Datenschutzanlage – Auftragsbearbeitungsvertrag der Siemens Schweiz AG (Siemens als Kunde)

Dieser Auftragsbearbeitungsvertrag („**AV-Vertrag**“) ist eine Anlage zum [Titel des Hauptvertrags einfügen] (der „**Vertrag**“). Alle verwendeten Begriffe, die nicht separate in diesem AV-Vertrag definiert werden, haben die im Vertrag definierte Bedeutung. Im Falle eines Konflikts zwischen den Bestimmungen dieses AV-Vertrags und Bestimmungen des Vertrags, gehen die Bestimmungen des AV-Vertrags vor.

1. Definitionen

„Anwendbares Datenschutzrecht“ bezeichnet alle geltenden Rechtsvorschriften in Bezug auf die Verarbeitung Personenbezogener Daten im Rahmen des Vertrags, einschliesslich, aber nicht beschränkt auf, (i) für Personenbezogene Daten, die von einem Berechtigten Unternehmen mit Sitz in der Schweiz stammen, das Bundesgesetz über den Datenschutz (DSG), (ii) für Personenbezogene Daten, die von einem Berechtigten Unternehmen mit Sitz im EWR stammen, die Datenschutz-Grundverordnung (EU) 2016/679 ("DSGVO") und (iii) für Personenbezogene Daten, die von einem Berechtigten Unternehmen mit Sitz im Vereinigten Königreich stammen, die UK DSGVO und der UK Data Protection Act 2018.

„Auftragnehmer“ bezeichnet den Auftragnehmer, welcher Partei des Vertrags oder einer darauf bezogenen individuellen Vereinbarung, Beitrittsvereinbarung, Bestellung oder anderen vertraglichen Vereinbarung ist, welche auf den Vertrag verweist.

„Auftragsbearbeiter“ bezeichnet eine natürliche oder juristische Person, Behörde, Agentur oder sonstige Einrichtung, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„**Berechtigtes Unternehmen“** bezeichnet eine juristische Person (einschliesslich Siemens und ihrer Konzerngesellschaften), die in ihrer Rolle als Verantwortlicher unter dem Vertrag berechtigt ist, mittelbar oder unmittelbar Dienste in Anspruch zu nehmen.

"**Dienste**" bezeichnet die Dienste, die vom Auftragnehmer im Rahmen des Vertrags in seiner Rolle als Auftragsbearbeiter im Sinne dieses AV-Vertrags erbracht werden. Dienste im Sinne dieser Definition können im Vertrag als "Cloud-Dienste", "Online-Dienste", "Angebot", "Produkt" oder anderweitig bezeichnet werden.

„**Drittlandtransfer**“ jede Verarbeitung (einschliesslich Übertragungen, internationaler Zugriff und Weiterübermittlungen) von Eingeschränkten Personenbezogenen Daten durch den Auftragnehmer oder einen seiner Unterauftragsbearbeiter ausserhalb des jeweiligen Ursprungsgebiets.

„Eingeschränkte Personenbezogene Daten“ bezeichnet alle Personenbezogenen Daten, die von einem Berechtigten Unternehmen aus einem Ursprungsgebiet stammen.

„**EU-Standardvertragsklauseln**" bezeichnet die Standardvertragsklauseln (EU) 2021/914.

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

„Land mit Angemessenheitsentscheidung“ bezeichnet jedes Land, für welches die EU-Kommission entschieden hat, dass dieses Land ein angemessenes Datenschutzniveau gewährleistet, und für Personenbezogene Daten aus dem Vereinigten Königreich jedes Land, für das gemäss den Abschnitten 17A oder 74A des Datenschutzgesetzes 2018 Angemessenheitsvorschriften des Vereinigten Königreichs erlassen wurden.

„Personenbezogene Daten“ bezeichnet alle Informationen, die sich direkt oder indirekt auf einen Betroffenen beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

“**Processor Binding Corporate Rules**” bezeichnet verbindliche unternehmensinterne Vorschriften für Auftragsbearbeiter, die von der zuständigen Aufsichtsbehörde genehmigt wurden.

„**Siemens**" bezeichnet das jeweilige Unternehmen des Siemens-Konzerns, das Partei des Vertrags oder einer darauf bezogenen individuellen Vereinbarung, Beitrittsvereinbarung, Bestellung oder anderen vertraglichen Vereinbarung ist, welche auf den Vertrag verweist.

„Übermittlungsgarantien“ bezeichnet angemessene Garantien für Drittlandtransfers, wie sie im geltenden Datenschutzrecht vorgeschrieben sind, wie z. B. angemessene Garantien im Sinne von Artikel 46 DSGVO.

„**UK DSGVO**" bezeichnet die DSGVO, wie sie gemäss Abschnitt 3 des European Union (Withdrawal) Act 2018 des Vereinigten Königreichs im Recht des Vereinigten Königreichs umgesetzt ist.

„UK-Standardvertragsklauseln" bezeichnet Standarddatenschutzklauseln, die von Zeit zu Zeit vom britischen Information Commissioner‘s Office ("ICO") gemäss Artikel 46 Absatz 2 der UK DSGVO angenommen werden, einschliesslich, aber nicht beschränkt auf das internationale Datenübermittlungsabkommen (UK IDTA) und die EU-Standardvertragsklauseln in der durch das International Data Transfer

Addendum des ICO zu den Standardvertragsklauseln der EU-Kommission („**UK Addendum**") geänderten Fassung.[1]

„**Unterauftragsbearbeiter**" bezeichnet jeden weiteren Auftragsbearbeiter, der an der Erbringung der Dienste beteiligt ist.

"**Ursprungsgebiet**" bezeichnet den EWR, das Vereinigte Königreich, die Schweiz und jedes Land mit ähnlichen Angemessenheitsanforderungen wie in Art. 45 ff. DSGVO.

„Verantwortlicher" bezeichnet eine natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Personenbezogenen Daten entscheidet.

„Verarbeitung" (und ihre anderen Formen wie Verarbeitet, Verarbeiten) bezeichnet den mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„Standardvertragsklauseln" bezeichnen die EU-Standardvertragsklauseln und die UK-Standardvertragsklauseln.

„Verletzung des Schutzes Personenbezogener Daten" oder „Datenschutzverstoss" bezeichnet eine Verletzung der Sicherheit, die, (i) ob unbeabsichtigt oder unrechtmässig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise im Rahmen des AV-Vertrags Verarbeitet werden oder (ii) nach geltendem Recht Meldepflichten gegenüber Dritten auslöst.

