Ergänzende Bedingungen für SINEMA Remote Connect as a Service

Diese ergänzenden Bedingungen legen zusätzliche Bedingungen und Konditionen für das Abonnement von SINEMA Remote Connect as a Service gemäß der Dokumentation fest und ändern das Universal Customer Agreement ("**UCA**") zwischen dem Kunden und Siemens ausschließlich in Bezug auf dieses SINEMA Remote Connect as a Service-Angebot. Diese produktspezifischen ergänzenden Bedingungen bilden zusammen mit dem UCA und anderen geltenden ergänzenden Bedingungen die Vereinbarung zwischen den Parteien ("**Vereinbarung**").

1. ALLGEMEIN

1.1. Rangfolge

Im Falle von Widersprüchen zwischen dem Auftrag, dem UCA und diesen produktspezifischen Ergänzungsbedingungen gilt folgende Rangfolge in untergeordneter Reihenfolge:

(i) Bestellung
(ii) Ergänzende Bedingungen für SINEMA Remote Connect as a Service
(iii) Zusätzliche referenzierte Anhänge
(iv) UCA

1.2. Definitionen

Die folgenden zusätzlichen Definitionen gelten für diese SINEMA Remote Connect Service ergänzende Bedingungen:

„Verbundenes Unternehmen“ (**Schwestergesellschaft**) bezeichnet jedes Unternehmen, das den Kunden kontrolliert, von ihm kontrolliert wird oder unter gemeinsamer Kontrolle mit ihm steht; In diesem Zusammenhang bedeutet „Kontrolle“ das direkte oder indirekte Eigentum an der Mehrheit des ausstehenden Eigenkapitals eines Unternehmens.

"Handlungsbevollmächtigter" bedeutet eine Person, die zur Unterstützung des internen Geschäfts des Kunden oder der verbundenen Unternehmen (Schwestergesellschaft) des Kunden als Berater, Vertreter oder Auftragnehmer Zugang zum Angebot benötigt.

"**Autorisierter Benutzer**" bezeichnet alle Mitarbeiter oder Bevollmächtigten des Kunden und seiner verbundenen Unternehmen (Schwestergesellschaft).

"Hochrisiko-System" bezeichnet einen Service-Gegenstand, der erweiterte Sicherheitsfunktionen erfordert oder enthält, wie beispielsweise ausfallsichere oder fehlertolerante Eigenschaften, um einen sicheren Zustand aufrechtzuerhalten. Dabei ist es absehbar, dass ein Versagen des Service-Gegenstandes direkt zum Tod, zu Personenschäden oder zu katastrophalen Sachschäden führen könnte. Hochrisikosysteme können in kritischer Infrastruktur, direkten Gesundheitsunterstützungseinrichtungen, Flugzeugen, Zügen, Booten oder Fahrzeugnavigationssystemen, Luftverkehrskontrolle, Waffensystemen, Kernkraftwerken, Kraftwerken, medizinischen Systemen und Einrichtungen sowie Transporteinrichtungen erforderlich sein.

"**Server**" ist das Gerät, auf dem die SINEMA Remote Connect Management Software läuft.

"**Service-Objekt**" bezeichnet jedes physische Gerät, das in der SINEMA Remote Connect Management Software so konfiguriert ist, dass es Daten an einen autorisierten Benutzer hochlädt oder Daten mit ihm austauscht.

"**SINEMA Remote Connect Client-Software**" ist die Software, die benötigt wird, um einen Windows-basierten Computer mit dem Server zu verbinden.

SINEMA Remote Connect Edge Client Software" ist die erforderliche Software, um eine Verbindung zwischen einem beliebigen EDGE-Gerät und dem Server herzustellen.

"**SINEMA Remote Connect Management-Software**" bezeichnet die im SINEMA Remote Connect enthaltene Software als Leistungsangebot.

"**Gebiet**" ist mit der geografischen Position eines autorisierten Benutzers und mit der geografischen Position eines Serviceartikels verknüpft und gilt weltweit (vorbehaltlich der Verpflichtungen des Kunden aus dem Vertrag zur Einhaltung der Exportkontrollen), es sei denn, in der Bestellung ist ein geografisches Gebiet angegeben.

