Cybersecurity Bedingungen – Deutschland Healthcare

Mit Wirkung vom 15. Dezember 2020

1 Definitionen und Geltungsbereich

1.1 Geltungsbereich dieser Bedingungen

Diese Bedingungen gelten zwischen dem Kunden und der im Vertrag genannten Siemens Healthineers Geschäftseinheit („Siemens Healthineers“). Sie dienen ggf. der Ergänzung der „Allgemeinen Lieferbedingungen – Deutschland, Healthcare“ und haben im Falle eines Konflikts Vorrang.

1.2 Definitionen

„Produkt(e)” steht für Produkte und Lösungen bestehend aus Hardware und/oder Software, welche Siemens Healthineers dem Kunden verkauft, lizensiert oder anderweitig übermittelt, ungeachtet dessen, ob der Hersteller Siemens Healthineers selbst ist oder ein Drittanbieter. Die Übermittlung umfasst jedoch nicht die Vermittlung von entsprechenden Transaktionen zwischen dem Kunden und einem Dritten, wie die Vermittlung von Dritt-Apps auf dem Siemens Heathineers Digital Ecosystem oder anderen Siemens Healthineers Plattformen.

„SRS” steht für Smart Remote Services, d. h. eine online Verbindung zwischen Siemens Healthineers und dem entsprechenden Produkt beim Kunden, welche eine elektronische Fernübermittlung von Software-Updates und Patches erlaubt.

„IT-Sicherheit“ steht für den Schutz des durchgehenden Betriebs der Produkte vor Störungen durch ausgenutzte Vulnerabilitäten und die Verfügbarkeit, die Vertraulichkeit und die Integrität von Daten und Informationen.

„Cyberbedrohung“ steht für Umstände oder Ereignisse, welche die Möglichkeit schaffen, ein Produkt durch unautorisierten Zugriff, Zerstörung, durch Weitergabe oder Veränderung von Information, und/oder durch einen „Denial of Service“-Angriff zu beeinträchtigen.

„Vulnerabilität“ steht für die Sicherheitslücke eines Produktes, welche durch eine Cyberbedrohung ausgenutzt werden könnte.

„Irrelevant“ kategorisiert eine Vulnerabilität, deren Ausnutzung unter Berücksichtigung der individuellen Produkteigenschaften und/oder der jeweiligen Systemumgebung nicht zu erwarten ist und/oder keine messbare Beeinträchtigung der IT-Sicherheit erwarten lässt.

„Patch“ steht für ein Software-Update, welches eine Vulnerabilität des Produkts behebt.

„EoS“ steht für das Ende des Supports, d. h. das von Siemens Healthineers dem Kunden mitgeteilte Datum, mit dessen Ablauf Ersatzteile und sonstige Dienstleistungen für das Produkt nicht mehr verfügbar sind oder ggf. zuvor für seine Software-Bestandteile die Unterstützung endet.

1.3 Regelungszweck

Diese Bedingungen zielen darauf ab, einen gerechten Ausgleich zwischen den Mitwirkungspflichten des Kunden sowie den Verpflichtungen von Siemens Healthineers im Hinblick auf einen angemessenen Umgang mit Cyberbedrohungen zu schaffen.

2 Siemens Healthineers‘ Serviceleistung bis EoS

2.1 Soweit nicht gesetzlich zwingend etwas anderes vorgeschrieben ist, gilt Folgendes:

(i) Sofern die Bereitstellung von Patches vertraglich vereinbart wurde, stellt Siemens Healthineers Patches nach Maßgabe der nachfolgenden Regelungen für die vereinbarte Dauer, andernfalls bis EoS, längstens jedoch für 10 Jahre nach Lieferung des betreffenden Produkts zur Verfügung. Dies setzt voraus, dass

2.1.2 Siemens Healthineers von einer Vulnerabilität Kenntnis erlangt, die Siemens Healthineers nicht als Irrelevant einstuft,

2.1.3 die Produktversion des Kunden zum gegebenen Zeitpunkt die neueste oder zumindest die vorletzte Version gemäß Abschnitt 3.4 ist, und

2.1.4 im Falle der Software eines Drittanbieters dieser einen entsprechenden Patch herausbringt und Siemens Healthineers zur Verfügung stellt; Siemens Healthineers ist nicht dafür verantwortlich sicherzustellen, dass der Drittanbieter einen Patch herausbringt oder dies zukünftig tut.