2. Einhaltung des Anwendbaren Datenschutzrechts

Die Parteien sind verpflichtet, das für sie geltende Anwendbare Datenschutzrecht entsprechend den Anforderungen dieser AV-Vereinbarung einzuhalten. Bei der Erbringung der Dienste hält der Auftragnehmer insbesondere die Bestimmungen des Anwendbaren Datenschutzrechts in Bezug auf die Verarbeitung Personenbezogener Daten als Auftragsbearbeiter ein.

3. Zulässige Verarbeitungstätigkeit

Der Auftragnehmer Verarbeitet Personenbezogene Daten nur im Einklang mit (i) den Bestimmungen dieses AV-Vertrags oder (ii) der dokumentierten Weisung von Siemens. Der Auftragnehmer ist insbesondere nicht berechtigt, Personenbezogenen Daten für eigene Geschäftszwecke zu verarbeiten oder an Dritte zu übermitteln, soweit er hierzu nicht durch diese AV-Vereinbarung autorisiert ist.

Der Auftragnehmer wird Siemens unverzüglich informieren, wenn eine Anweisung von Siemens nach seiner Auffassung gegen Anwendbares Datenschutzrecht verstösst.

4. Beschreibung der Auftragsbearbeitungstätigkeiten

Die Einzelheiten der vom Auftragnehmer zu erbringenden Auftragsbearbeitungstätigkeiten, insbesondere der Gegenstand der Verarbeitung, die Art und der Zweck der Verarbeitung, die Art der Verarbeiteten Personenbezogenen Daten und die Kategorien der betroffenen Personen, sind in **Anhang I** beschrieben.

5. Technische und organisatorische Massnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zweck der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, trifft der Auftragnehmer geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, einschliesslich, aber nicht beschränkt auf: (i) die Pseudonymisierung und Verschlüsselung Personenbezogener Daten; (ii) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; (iii) die Fähigkeit, die Verfügbarkeit der Personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; (iv) ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung. In diesem Zusammenhang trifft der Auftragnehmer mindestens die in **Anhang II** beschriebenen technischen und organisatorischen Massnahmen.

6. Verpflichtung zur Vertraulichkeit

Der Auftragnehmer verpflichtet sich den Zugriff auf Personenbezogene Daten auf einen Personenkreis zu beschränken, für den der Zugriff für die Erbringung der vertragsgegenständlichen Verarbeitungstätigkeiten erforderlich ist. Der Auftragnehmer ist verpflichtet seine Beschäftigten über die einschlägigen gesetzlichen und vertraglich vereinbarten Datenschutzvorschriften ausführlich zu unterrichten und sie auf deren Einhaltung und zur Vertraulichkeit zu verpflichten. Den Beschäftigten ist dabei insbesondere zu untersagen,

[1] Siehe https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

Personenbezogene Daten entgegen den Weisungen von Siemens zu verarbeiten. Die Verpflichtung zur Vertraulichkeit nach diesem Artikel wirkt auch nach Beendigung dieses AV-Vertrags, sowie dem Arbeitsverhältnis der Beschäftigten fort. Der Auftragnehmer wird Siemens die Verpflichtungserklärungen auf Wunsch zur Prüfung zur Verfügung stellen.

7. Unterauftragsbearbeiter

a) Der Auftragnehmer hat die allgemeine Genehmigung von Siemens für die Beauftragung von Unterauftragsbearbeitern. Eine aktuelle Liste der vom Auftragnehmer eingesetzten Unterauftragsbearbeiter ist in **Anhang III** enthalten.
b) Der Auftragnehmer wird Siemens über beabsichtigte Änderungen dieser Liste durch Ergänzung oder Ersatz von Unterauftragsbearbeitern mindestens 30 Tage im Voraus ausdrücklich schriftlich informieren. Der Auftragnehmer stellt Siemens die Informationen zur Verfügung, die zur Ausübung des Widerspruchsrechts erforderlich sind. Erhebt Siemens innerhalb dieser 30-tägigen Frist keine Einwände, so gilt dies als Genehmigung des neuen Unterauftragsbearbeiters. Wenn Siemens Einwände erhebt, wird der Auftragnehmer - bevor er den Unterauftragsbearbeiter zum Zugriff auf Personenbezogene Daten ermächtigt - angemessene Anstrengungen unternehmen, um die von Siemens geäusserten Bedenken und Vorbehalte auszuräumen und (i) von der Nutzung des Unterauftragsbearbeiters absehen oder (ii) Siemens eine angemessene Änderung der Dienste oder der Konfiguration oder Nutzung der Dienste von Siemens vorschlagen, um die Verarbeitung Personenbezogener Daten durch den beanstandeten neuen Unterauftragsbearbeiter zu vermeiden. Kann der Auftragnehmer die Gründe für den Widerspruch von Siemens nicht beseitigen, ist Siemens berechtigt, die betroffenen Services ohne Schadenersatz oder Pönalen zu kündigen. Im Falle einer Kündigung durch Siemens erstattet der Auftragnehmer alle vorausbezahlten Beträge für den jeweiligen Service anteilig zurück.
c) Beauftragt der Auftragnehmer einen Unterauftragsbearbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag von Siemens und/oder Berechtigten Unternehmen), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie jene, die dem Auftragnehmer durch diesen AV-Vertrag auferlegt werden.
d) Der Auftragnehmer stellt dem Auftraggeber auf dessen Verlangen eine Kopie eines solchen Unterauftrags und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschliesslich Personenbezogener Daten, notwendig ist, darf der Auftragnehmer den Text des Vertrags vor der Weitergabe einer Kopie unkenntlich machen.
e) Der Auftragnehmer wird den Unterauftragsbearbeiter regelmässig und in angemessener Weise im Hinblick auf die Einhaltung dieser Anforderungen kontrollieren und die Ergebnisse der Kontrollen dokumentieren.
f) Der Auftragnehmer bleibt gegenüber Siemens vollumfänglich verantwortlich für die Erfüllung der Verpflichtungen des Unterauftragsbearbeiters. Der Auftragnehmer ist verpflichtet, Siemens über jeden Verstoss des Unterauftragsbearbeiters gegen seine vertraglichen Verpflichtungen zu unterrichten.

8. Internationale Verarbeitung

Der Auftragnehmer stellt sicher, dass Drittlandtransfers durch Übermittlungsgarantien gemäss den **Anhängen III und IV** abgedeckt sind, es sei denn, der Drittlandtransfer erfolgt in ein Land mit einem Angemessenheitsbeschluss.