"**Benutzerkonto**" bezeichnet ein bestimmtes Benutzerkonto, das in der SINEMA Remote Connect Management Software angelegt wird.

"**VPN-Verbindung**" bezeichnet (1) eine VPN-Verbindung zwischen einem Serviceclient und dem Server, die in der SINEMA Remote Connect Management Software vorkonfiguriert ist, und (2) eine VPN-Verbindung zwischen dem Server und einem Benutzerkonto, die in der SINEMA Remote Connect Management Software vorkonfiguriert ist.

2. NUTZUNG DES ANGEBOTS

2.1. Autorisierter Zugriff und Nutzung

Ungeachtet der Abschnitte 3.1 und 3.3 des UCA und sofern in den Berechtigungen nicht anders definiert, kann das SINEMA Remote Connect as a Service-Angebot von autorisierten Benutzern in Übereinstimmung mit den Berechtigungen im Gebiet für die Abonnementlaufzeit ausschließlich für den internen Gebrauch des Kunden oder seiner verbundenen Unternehmen zur Erbringung von Dienstleistungen für Dritte abgerufen und genutzt werden.

2.2. Anspruch

Es stehen verschiedene Optionen des SINEMA Remote Connect as a Service zur Verfügung. Der Kunde ist nur berechtigt, das SINEMA Remote Connect as a Service Angebot entsprechend der Größe zu nutzen, für die der Kunde ein gültiges Abonnement besitzt. Die Kennzahlen in der folgenden Tabelle sind Grenzwerte, die für den gesamten Abonnementzeitraum gelten. Das SINEMA Remote Connect as a Service beinhaltet einen monatlichen Datenverkehr von 100 GB. Wenn ein Kunde diese Datenmenge überschreitet, ist eine separate Vereinbarung zwischen den Vertragsparteien zu treffen.

Optionen	S	M	L
Maximale Anzahl von VPN-Verbindungen	64	256	1024
Maximale Anzahl von SINEMA Remote Connect Client-Software Instanzen	10	32	60
Maximale Anzahl von Sinema Remote Connect Edge Client-Software Instanzen	5	20	50

2.3. Dokumentation.

Die Einzelheiten des SINEMA Remote Connect as a Service Angebots und der Berechtigungen werden in der Dokumentation beschrieben, die unter [https://support.industry.siemens.com/cs/ww/de/view/109823836] verfügbar ist und hierdurch als Referenz in diesem Dokument aufgenommen wird. Die Dokumentation enthält Informationen über geltende Grenzwerte oder Eigenschaften und Kennzahlen der verfügbaren Optionen, Voraussetzungen des SINEMA Remote Connect as a Service sowie zusätzliche Bedingungen von Drittanbietern, die für Drittanbieter-Software, -Technologie, -Daten und andere Materialien gelten, einschließlich Open-Source-Software, die von Dritten lizenziert ist.

2.4. Einschränkungen bei der Nutzung der VPN-Technologie und entsprechende Pflichten des Kunden

Der Kunde erkennt an, dass die Verwendung von VPN-Technologie oder andere Mittel für einen sicheren Remote-Zugriff, Remote-Engineering oder Datenübertragung im Zusammenhang mit der Nutzung des SINEMA Remote Connect as a Service nur dann vom Kunden genutzt werden darf, wenn der Kunde Eigentümer des Systems oder der Daten ist, auf welches durch das SINEMA Remote Connect as a Service zugegriffen wird oder die übertragen werden, oder wenn der Kunde vom Eigentümer solcher Systeme oder Daten rechtlich dazu autorisiert ist, auf diese durch das SINEMA Remote Connect as a Service zuzugreifen oder diese übertragen zu lassen. Der Kunde erkennt weiterhin an, dass die Nutzung des SINEMA Remote Connect as a Service lokalen Beschränkungen oder Verboten unterliegen kann, einschließlich, aber nicht beschränkt auf solche in Bezug auf Verschlüsselung (z.B. Verwendung von Tunneln), Datenvertraulichkeit (z.B. produktionsbezogene Daten) oder grenzüberschreitenden Datenverkehr in bestimmten Ländern. Es liegt in der Verantwortung des Kunden, zu überprüfen, ob solche lokalen Beschränkungen oder Verbote gelten, und das SINEMA Remote Connect as a Service in Übereinstimmung mit geltendem Recht zu nutzen.