(i) Die Zurverfügungstellung durch Siemens Healthineers nach Abschnitt 2.1.1 erfolgt innerhalb eines angemessenen Zeitraums, der es Siemens Healthineers erlaubt, die erforderlichen Tests und Validierungen durchzuführen. Im Falle von Software von Drittanbietern beginnt dieser Zeitraum nach Erhalt des jeweiligen Patches durch Siemens Healthineers von dem betreffenden Drittanbieter. Je nach Schweregrad der Vulnerabilität behält sich Siemens Healthineers vor, den Patch zum Zeitpunkt und im Rahmen eines Routine Updates zur Verfügung zu stellen.

(ii) Wenn das Produkt SRS kompatibel ist und der Kunde den Fernbezug des Patches über SRS ermöglicht oder wenn Siemens Healthineers den Patch über teamplay Fleet[1] zum Download zur Verfügung stellt und der Kunde einen teamplay Fleet Account eröffnet hat, fällt kein Installationsentgelt an. Andernfalls, wenn der Patch vor Ort durch oder im Auftrag von Siemens Healthineers installiert werden muss, ist Siemens Healthineers berechtigt, dem Kunden die durch die Installation entstehenden Kosten in Rechnung stellen.

2.2 Wartungsverträge

(i) Für Produkte, welche von einem gültigen Wartungsvertrag umfasst sind, gelten Abschnitt 2.1.1 bis 2.1.2 entsprechend.

(ii) Im Falle eines Konflikts gehen die Bedingungen des Wartungsvertrages vor. Die Installation von Patches durch Siemens Healthineers ist jedoch nicht Bestandteil des Vertragsumfangs, es sei denn, dass dies ausdrücklich schriftlich vereinbart wurde.

3 Mitwirkungspflichten des Kunden

3.1 Zum Schutz der Produkte vor Cyberbedrohungen ist es erforderlich, dass der Kunde ein ganzheitliches, dem Stand der Technik entsprechendes Sicherheitskonzept für seine IT-Infrastruktur implementiert und kontinuierlich aufrechterhält, einschließlich regelmäßiger Scans auf etwaige Vulnerabilitäten, jedoch unter der Voraussetzung dass

3.1.1 während des klinischen Einsatzes keine Scans oder Tests durchgeführt werden dürfen,

3.1.2 die Systemkonfiguration und/oder die IT-Sicherheitseinrichtungen des Produkts nicht verändert werden darf, und

3.1.3 der Kunde, falls er während der Bereitstellung des Produktes eine Vulnerabilität feststellt, sich mit Siemens Healthineers hinsichtlich des Schweregrads der Vulnerabilität unter Berücksichtigung der individuellen Produkteigenschaften und der geplanten Systemumgebung abstimmt. Der Kunde darf die Annahme des Produktes nicht verweigern, wenn Siemens Healthineers die Vulnerabilität als Irrelevant einstuft.

3.2 Der Kunde ist dafür verantwortlich, einen unbefugten Zugriff auf die Produkte zu verhindern, indem er z.B. Passwörter ändert und andere

[1] In den meisten Ländern ab Oktober 2018 verfügbar

Schutzeinstellungen von ihren Standardeinstellungen auf individuelle Werte umstellt. Die Produkte dürfen nur dann mit dem Kundennetzwerk oder dem Internet verbunden werden, wenn und soweit Siemens Healthineers die Verbindung in der Gebrauchsanweisung gestattet hat und der Kunde geeignete Sicherheitsmaßnahmen (wie z.B. Firewalls, Netzwerk-Client-Authentifizierung und/oder Netzwerk-Segmentierung) getroffen hat.

3.3 USB-Speichermedien und andere Wechseldatenträger dürfen nur dann an Produkte angeschlossen werden, wenn und soweit Siemens Healthineers dies in der Gebrauchsanweisung gestattet hat und das Risiko eines Befalls mit Schadsoftware durch Virenscanner oder andere geeignete Mittel minimiert ist.

3.4 Die Produkte werden einer stetigen Weiterentwicklung unterzogen, um deren IT-Sicherheit weiter zu erhöhen. Siemens Healthineers empfiehlt ausdrücklich die Implementierung von Produkt Updates, sobald diese verfügbar sind, sowie die Verwendung der aktuellen Produkt-Version durch den Kunden. Letzteres kann auch den Kauf von Upgrades von Hard- und Software durch den Kunden beinhalten. Der Einsatz von Produktversionen, welche nicht länger unterstützt werden, sowie die Nichtverwendung der aktuellsten Updates/Upgrades können ein erhöhtes Risiko von Cyberbedrohungen für den Kunden zur Folge haben.

3.5 Der Kunde unterrichtet Siemens Healthineers unverzüglich über mutmaßliche oder nachweisliche Vulnerabilitäten des Produkts oder diesbezügliche Vorfälle. Die Weitergabe solcher Informationen an Dritte bedarf der vorherigen Zustimmung von Siemens Healthineers.