9. Unterstützungspflichten des Auftragnehmers

Der Auftragnehmer ist verpflichtet, Siemens bei der Einhaltung des Anwendbaren Datenschutzrechts angemessen zu unterstützen, insbesondere wie folgt:

a) Berichtigung, Löschung oder Einschränkung der Verarbeitung. Der Auftragnehmer ist verpflichtet (i) entweder die Berichtigung, Löschung oder Einschränkung der Verarbeitung der Verarbeiteten Personenbezogenen Daten über die Funktionalitäten der Dienste zu ermöglichen, oder (ii) die Berichtigung, Löschung oder Einschränkung der Verarbeitung entsprechend den Anweisungen von Siemens umzusetzen.
b) Auskunftsansprüche. Soweit Informationen über eine betroffene Person über die Funktionalitäten der Dienste nicht selbst abrufbar sind, stellt der Auftragnehmer Siemens diese Information zur Verfügung, soweit dies zur Erfüllung des für Siemens und Berechtigte Unternehmen Anwendbaren Datenschutzrechts erforderlich ist.
c) Anfragen von Betroffenen und Behörden. Der Auftragnehmer informiert Siemens unverzüglich über (i) Anordnungen oder Anfragen einer Aufsichts- oder Ermittlungsbehörde oder eines zuständigen Gerichts, oder (ii) Anfragen von betroffenen Personen. Der Auftragnehmer ist nicht berechtigt die vorgenannten Anfragen, ohne entsprechende Weisung von Siemens, selbst zu beantworten. Der Auftragnehmer ist verpflichtet, Siemens auf Verlangen in angemessenem Umfang bei der Beantwortung der Anfragen zu unterstützen.
d) Datenportabilität. Auf Siemens Anforderung und soweit Betroffene nach Anwendbarem Datenschutzrecht einen Anspruch auf Datenportabilität haben, wird der Auftragnehmer bei der Umsetzung von solchen Ansprüchen unterstützen und (i) ermöglichen Personenbezogene Daten eines bestimmten Betroffenen gemäss den Funktionalitäten des Dienstes zu extrahieren oder (ii) Siemens und/oder dem Berechtigten Unternehmen den betreffenden Datensatz in einem strukturierten, marktüblichen und maschinenlesbaren Format zur Verfügung stellen.

e) Datenschutzfolgenabschätzungen. Auf Verlangen von Siemens unterstützt der Auftragnehmer bei der Durchführung von Datenschutzfolgenabschätzungen im Sinne des Anwendbaren Datenschutzrechten in angemessenem Umfang.

10. Beendigung des Auftrags

Im Falle der Beendigung des Auftrags hat der Auftragnehmer die ihm überlassenen oder im Rahmen der Auftragsbearbeitung erstellten Personenbezogenen Daten - vorbehaltlich anderer vertraglicher Vereinbarungen oder Vorgaben seitens Siemens - zurückzugeben und im Verfügungsbereich des Auftragnehmers verbleibende Daten unwiederbringlich zu löschen bzw. zu vernichten. Die Löschung bzw. Vernichtung ist Siemens auf Verlangen schriftlich zu bestätigen.

11. Mitteilungspflichten

a) Der Auftragnehmer unterrichtet Siemens unverzüglich, spätestens jedoch innerhalb von 48 Stunden, bei Eintritt oder bei begründetem Verdacht des Eintritts eines Datenschutzverstosses.
b) In der Unterrichtung hat der Auftragnehmer Siemens folgende Informationen mitzuteilen: (i) Die Kontaktdaten, eine Anlaufstelle für weitere Informationen, (ii) eine Beschreibung der Art der Verletzung (soweit möglich unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Personenbezogene Datensätze), (iii) die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Massnahmen zur Behebung des Datenschutzverstosses und Massnahmen zur Abmilderung möglicher nachteiligen Auswirkungen. Wenn und soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschliessend ohne schuldhaftes Zögern bereitgestellt.
c) Meldungen nach diesem Artikel sind an den im Vertrag benannten Ansprechpartner sowie an datenschutz@siemens.com zu richten.
d) Der Auftragnehmer verpflichtet sich auf eigene Kosten (i) im Benehmen mit Siemens einen Datenschutzverstoss umfassend aufzuklären, (ii) Siemens bei der Erfüllung gegebenenfalls bestehender gesetzlicher Meldepflichten gegenüber betroffenen Personen oder Behörden (durch Einzelansprachen der betroffenen Personen, Veröffentlichungen in den Medien oder ähnliche Massnahmen) oder (iii) bei sonstigen Massnahmen im Zusammenhang mit dem Datenschutzverstoss zu unterstützen.
e) Die Entscheidung, (i) ob ein Datenschutzverstoss Meldepflichten auslöst und (ii) wie und in welcher Form eine Meldung erfolgt, liegt im alleinigen Ermessen von Siemens, es sei denn der Auftragnehmer ist nach Anwendbarem Datenschutzrecht selbst zur Meldung verpflichtet.
f) Der Auftragnehmer verpflichtet sich auf seine Kosten angemessene Massnahmen zu treffen, um den Datenschutzverstoss zu beheben und nachteilige Auswirkungen abzumildern. Des Weiteren ist der Auftragnehmer verpflichtet, angemessene Massnahmen zu ergreifen, die verhindern, dass sich der Datenschutzverstoss wiederholt, einschliesslich aller Massnahmen, die nach Anwendbarem Datenschutzrecht erforderlich sind.
g) Der Auftragnehmer ist verpflichtet, Siemens alle Kosten und Aufwendungen zu erstatten, die durch einen vom Auftragnehmer schuldhaft verursachten Datenschutzverstoss entstehen. Erfasst sind dabei insbesondere auch Kosten für Credit-Monitoring-Services für Personen, deren Personenbezogene Daten von einem Datenschutzverstoss betroffen sind. Haftungsbeschränkungen zu Gunsten des Auftragnehmers nach diesem Vertrag finden insoweit keine Anwendung.

12. Dokumentation und Kontrollen

a) Der Auftragnehmer ist verpflichtet, (i) angemessene Massnahmen zu ergreifen, um die Einhaltung der Pflichten nach diesem AV-Vertrag und Anwendbarem Datenschutzrechts zu prüfen und (ii) die Ergebnisse der Prüfung in regelmässigen (mindestens jährlichen) und anlassbezogenen Auditberichten (jeweils ein „**Auditbericht**“), zu dokumentieren und (iii) Siemens und Berechtigten Unternehmen, die Verarbeitungsleistungen unter dem Vertrag beziehen, auf Verlangen zur Verfügung zu stellen. Sieht eine vom Auftragnehmer umgesetzte Zertifizierung oder ein umgesetzter Standard-Prüfungen vor, ist jede Prüfung entsprechend den Regeln der zuständigen Aufsichts- oder Akkreditierungsstellen durchzuführen.
b) Wenn dies zur Erfüllung von Anforderungen an Kontrollen nach Anwendbarem Datenschutzrecht erforderlich ist oder ein entsprechender Bescheid einer zuständigen Aufsichtsbehörde vorliegt, stellt der Auftragnehmer Siemens und Berechtigten Unternehmen, neben den Auditberichten, alle weiteren erforderlichen Informationen zur Verfügung und ermöglicht weitere Überprüfungen - einschliesslich Inspektionen -, die von Siemens oder einem Berechtigten Unternehmen oder von einem von Siemens oder einem Berechtigten Unternehmen beauftragten Prüfer durchgeführt werden. Zu diesem Zweck hat Siemens, Berechtigte Unternehmen oder ein von Siemens oder einem Berechtigten Unternehmen beauftragter Prüfer das Recht, Vor-Ort-Kontrollen durchzuführen. Vor-Ort-Kontrollen sind mit angemessener Frist anzukündigen und erfolgen nur zu den üblichen Geschäftszeiten und ohne den Geschäftsbetrieb des Auftragnehmers zu stören.