3. DATENSCHUTZ

3.1. Anwendbar Bedingungen

SINEMA Remote Connect as a Service finden Sie die zusätzlichen Datenschutzbestimmungen (einschließlich der Liste der Unterauftragsverarbeiter) unter

https://www.siemens.com/global/en/company/about/compliance/dataprivacy/dataprivacyterms/di-subprocessors.html.

3.2. Standort von Rechenzentren

Gespeicherte Kundeninhalte (Data at Rest) werden innerhalb der Europäischen Union gespeichert.

4. ABONNEMENTBEDINGUNGEN/VERLÄNGERUNGEN

Die Laufzeit des Abonnements für SINEMA Remote as a Service beträgt 12 Monate. Die Abonnementbedingungen enden automatisch.

5. SERVICE-LEVEL

5.1. Service-Level

Siemens wird wirtschaftlich vertretbare Anstrengungen unternehmen, um das SINEMA Remote Connect as a Service dem Kunden bis zu 24 Stunden am Tag und 7 Tage die Woche zur Verfügung zu stellen, mit Ausnahme von Ausfallzeiten, die sich direkt oder indirekt aus den SLA-Ausschlüssen ergeben. Die Cloud-Services stehen dem Kunden zur Verfügung, wenn deren Benutzeroberfläche durch Login am Ausgang des Wide Area Network des Rechenzentrums, das von Siemens zur Bereitstellung des SINEMA Remote Connect a Service genutzt wird, erreichbar ist.

5.2. Service-Level-Ausschlüsse ("SLA-Ausschlüsse")

Service-Level-Verpflichtungen schließen Ausfallzeiten aus, die sich direkt oder indirekt aus SLA-Ausschlüssen ergeben. "SLA-Ausschlüsse" bezeichnet die Nichtverfügbarkeit oder ein anderes Leistungsproblem, das zu Ausfallzeiten der Cloud-Dienste führt, und zwar aufgrund von:

(i) geplante und kommunizierte Wartung;
(ii) Ausfallzeiten, für die der Kunde mindestens 24 Stunden im Voraus informiert wird;
(iii) Faktoren, die außerhalb der angemessenen Kontrolle von Siemens liegen;
(iv) Handlungen oder Unterlassungen des Kunden oder Dritter;
(v) Geräte, Software oder andere Technologien, die nicht von Siemens zur Verfügung gestellt werden; oder
(vi) Aussetzung oder Beendigung des Angebots gemäß der Vereinbarung

5.3. Voraussetzungen und Zeitplan für die Bereitstellung von Updates

Der Kunde wird von Siemens per E-Mail an die vom Kunden bereitgestellte E-Mail-Adresse darüber informiert, dass ein neues Update für die SINEMA Remote Connect Management Software verfügbar ist. In der Benachrichtigung werden mindestens zwei mögliche Wartungsfenster mitgeteilt, in denen das Update von Siemens durchgeführt werden kann. Der Kunde kann eines dieser Fenster auswählen. Wenn der Kunde nicht auf die Anfrage reagiert, wird das Update der SINEMA Remote Connect Management Software im letzten angebotenen Wartungsfenster von Siemens durchgeführt. Die möglichen Wartungsfenster werden mindestens eine Woche im Voraus mitgeteilt.

Im Falle eines sicherheitskritischen Updates, das sofortige Maßnahmen erfordert, kann das Update der SINEMA Remote Connect Management Software von Siemens nach einer Vorankündigung von 24 Stunden gemäß Absatz 5.2 (ii) durchgeführt werden.

Der Kunde hat auch die Möglichkeit, das Update der SINEMA Remote Connect Management Software jederzeit vor dem letzten angebotenen Wartungsfenster selbst durchzuführen. Eine Anleitung zum Durchführen des Updates wird von Siemens bereitgestellt, z.B. über das Siemens Industry Online Support-Portal.

Nach erfolgreichem Update wird der Kunde per E-Mail informiert.

Voraussetzungen:

Der Kunde muss im Bestellprozess des SINEMA Remote Connect as a Service-Angebots aktuelle E-Mail-Adressinformationen angeben. Der Kunde muss Siemens über etwaige Änderungen dieser Informationen informieren.