3.6 Im Falle des Weiterverkaufs des Produkts teilt der Kunde Siemens Healthineers schriftlich den Namen und die Anschrift des neuen Eigentümers mit und wird diesem eine entsprechende Verpflichtung für den Fall weiterer Veräußerungen auferlegen.

3.7 Der Kunde hat Patches, die Siemens Healthineers via SRS übermittelt oder via teamplay Fleet zum Download zur Verfügung stellt, unverzüglich gemäß der entsprechenden Installationsanleitung von Siemens Healthineers zu installieren. Andernfalls hat der Kunde die Installation der Patches gemäß Abschnitt 2.1.3 Satz 2 zu dulden, unabhängig davon, ob der Patch auf Basis vertraglicher oder gesetzlicher Bestimmungen oder freiwillig zur Verfügung gestellt wird.

3.8 Um einen Zugang zum teamplay Fleet sowie zu den zum Download zur Verfügung gestellten Patches zu erhalten, hat sich der Kunde zu registrieren und diese Registrierung für die Dauer seiner Produktnutzung aufrechtzuerhalten.

4 Haftung

4.1 Soweit nichts anderes schriftlich vereinbart wurde, sind jegliche Schadensersatzansprüche des Kunden aus oder in Zusammenhang mit Cyberbedrohungen wie z.B. wegen Datenverlust, Ausfallzeit, Betriebsstörung, entgangenem Gewinn, Kosten für die Neukonfiguration von Produkten oder die Wiederherstellung von Daten, gleich aus welchem Rechtsgrund, ausgeschlossen. Insbesondere übernimmt Siemens Healthineers keinerlei Haftung für Schäden, die verursacht werden durch

4.1.1 intrusive Sicherheitstests durch Kunden,

4.1.2 eine unbefugte Änderung der Systemkonfiguration oder der IT-Sicherheitseinrichtungen des Produkts,

4.1.3 die Installation von Patches, welche nicht von Siemens Healthineers autorisiert wurden, oder

4.1.4 die kundenseitige Verzögerung der Installation von Patches, die von Siemens Healthineers via SRS übermittelt oder via teamplay Fleet zum Download zur Verfügung gestellt wurden.

4.2 Dies gilt nicht, soweit zwingend gehaftet wird, z.B. nach dem Produkthaftungsgesetz, in Fällen des Vorsatzes, der groben Fahrlässigkeit, wegen der Verletzung des Lebens, des Körpers oder der Gesundheit, wegen einer Übernahme der Garantie für die Beschaffenheit einer Sache oder wegen der Verletzung wesentlicher Vertragspflichten. Der Schadensersatzanspruch für die Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegt, oder wegen der Verletzung des Lebens, des Körpers oder der Gesundheit gehaftet wird.

4.3 Eine Änderung der Beweislast zum Nachteil des Kunden ist mit den vorstehenden Regelungen nicht verbunden.

5 Abschließende Rechte

5.1 Die vorstehenden Verpflichtungen von Siemens Healthineers gemäß den Abschnitten 2 und 4 sind abschließend. Soweit nicht ausdrücklich anderweitig schriftlich vereinbart, sind weitergehende Ansprüche des Kunden aus oder in Zusammenhang mit Cyberbedrohungen ausgeschlossen.

5.2 Auf Wunsch des Kunden ist Siemens Healthineers bereit, bei der etwaigen Neukonfiguration der Produkte gegen Kostenerstattung zuzüglich eines angemessenen Gewinns Unterstützung zu leisten.

6 Änderungen der Bedingungen und des IT-Sicherheitskonzepts

6.1 Siemens Healthineers behält sich das Recht vor, diese Cybersecurity Bedingungen an den technischen Fortschritt, Gesetzesänderungen und an die Weiterentwicklungen der Siemens Healthineers-Angebote sowie an andere unvorhersehbare Umstände anzupassen.

6.2 Solche Änderungen dürfen nicht zu einer unangemessenen Schlechterstellung des Kunden führen.

6.3 Siemens Healthineers wird den Kunden schriftlich unter Einhaltung einer angemessenen Frist von mindestens 28 Kalendertagen über Änderungen dieser Cybersecurity Bedingungen informieren mit dem Hinweis, dass die Änderungen von dem Kunden als akzeptiert gelten, wenn der Kunde innerhalb der vorgenannten Frist keinen Widerspruch erhebt. Mit Ablauf der Frist werden die Änderungen wirksam, falls der Kunde bis zum Ablauf der Frist keinen Widerspruch erhoben hat