13. Einsatz von Cookies

Für den Einsatz von Cookies und ähnlichen Lösungen im Rahmen der Dienste gilt das Folgende: ohne das ausdrückliche Einverständnis von Siemens unter Bezugnahme auf diese Ziffer 13 ist die Speicherung von Informationen oder

der Zugriff auf Informationen, die im Endgerät eines Nutzers der Dienste gespeichert sind, nur zulässig, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um die Kernfunktionalitäten der Dienste zu erbringen.

14. Verschiedenes

Die Bestimmungen dieses AV-Vertrags gelten als integraler Bestandteil des Vertrags und ein wesentlicher Verstoss gegen die Bestimmungen dieses AV-Vertrags gilt als wesentlicher Verstoss gegen die Bestimmungen des Vertrags, der Siemens zu in der Vereinbarung enthaltenen Abhilfemassnahmen im Zusammenhang mit wesentlichen Verstössen berechtigt.

Anhang I zum AV-Vertrag (und, soweit anwendbar, den Standardvertragsklauseln)

A. LISTE DER PARTEIEN

Service-Empfänger / Datenexporteur(e):

Name:	[Siemens Schweiz AG]
Anschrift:	[Freilagerstrasse 40, 8047 Zürich, Schweiz]
Name, Funktion und Kontaktdaten der Kontaktperson	Büro des Siemens Datenschutzbeauftragten Werner-von-Siemens-Strasse 1, 80333 München, Deutschland E-Mail: datenschutz@siemens.com
Aktivitäten relevant für die Datenübertragung/-verarbeitung	Siemens ist ein Technologieunternehmen mit den Schwerpunkten Industrie, Infrastruktur, Verkehr und Gesundheitswesen.
Rolle (Verantwortlicher/Auftragsbearbeiter)	Siemens agiert als Verantwortlicher der Verarbeitungstätigkeit, die durch den Auftragnehmer gegenüber Siemens erbracht wird und als Auftragsbearbeiter gemäss den Weisungen seiner Berechtigten Unternehmen für Verarbeitungstätigkeiten des Auftragnehmers gegenüber den Berechtigten Unternehmen.

Datenimporteur(e):

Name:	[Einfügen]
Anschrift:	[Einfügen]
Name, Funktion und Kontaktdaten der Kontaktperson	[Einfügen]
Aktivitäten relevant für die Datenübertragung/-verarbeitung	[Einfügen]
Rolle (Verantwortlicher/Auftragsbearbeiter)	Der Auftragnehmer agiert als Auftragsbearbeiter, der Personenbezogenen Daten im Auftrag und nach Weisung von Siemens und, gegebenenfalls, im Auftrag Berechtigter Unternehmen verarbeitet.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien von Betroffenen, deren Personenbezogene Daten übermittelt/verarbeitet werden	☐ Angestellte und sonstiges Personal (einschliesslich Bewerber, regulär / zeitlich befristet Beschäftigte, Teilzeitkräfte, Auszubildende, Auftragnehmer und Vertreter) ☐ Ansprechpartner bei Geschäftspartnern, Lieferanten, Dienstleistern und anderen Kooperationspartnern ☐ Kunde(n) und/oder deren Angestellte oder sonstiges Personal (einschliesslich Bewerber, regulär / zeitlich befristet Beschäftigte, Teilzeitkräfte, Auszubildende, Auftragnehmer und Vertreter) ☐ Anwender von Siemens Softwareprodukten/-dienstleistungen ☐ Sonstiges, bitte auflisten: [Einfügen] Weitere betroffene Personen, deren Personenbezogene Daten in einer Anwendung oder einem IT-System enthalten sind, das im Rahmen der bereitgestellten Dienste liegt.

Kategorien der übermittelten Personenbezogener Daten	☐ Kontaktinformationen (wie Name, Adresse, Telefon- oder Faxnummer, E-Mail-Adresse) ☐ Organisationsorganisation (z.B. Stellenbezeichnung, Abteilung) ☐ Standortdaten (z.B. GPS) ☐ Staatliche und persönliche Identifikationsnummern (z. B. Sozialversicherungsnummer, Führerscheinnummer) ☐ Finanzdaten (wie Einkommen, Kreditakten, Transaktionen, Kreditauskünfte, Kauf- und Konsumgewohnheiten, Insolvenzstatus) ☐ Beschäftigungsdaten (z.B. Bewerbungsdaten und Qualifikation, Vergütungs- und Gehaltsabrechnungsdaten, Mitarbeiteridentifikationsdaten, Mitarbeiterstatus, Anwesenheitsdaten, Beschäftigungshistorie) ☐ Benutzerkontodaten (z.B. Benutzername/ID und Passwort) ☐ Informationen im Zusammenhang mit der Nutzung von IT-Geräte durch die betroffene Person (z.B. IP-Adresse, Anmeldeinformationen) ☐ Finanzkontoinformationen wie Bank-/Kreditkartendaten, Kontonummern, Kreditkartennummern usw. ☐ Sonstiges; bitte auflisten: [Einfügen] Alle weiteren Personenbezogenen Daten, die in einer Anwendung oder einem IT-System enthalten sind, das im Anwendungsbereich der erbrachten Dienste enthalten ist.
Besondere Kategorien Personenbezogener Daten, auf die zugegriffen oder die verarbeitet werden sollen	☐ Angaben zur Rasse oder ethnischen Herkunft ☐ Informationen zu politischen Meinungen ☐ Informationen über religiöse oder philosophische Überzeugungen ☐ Informationen zur Gewerkschaftsmitgliedschaft ☐ Informationen zum Sexualleben oder zur sexuellen Orientierung ☐ Biometrische Daten ☐ Genetische Daten ☐ Gesundheitsdaten (geistige oder körperliche Behinderungen, Familienanamnese, persönliche medizinische Anamnese, Krankenakten, Rezepte usw.) ☐ Sonstiges; bitte auflisten: [Einfügen] Die Beschränkungen oder Garantien, die für solche sensiblen Personenbezogenen Daten gelten, sind in **ANHANG II** beschrieben.