5.4. Backup-Funktionen

Backups der Serverinstanz werden von Siemens zyklisch einmal pro Woche sowie vor einem Update der SINEMA Remote Connect Management-Software erstellt. Die Backups werden für einen Zeitraum von drei Monaten aufbewahrt.

Die interne Backup-Funktionalität der SINEMA Remote Connect Management Software kann vom Kunden genutzt werden, um eigene Backups zu erstellen. Die Einstellungen im Menü "Sichern & Wiederherstellen" dürfen jedoch nicht geändert werden. Dazu gehören "Maximale Anzahl lokaler Sicherungskopien", "Automatisches Sicherungsintervall" und "Kodierungsschlüssel". Der konfigurierte Kodier Schlüssel wird von Siemens verschlüsselt gespeichert und initial an den Kunden ausgeliefert.

6. TECHNISCHER SUPPORT

6.1. Kontakt

Der Kunde kann sich an den technischen Support von Siemens als primären Ansprechpartner für Support in Bezug auf das Angebot wenden. Alle Support-Anfragen müssen wie folgt gestellt werden:

https://support.industry.siemens.com/cs/my/src

6.2. Umfang des technischen Supports

Je nach Verfügbarkeit bietet Siemens von Montag bis Freitag von 8:00 bis 17:00 Uhr (MEZ, MESZ) technische Support Services an, ausgenommen sind nationale und lokale Feiertage in Deutschland. Siemens beantwortet Supportanfragen des Kunden nach eigenem Ermessen per E-Mail, Hotline oder

per Fernzugriff, wie in diesem Absatz beschrieben. Der Kunde muss sicherstellen, dass der Fernzugriff auf seine lokalen Netzwerke / Anlagen möglich ist, z.B. für Ferndiagnosen.

Die folgenden Arten von Problemfällen sind nicht im Umfang des Supports enthalten, aber der Kunde kann für solche Anfragen das Vertriebsteam einbinden, um eine Lösung zu finden

- Vorfälle in Bezug auf eine Version, Version und/oder Funktionalitäten eines Dienstes, die speziell für den Kunden entwickelt oder konfiguriert wurde (sofern nicht ausdrücklich in einer Bestellung anders angegeben);
- Vorfälle, die einer Beratungs- oder Schulungsanfrage zugeschrieben werden ("How-to"). Diese werden in der Online-Benutzerdokumentation behandelt;
- Vorfälle, die einer benutzerdefinierten Entwicklungsanfrage zugeordnet sind.

Der technische Support ist in deutscher und englischer Sprache verfügbar.

Um Supportleistungen im Rahmen dieser Vereinbarung zu erhalten, muss der Kunde in angemessener Weise mit dem Siemens-Support zusammenarbeiten, um Supportfälle zu lösen. Der Kunde muss über ausreichende technische Fachkenntnisse und Kenntnisse seiner Konfigurationen verfügen, um relevante Informationen bereitzustellen, die es dem Siemens-Support ermöglichen, den aufgetretenen Fehler zu reproduzieren, zu diagnostizieren und zu beheben, wie z. B. Instanzname, Benutzername, Formularname und Screenshot. Solche Support-Dienstleistungen können erfordern, dass Siemens Zugriff auf Kundeninhalte erhält. In diesem Fall muss der Kunde Siemens temporäre Zugangsdaten ausstellen, um diesen Zugriff zu ermöglichen. Standardmäßig wird ein dedizierter Service-Account zu diesem Zweck erstellt.

7. NOTIZEN

Abweichend von Ziffer 13.7 UCA sind Mitteilungen an Siemens zu richten an:

sinemarc.aas.industry@siemens.com

8. VERBOTENE VERWENDUNG MIT HOHEM RISIKO

Der Kunde erkennt an und stimmt zu, dass (i) die SINEMA Remote Connect as a Service-Angebote nicht für den Betrieb eines Hochrisikosystems verwendet werden sollten, wenn die Funktionsfähigkeit des Hochrisikosystems von der ordnungsgemäßen Funktion des SINEMA Remote Connect as a Service-Angebots abhängt, und (ii) das Ergebnis jeglicher Datenverarbeitung durch die Verwendung des SINEMA Remote Connect as a Service-Angebots außerhalb der Kontrolle von Siemens liegt. Der Kunde wird Siemens, seine verbundenen Unternehmen (Schwestergesellschaften), seine Unterauftragnehmer und deren Vertreter von jeglichen Ansprüchen, Schäden, Geldbußen und Kosten (einschließlich Anwaltsgebühren und Auslagen) in Bezug auf die Verwendung eines SINEMA Remote Connect as a Service-Angebots für den Betrieb eines Hochrisikosystems freistellen.

