genehmigter Unterauftragsverarbeiter

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

Annex IV zum DPA

Übersicht zur Datenschutzgrundverordnung (EU) 2016/679 (DSGVO)

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

#	Norm der DSGVO	Ziffer des DPA	Titel
1.	Artikel 28 (1)	Ziffer 4 und DPA Annexes	Technische und organisatorische Maßnahmen und DPA Annexes
2.	Artikel 28 (2), (3) (d) und (4)	Ziffer 6 und DPA Annexes	Unterauftragsverarbeiter
3.	Artikel 28 (3) Satz 1	Ziffer 2 und DPA Annexes	Beschreibung der Datenverarbeitung und DPA Annexes
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 DPA Annexes	Technische und organisatorische Maßnahmen und DPA Annexes
7.	Artikel 28 (3) (e)	Ziffer 10.1	Rechte Betroffener Personen
8.	Artikel 28 (3) (f) and 32	Ziffer 10.2, Ziffer 4 und DPA Annexes	Weitere Unterstützungsleistungen durch Siemens, Technische und organisatorische Maßnahmen und DPA Annexes
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 13	Laufzeit und Vertragsende
12.	Artikel 28 (3) (h)	Ziffer 11	Kontrollrechte
13.	Artikel 28 (4)	Ziffer 6	Unterauftragsverarbeiter
14.	Artikel 46 (1) (b) und (c)	Ziffer 7 und EU-Standardvertragsklauseln	Internationale Datentransfers und EU-Standardvertragsklauseln