Die Häufigkeit der Übermittlung (Zugriff/Übermittlung)	☐ Der Auftragnehmer hostet Personenbezogene Daten im Auftrag von Siemens und gegebenenfalls Berechtigten Unternehmen ☐ Auftragnehmer greift bei der Bereitstellung der Dienste aus der Ferne auf Personenbezogene Daten zu ☐ einmalig ☐ kontinuierlich ☐ Der Auftragnehmer Verarbeitet Personenbezogene Daten bei der Erbringung der Dienstleistungen anderweitig ☐ einmalig ☐ kontinuierlich
Art der Verarbeitung und Zweck(e) der Datenübermittlung und Weiterverarbeitung	☐ Provider bietet **Wartungs- und Supportleistungen** an und kann Zugriff, einschliesslich Remote-Zugriff, auf Personenbezogene Daten haben. ☐ Der Auftragnehmer erbringt **professionelle Dienstleistungen**, indem er Dienstleistungen in Verbindung mit einer Anwendung / einem System oder einem Netzwerk erbringt, wie z. B. Installation, Konfiguration oder Datenmigration oder andere damit verbundene IT-Dienste, und kann Zugriff, einschliesslich Remote-Zugriff, auf Personenbezogene Daten haben. ☐ Der Auftragnehmer bietet Managed Services, einschliesslich Rechenzentrums- und Infrastrukturmanagement, Backup- und Recovery-Management und hat möglicherweise Zugriff, einschliesslich Remote-Zugriff, auf Personenbezogene Daten. ☐ Der Auftragnehmer stellt XaaS-Dienste (Software-, Plattform- oder Infrastructure-as-a-Service) bereit, die vom Auftragnehmer (oder einem seiner UnterAuftragsbearbeiter) gehostet werden. Dies kann die Erhebung, Speicherung, Reorganisation, Anpassung und Bereitstellung Personenbezogener Daten umfassen. ☐ Sonstiges: [Einfügen]
Dauer	☐ Die Personenbezogenen Daten werden für die Dauer des Vertrags aufbewahrt. Siemens hat die Möglichkeit, die Verarbeitung Personenbezogener Daten über die Funktionen der Dienste zu berichtigen, zu löschen oder einzuschränken oder der Auftragnehmer wird die Verarbeitung Personenbezogener Daten gemäss den Anweisungen von Siemens zu berichtigen, löschen oder einschränken. ☐ Die Personenbezogenen Daten werden für einen Zeitraum aufbewahrt von: [bitte angeben] ☐ Sonstiges: [Einfügen]
Bei Datenübermittlungen an (Unter-)Auftragsbearbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben	Der Gegenstand, die Art und die Dauer der Verarbeitung sind pro UnterAuftragsbearbeiter in **Anhang III** angegeben.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

- Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)
  Feldeggweg 1
  CH - 3003 Bern
  Schweiz
- Ist Siemens nicht in einem EU-Mitgliedstaat niedergelassen, sondern fällt gemäss Art. 3 Abs. 2 DSGVO in deren räumlichen Anwendungsbereich, so fungiert die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter im Sinne des Art. 27 Abs. 1 DSGVO niedergelassen ist, als zuständige Aufsichtsbehörde, nämlich die Aufsichtsbehörde:
  Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
  Promenade 18
  91522 Ansbach
  Deutschland

ANHANG II zum AV-Vertrag (und, soweit anwendbar, den Standardvertragsklauseln

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN EINSCHLIESSLICH TECHNISCHER UND ORGANISATORISCHER MASSNAHMEN ZUR GEWÄHRLEISTUNG DER DATENSICHERHEIT

Beschreibung der technischen und organisatorischen Sicherheitsmassnahmen, die der Auftragnehmer und Unterauftragsbearbeiter umsetzen:

☐ Die technischen und organisatorischen Massnahmen sind in den Cybersicherheitsklauseln und/oder Anhängen des Abkommens, einschliesslich Anhang [Referenz auf den Cybersecurity Anhang einfügen], beschrieben.

☒ Der Auftragnehmer und Unterauftragsbearbeiter setzen die nachstehend beschriebenen technischen und organisatorischen Massnahmen um. Die Parteien vereinbaren, dass Vertragsklauseln zur Cybersicherheit und/oder Anhänge der Vereinbarung (falls vorhanden) weitere technische und organisatorische Massnahmen enthalten können.

#	Massnahmen
1.	Physische Sicherheitsmassnahmen und Zutrittskontrollen
	Der Auftragnehmer 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; b) Sicherung und Einschränkung der Zugangswege; c) Sicherung der dezentralen Datenverarbeitungsanlagen und Personalcomputer; d) Festlegung von Zugriffsberechtigungen für Mitarbeiter und Dritte, einschliesslich der entsprechenden Dokumentation; e) Regelung zu den Zugangskarten f) Beschränkung der Zugangskarten g) Protokollierung, Überwachung und Nachverfolgung aller Zugriffe auf das Rechenzentrum, in dem Siemens Daten gehostet werden; h) Sicherung des Rechenzentrums, in dem Siemens Daten gehostet werden, durch Zugangskontrollen und andere geeignete Sicherheitsmassnahmen; und i) Wartung und Inspektion in IT-Bereichen und Rechenzentren nur durch autorisiertes Personal
2.	Zugriffskontrolle (IT-Systeme und/oder IT-Anwendungen)
	2.1 Der Auftragnehmer implementiert ein Rollen- und Berechtigungskonzept.