9. IT-SICHERHEIT

Sofern in der Dokumentation nichts anderes festgelegt ist, gelten folgende Bestimmungen in Bezug auf die Sicherheit: Siemens unterhält ein formelles Sicherheitsprogramm, das entwickelt wurde, um Bedrohungen oder Gefahren für die Sicherheit von Kundendaten zu schützen. Die Anbieter von Siemens Cloud-Infrastruktur sind verpflichtet, (i) ein Sicherheitsprogramm zu implementieren und aufrechtzuerhalten, das unter anderem den Anforderungen der ISO 27001 oder einer Nachfolgenorm entspricht, die im Wesentlichen gleichwertige Risikomanagement- und Sicherheitskontrollen wie die ISO 27001-Zertifizierung der Anbieter bietet, und (ii) die Angemessenheit ihrer Sicherheitsmaßnahmen jährlich von unabhängigen Prüfern überprüfen zu lassen. Die Cloud-Infrastruktur von Siemens (i) verwendet Firewalls, Anti-Malware, Intrusion Detection/Prevention-Systeme (IDS/IPS) und entsprechende Managementprozesse zum Schutz der Servicebereitstellung vor Malware und (ii) wird nach einem Sicherheits-Governance-Modell betrieben, das auf ISO 27001 ausgerichtet ist. Dieser Abschnitt enthält die gesamte Verpflichtung von Siemens in Bezug auf die Sicherheit von Kundendaten und der Cloud-Infrastruktur für das Angebot SINEMA Remote Connect as a Service.

10. HAFTUNGSAUSSCHLUSS

Um Umstände oder Ereignisse zu vermeiden, die potenziell nachteilige Auswirkungen auf die Anlagen, Systeme, Maschinen und Netzwerke des Kunden und/oder seiner verbundenen Unternehmen durch unbefugten Zugriff, Zerstörung, Offenlegung und/oder Veränderung von Informationen, Denial-of-Service-Angriffe oder vergleichbare Szenarien (sogenannte "Cyberbedrohungen") haben können, ist es notwendig, ein ganzheitliches, hochmodernes Konzept für die industrielle Sicherheit zu implementieren und kontinuierlich aufrechtzuerhalten. Obwohl die Industrial Edge-Angebote mit Sicherheitsfunktionen entwickelt wurden, die sichere industrielle Abläufe unterstützen, stellen Siemens' Produkte und Lösungen nur ein Element eines solchen Konzepts dar, und es obliegt dem Kunden und seinen verbundenen Unternehmen (Schwestergesellschaften), diese Funktionen zu konfigurieren. Folglich bleibt der Kunde und seine verbundenen Unternehmen (Schwestergesellschaften) dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern, und Siemens lehnt jede Haftung für Schäden ab, die aus solchen Cyberbedrohungen resultieren, soweit dies gesetzlich zulässig ist. Solche Systeme, Maschinen und Komponenten sollten nur einmal im Monat mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, um Updates zu erhalten, jedoch nur, wenn angemessene Sicherheitsmaßnahmen (z. B. Firewalls und/oder Netzwerksegmentierung) vorhanden sind. Der Kunde und seine verbundenen Unternehmen werden darauf hingewiesen, Siemens' Anleitung zu angemessenen Sicherheitsmaßnahmen zu berücksichtigen, die unter https://www.siemens.com/industrialsecurity zu finden sind. In diesem Zusammenhang sollten Updates für die Angebote so bald wie möglich angewendet werden, und die neueste Version des Angebots sollte verwendet werden, da die Verwendung nicht mehr unterstützter Versionen und das Versäumnis, Updates anzuwenden, das Risiko von Cyberbedrohungen erhöhen können.