#	Massnahmen
	2.2. Der Auftragnehmer implementiert ein Autorisierungs- und Authentifizierungs-Framework, das unter anderem die folgenden Elemente umfasst: a) Rollenbasierte Zugriffskontrollen; b) Verfahren zum Erstellen, Ändern und Löschen von Accounts; c) Schutz des Zugriffs auf IT-Systeme und IT-Anwendungen durch Authentifizierungsmechanismen; d) Nutzung geeigneter Authentifizierungsmethoden, basierend auf den Eigenschaften und technischen Möglichkeiten des IT-Systems oder der IT-Anwendung; e) Erfordernis einer angemessenen Authentifizierung für den Zugang zu IT-Systemen und IT-Anwendungen; f) Protokollierung, Überwachung, Nachverfolgung sämtlicher Zugriffe auf Siemens Daten; g) Autorisierungs- und Protokollierungsmassnahmen für ein- und ausgehende Netzwerkverbindungen zu IT-Systemen und IT-Anwendungen (insbesondere Firewalls zum Zulassen oder Verweigern eingehender Netzwerkverbindungen); h) Vergabe privilegierter Zugriffsrechte auf IT-Systeme, IT-Anwendungen und Netzwerkdienste nur an Personen, die diese zur Erfüllung ihrer Aufgaben benötigen (Least-Privilege-Prinzip) i) Dokumentation und laufende Aktualisierung der privilegierten Zugriffsrechte auf IT-Systeme und IT-Anwendungen; j) Regelmässige Überprüfung und Aktualisierung der Zugriffsrechte auf IT-Systeme und -Anwendungen; k) Passwort-Policy mit Anforderungen an die Komplexität von Passwörtern, Mindestlänge und Ablauf nach angemessener Zeit, sowie keiner Wiederverwendung von kürzlich verwendeten Passwörtern; l) Technische Durchsetzung der Passwort-Policy durch IT-Systeme und IT-Anwendungen; m) Entzug der Zugriffsrechte von Mitarbeitern und externem Personal auf IT-Systeme und IT-Anwendungen bei Beendigung des Arbeitsverhältnisses oder des Vertrages; und n) Verwendung von sicheren, dem Stand der Technik entsprechenden Authentifizierungszertifikaten.
	2.3. IT-Systeme und IT-Anwendungen sperren sich automatisch oder beenden die Sitzung nach Überschreiten einer zuvor definierten, angemessenen Leerlaufzeit.
	2.4 Der Auftragnehmer beschränkt den privilegierten Zugang zu Cloud-Ressourcen auf einzelne oder bestimmte Bereiche von IP-Adressen
	2.5 Der privilegierte Zugang zu Cloud-Ressourcen erfolgt über einen Bastion-Host.
	2.6 Der Auftragnehmer unterhält Anmeldeverfahren an IT-Systemen mit Schutzmassnahmen gegen verdächtige Anmeldeaktivitäten (z. B. gegen Brute-Force- und Password-Guessing-Angriffe).
3.	Verfügbarkeitskontrolle
	3.1 Der Auftragnehmer implementiert geeigneter und dem Stand der Technik entsprechender Anti-Malware-Lösungen zum Schutz der Systeme und Anwendungen vor Schadsoftware.
	3.2 Der Auftragnehmer 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); b) vordefinierte Backup-Intervalle; und c) regelmässiges Testen der Wiederherstellung von Daten aus Backups entsprechend der Sensibilität des IT-Systems oder der IT-Anwendung.
	3.3 Der Auftragnehmer speichert Backups an einem anderen physischen Ort als dem Ort, an dem das laufende System gehostet wird.
	3.4 IT-Systeme und IT-Anwendungen in Nicht-Produktionsumgebungen sind logisch oder physikalisch von IT-Systemen und IT-Anwendungen in Produktionsumgebungen getrennt.
	3.5 Rechenzentren, in denen Siemens Daten gespeichert oder verarbeitet werden, sind gegen Naturkatastrophen, physische Angriffe und Unfälle geschützt.
	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.
4.	Betriebssicherheit
	4.1 Der Auftragnehmer unterhält und implementiert ein unternehmensweites ISO 27001 Information Security Framework, das regelmässig überprüft und aktualisiert wird.

#	Massnahmen
	4.2 Der Auftragnehmer 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.
	4.3 Der Auftragnehmer analysiert kontinuierlich die jeweiligen Protokolldaten der IT-Systeme und IT-Applikationen auf Anomalien, Unregelmässigkeiten, Hinweise auf Kompromittierung und andere verdächtige Aktivitäten.
	4.4 Der Auftragnehmer scannt und testet IT-Systeme und IT-Anwendungen regelmässig auf Sicherheitslücken.
	4.5 Der Auftragnehmer implementiert und unterhält einen Change-Management-Prozess für IT-Systeme und IT-Applikationen.
	4.6 Der Auftragnehmer unterhält einen Prozess zur Aktualisierung und Implementierung von Security Fixes und Updates der Hersteller auf den jeweiligen IT-Systemen und IT-Applikationen.
	4.7 Der Auftragnehmer löscht Daten unwiederbringlich oder vernichtet die Datenträger physisch, bevor ein IT-System entsorgt oder wiederverwendet wird.
5.	Übertragungssteuerung
	5.1 Der Auftragnehmer dokumentiert und aktualisiert regelmässig die Netzwerktopologien und deren Sicherheitsanforderungen.
	5.2 Der Auftragnehmer 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); b) Proxy-Server; c) Intrusion Detection Systems (IDS) und/oder Intrusion Prevention Systems (IPS); d) UR-Filterung; und e) Security Information and Event Management (SIEM) Systeme.
	5.3 Der Auftragnehmer verwaltet IT-Systeme und IT-Anwendungen unter Verwendung von verschlüsselten Verbindungen, die dem Stand der Technik entsprechen.
	5.4 Der Auftragnehmer schützt die Integrität von Inhalten bei der Übertragung durch modernste Netzwerkprotokolle, wie z.B. TLS.
	5.5 Der Auftragnehmer verschlüsselt oder ermöglicht Siemens die Verschlüsselung von Kundendaten, die über öffentliche Netze übertragen werden.
	5.6 Der Auftragnehmer verschlüsselt oder ermöglicht Siemens die Verschlüsselung von Siemens-Daten, wenn diese auf Datenbanken des Auftragnehmers gespeichert werden.
	5.7 Der Auftragnehmer nutzt sichere Key Management Systeme (KMS) zur Speicherung von geheimen Schlüsseln in der Cloud.
6.	Sicherheitstechnische Vorfälle

#	Massnahmen
	Der Auftragnehmer unterhält und implementiert einen Prozess zur Behandlung von sicherheitstechnischen Vorfällen, der unter anderem Folgendes umfasst: a) Aufzeichnungen über Sicherheitsverstösse; b) Prozesse zur Benachrichtigung des Auftragnehmers; und 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.
7.	Asset Management, Systembeschaffung, Entwicklung und Wartung
	7.1 Der Auftragnehmer 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.
	7.2 Der Auftragnehmer implementiert einen formalen Prozess zur Kontrolle und Durchführung von Änderungen an entwickelten Anwendungen.
	7.3 Der Auftragnehmer konzipiert und integriert Sicherheitstests in den System Development Life Cycle von IT-Systemen und IT-Anwendungen.
	7.4 Der Auftragnehmer implementiert einen angemessenen Security-Patching-Prozess, der Folgendes umfasst:
	a) Überprüfung der Komponenten auf mögliche Schwachstellen (CVEs);
	b) Prioritätseinstufung der Fehlerbehebungen;
	c) rechtzeitige Implementierung des Fixes; und
	d) das Herunterladen von Patches aus vertrauenswürdigen Quellen.
8.	Personalsicherheit
	8.1 Der Auftragnehmer setzt im Bereich der Personalsicherheit folgende Massnahmen um:
	a) Verpflichtung von Mitarbeitern mit Zugang zu Siemens Daten zur Vertraulichkeit; und
	b) Regelmässige Schulung von Mitarbeitern mit Zugang zu Siemens Daten hinsichtlich anwendbarer Datenschutzgesetze und -vorschriften.
	8.2 Der Auftragnehmer implementiert einen Offboarding-Prozess für Mitarbeiter des Auftragnehmers und externe Lieferanten.
9.	Kryptographie
	9.1. Der Auftragnehmer verwendet sichere, dem Stand der Technik entsprechende Zertifikate und setzt Folgendes um:
	a) Digitale Zertifikate werden nur dann akzeptiert und als vertrauenswürdig eingestuft, wenn das digitale Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde,
	b) Zertifikate werden verwendet und dedizierten IT-Systemen und Anwendungen zugeordnet; und die Gültigkeit von digitalen Zertifikaten überprüft wird.
	9.2 Der Auftragnehmer implementiert einen Prozess für die Verwaltung und Implementierung von kryptographischen Schlüsseln, einschliesslich Regeln und Anforderungen für die Erzeugung, Speicherung, Sicherung, Verteilung und den Widerruf von kryptographischen Schlüsseln.

ANHANG III zum AV-Vertrag (und, soweit anwendbar, den Standardvertragsklauseln)

LISTE DER UNTERAUFTRAGSBEARBEITER UND RECHENZENTRUMSSTANDORTE

A. **Unternehmen (einschliesslich Auftragnehmer und Unterauftragsbearbeiter), die an der Speicherung/dem Hosting von Inhalten beteiligt sind**

Wenn und soweit die Bereitstellung der Dienste das Hosting Personenbezogener Daten umfasst oder beinhaltet, speichert der Auftragnehmer die Personenbezogenen Daten an den unten angegebenen Rechenzentrumsstandorten ("Rechenzentrumsstandort"). Der Auftragnehmer darf ohne Zustimmung von Siemens keine Personenbezogenen Daten vom jeweiligen Rechenzentrumsstandort übertragen. Der in Abschnitt 7 enthaltene Benachrichtigungs- und Einspruchsmechanismus findet insoweit keine Anwendung.

Name des Unternehmens, Adresse und Kontaktperson (einschliesslich Name, Position und Kontaktdaten)	**Rechenzentrumsstandort**	**Regionen, die vom Rechenzentrumsstandort bedient werden**	**Übermittlungsgarantien im Falle eines Drittlandtransfers**
Name des Unternehmens: […] Adresse: […] Kontaktperson: […]	[Ort des Rechenzentrums einfügen, z.B. Europäische Union]	[Beschreiben Sie, ob ein bestimmtes Rechenzentrum alle Regionen bedient oder ob es dedizierte Rechenzentren für bestimmte Regionen gibt]	☐ Kein Drittlandtransfer ☐ Standardvertragsklauseln ☐ Prozessor BCR ☐ Sonstiges: _____
Name des Unternehmens: […] Adresse: […] Kontaktperson: […]	[…]	[…]	☐ Kein Drittlandtransfer ☐ Standardvertragsklauseln ☐ Prozessor BCR ☐ Sonstiges: _____

B. Unterauftragsbearbeiter, die an der Verarbeitung Personenbezogener Daten für <u>andere Zwecke als Speicherung / Hosting</u> beteiligt sind

Name des Unternehmens, Adresse und Kontaktperson (einschliesslich Name, Position und Kontaktdaten)	**Land/Region, in der die Verarbeitung durchgeführt wird**	**Regionen, die vom Unterauftragsbearbeiter bedient werden**	**Beschreibung der Verarbeitung (einschliesslich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere UnterAuftragsbearbeiter genehmigt sind)**	**Übermittlungsgarantien im Falle eines Drittlandtransfers**
Name des Unternehmens: […] Adresse: […] Kontaktperson: […]	[Ort einfügen, an dem die Daten verarbeitet werden, z.B. Europäische Union]	[Beschreiben Sie, ob ein bestimmtes Rechenzentrum alle Regionen bedient oder ob es dedizierte Rechenzentren für bestimmte Regionen gibt]	[bitte beschreiben, bitte ggf. auch die Dauer der Verarbeitung angeben]	☐ Kein Drittlandtransfer ☐ Standardvertragsklauseln ☐ Prozessor BCR ☐ Sonstiges: _____
Name des Unternehmens: […] Adresse: […] Kontaktperson: […]	[…]	[…]		☐ Kein Drittlandtransfer ☐ Standardvertragsklauseln ☐ Prozessor BCR ☐ Sonstiges: _____

Anhang IV des AV-Vertrags

INTERNATIONALE DATENVERARBEITUNG

Im Falle von Drittlandtransfers an den Auftragnehmer gelten die Standardvertragsklauseln als Übermittlungsgarantie, sofern nichts anderes schriftlich mit Siemens vereinbart ist. Im Falle von Drittlandtransfers an Unterauftragsbearbeiter stellt der Auftragnehmer sicher, dass solche Drittlandtransfers durch die in Anhang III aufgeführten Übermittlungsgarantien abgedeckt sind.

1. Standardvertragsklauseln. Folgendes gilt, wenn eine Übermittlungsgarantie auf den Standardvertragsklauseln beruht:

a) **EWR Auftragnehmer**. Wenn der Auftragnehmer seinen Sitz im EWR hat, schliesst der Auftragnehmer mit seinem UnterAuftragsbearbeiter die Standardvertragsklauseln (Modul 3) ab. Abschnitt 1 Absatz g), h), i) (ii) und Absatz j) Satz 2 gelten nicht, wenn der Auftragnehmer seinen Sitz im EWR hat.

b) **Auftragnehmer ausserhalb des EWR**. Befindet sich der Auftragnehmer ausserhalb des EWR, unterliegt der Drittlandtransfer den Modulen 2 und 3 der Standardvertragsklauseln. Die betreffenden Regelungen der Standardvertragsklauseln werden durch Bezugnahme einbezogen und sind integraler Bestandteil dieses AV-Vertrags. Die für die Zwecke der Anhänge der Standardvertragsklauseln erforderlichen Informationen sind in den Anhängen I bis III dieses AV-Vertrags enthalten.

c) **Docking Klausel**. Die Option in Klausel 7 der Standardvertragsklauseln findet keine Anwendung.

d) **Weiterübermittlungen**. Jede weitere Übermittlung muss den Klauseln 8 und 9 des anwendbaren Moduls der Standardvertragsklauseln entsprechen. Für den Fall, dass Siemens seinen Sitz ausserhalb des EWR hat und selbst als Datenimporteur im Rahmen von Standardvertragsklauseln mit Berechtigten Unternehmen auftritt, gilt die drittbegünstigende Klausel in Klausel 9 (e) der Standardvertragsklauseln zugunsten dieser Berechtigten Unternehmen.

e) **Einsatz von Unterauftragsbearbeitern**. Es gilt Option 2 von Klausel 9. Für die Zwecke der Klausel 9 a) hat der Auftragnehmer die allgemeine Genehmigung von Siemens, UnterAuftragsbearbeiter gemäss Ziffer 7 dieses AV-Vertrags zu beauftragen.

f) **Rechtsbehelfe**. Für den Fall, dass der Auftragnehmer betroffenen Personen anbietet, eine Beschwerde bei einer unabhängigen Streitbeilegungsstelle einzureichen (siehe Option in Klausel 11), wird der Auftragnehmer Siemens schriftlich über die zuständige Schlichtungsstelle informieren und die geltenden Anforderungen in Klausel 11 und der anwendbaren Schiedsgerichtsordnung einhalten.

g) **Anwendbares Recht**. Das anwendbare Recht für die Zwecke von Klausel 17 ist das Recht, das im Abschnitt über das anwendbare Recht des Vertrags bezeichnet ist. Unterliegt der Vertrag nicht dem Recht eines EU-Mitgliedstaates, so unterliegen die EU-Standardvertragsklauseln dem Recht der Bundesrepublik Deutschland.

h) **Wahl des Gerichtsstands und der Gerichtsbarkeit**. Die Gerichte gemäss Klausel 18 sind diejenigen, die im Abschnitt über den Gerichtsstand des Vertrags benannt sind. Wenn die ausschliessliche Zuständigkeit für die Beilegung von Streitigkeiten oder Rechtsstreitigkeiten, die sich aus oder im Zusammenhang mit dem Vertrag ergeben, nach dem Vertrag nicht bei einem Gericht eines EU-Mitgliedstaats liegt, vereinbaren die Parteien, dass die Gerichte Deutschlands die ausschliessliche Zuständigkeit für die Beilegung von Streitigkeiten haben, die sich aus den EU-Standardvertragsklauseln ergeben.

i) **Berechtigte Unternehmen im Vereinigten Königreich.** Falls Drittlandtransfers von Berechtigten Unternehmen mit Sitz im Vereinigten Königreich stammen, gilt Folgendes:

(i) Es ist das UK Addendum zu verwenden, sofern mit Siemens nichts anderes schriftlich vereinbart ist.

(ii) Teil 1 des UK Addendums wird wie folgt angewandt:

Tabelle 1 des UK Addendums: Die Einzelheiten und Kontaktinformationen der Parteien sind in Anhang 1 dieses AV-Vertrags enthalten.

Tabelle 2 des UK Addendums: Die Fassung der Approved EU SCCs (wie im UK Addendum definiert), denen das UK Addendum beigefügt ist, sind die EU-Standardvertragsklauseln mit den in Abschnitt 1 dieses Anhangs IV

ausgewählten Modulen und Klauseln. Keine vom Importeur erhaltenen Personenbezogenen Daten werden mit den vom Exporteur erhobenen Personenbezogenen Daten zusammengeführt.

Tabelle 3 des UK Addendums: Die in Tabelle 3 des UK Addendums geforderten Informationen sind in den Anhängen I bis III dieses AV Vertrags enthalten.

Tabelle 4 des UK Addendums: Keine der Parteien darf das UK Addendum beenden, wenn sich das Approved Addendum (wie im UK Addendum definiert) ändert.

j) **Berechtigte Unternehmen in anderen Ländern**. [1]Wenn die Standardvertragsklauseln Drittlandtransfers von Berechtigten Unternehmen ausserhalb des EWR und des Vereinigten Königreichs (z. B. Schweiz) schützen, haben (i) allgemeine und spezifische Verweise in den Standardvertragsklauseln auf die DSGVO oder das Recht der EU oder der Mitgliedstaaten die gleiche Bedeutung wie die entsprechende Bezugnahme im Anwendbaren Datenschutzrecht des Landes, in dem sich das Berechtigte Unternehmen befindet, soweit zutreffend; und ii) Bezugnahmen auf die "zuständige Aufsichtsbehörde" sind als Bezugnahmen auf die zuständige Datenschutzbehörde in diesem Land auszulegen. [2]Das anwendbare Recht, die Wahl des Gerichtsstands und die Gerichtsbarkeit unterliegen den vorstehenden Abschnitten 1 g) und h), sofern die für das jeweilige Berechtigte Unternehmen geltenden Gesetze nichts anderes erfordern, in welchem Fall die Standardvertragsklauseln den Gesetzen des Landes unterliegen, in dem sich das Berechtigten Unternehmen befindet, und alle Verweise auf die zuständigen "Gerichte" sind als Bezugnahmen auf zuständige Gerichte in diesem Land auszulegen.

2. Processor Binding Corporate Rules. Folgendes gilt, wenn eine Übermittlungsgarantie auf Processor Binding Corporate Rules basiert: Der Auftragnehmer verpflichtet den betreffenden UnterAuftragsbearbeiter vertraglich zur Einhaltung der Processor Binding Corporate Rules in Bezug auf die im Rahmen dieses AV-Vertrags Verarbeiteten Personenbezogenen Daten.

3. Zusätzliche Übermittlungsgarantien. Für den Fall, dass eine Übermittlungsgarantie nicht auf Standardvertragsklauseln beruht, gelten die Klauseln 14 und 15 der Standardvertragsklauseln sinngemäss für Drittlandtransfers im Rahmen dieser anderen Übermittlungsgarantie, es sei denn, die jeweilige Übermittlungsgarantie enthält im Wesentlichen die gleichen Rechte und Pflichten in Bezug auf (i) lokale Gesetze und Praktiken, die die Einhaltung der Übermittlungsgarantien beeinflussen, und (ii) Verpflichtungen im Falle des Zugangs durch Behörden gemäss den Klauseln 14 und 15 der Standardvertragsklauseln.

4. Sonstiges. Der Auftragnehmer stimmt zu und versteht, dass das lokale Anwendbare Datenschutzrecht ähnliche oder zusätzliche Beschränkungen von Drittlandtransfers wie jenen in diesem Anhang IV enthalten kann. In diesem Fall verpflichtet sich der Auftragnehmer, angemessene Anstrengungen zu unternehmen und mit Siemens in gutem Glauben zusammenzuarbeiten, um diese Anforderungen zu erfüllen.