VEREINBARUNG ZUR DATENVERARBEITUNG

Diese Vereinbarung zur Datenverarbeitung (die „Vereinbarung“) wird abgeschlossen zwischen der Siemens Product Lifecycle Management Software Inc., auch bekannt als Siemens Industry Software (im Folgenden als „SISW“ bezeichnet) und dem diese Vereinbarung akzeptierenden Kunden („Kunde“). SISW behält sich das Recht vor, ihre Rechte und Pflichten unter dieser Vereinbarung von ihren verbundenen Unternehmen wahrnehmen zu lassen. Daher bezieht sich der hier verwendete Begriff „SISW“ auch auf die verbundenen Unternehmen, die sich direkt oder indirekt im Besitz der Konzernmuttergesellschaft von Siemens Product Lifecycle Management Software Inc. befinden oder von dieser kontrolliert werden und von Siemens Product Lifecycle Management Software Inc. zur Durchführung von SISW-Cloud-Services (der „Cloud-Service“) autorisiert sind.

Der Kunde bestimmt alleinverantwortlich, welche Art von Daten und welche Personen die Verarbeitung betrifft, und stellt die Rechtmäßigkeit dieser Verarbeitung im Rahmen des Cloud-Service sicher. Darüber hinaus ist der Kunde verantwortlich für die Berichtigung, Löschung oder Sperrung personenbezogener Daten mit den Funktionen des Cloud-Service. Der Kunde kann seine Daten einschließlich personenbezogener Daten mit den Funktionen des Cloud-Service exportieren und löschen. Im Falle des Rücktritts von dieser Vereinbarung zur Datenverarbeitung kann der Kunde SISW binnen 30 Tagen schriftlich ersuchen, ihm die Kundendaten zum Herunterladen bereitzustellen. Nach Ablauf einer Frist, die SISW auf dieses Ersuchen hin festlegt, werden die verbleibenden Kundendaten gelöscht und stehen dem Kunden nicht mehr zur Verfügung. SISW und der Kunde vereinbaren, dass das Recht des Kunden auf Erteilung von Anweisungen im Geltungsbereich des Cloud-Service ausschließlich auf die im Rahmen des Cloud-Service bereitgestellten Funktionen beschränkt ist. Weitere Anweisungen in Bezug auf die Daten des Kunden bedürfen einer separaten, schriftlichen Vereinbarung zwischen SISW und dem Kunden, die auch eine Vereinbarung über die zusätzlichen Gebühren, die vom Kunden für die Ausführung dieser Anweisungen zu zahlen sind, beinhaltet. Der Kunde versichert, dass er den Cloud-Service nicht zum Hochladen geschützter Informationen über den Gesundheitszustand nutzt, es sei denn, die Speicherung solcher Informationen im Rahmen des Cloud-Service wird in einer separaten, von SISW und dem Kunde abgeschlossenen schriftlichen Vereinbarung ausdrücklich erlaubt.

Bei der Bereitstellung des Cloud-Service erfüllt SISW hinsichtlich des Produktionssystems die in Anlage A, Anhang 2 zu dieser Vereinbarung zur Datenverarbeitung beschriebenen technischen und organisatorischen Maßnahmen. Im Zusammenhang mit dem Cloud-Service stehende Systeme außerhalb der Produktionsumgebung können die in Anlage A, Anhang 2 zu dieser Vereinbarung zur Datenverarbeitung beschriebenen technischen und organisatorischen Maßnahmen erfüllen. SISW kann die auf das Produktionssystem anwendbaren technischen und organisatorischen Maßnahmen nach Bedarf unter der Voraussetzung ändern, dass diese Änderungen das von diesen Maßnahmen gebotene Schutzniveau nicht wesentlich beeinträchtigen. SISW untersagt die unberechtigte Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch ihre Mitarbeiter ein und setzt nur Mitarbeiter, die auf die Einhaltung des Datenschutzes besonders hingewiesen wurden, für die Verarbeitung der personenbezogenen Daten des Kunden ein.

SISW ist berechtigt, Unterauftragsverarbeiter in die Durchführung des Cloud-Service einzubeziehen. Soweit der Zugriff von Unterauftragsverarbeitern auf personenbezogene Daten des Kunden nicht ausgeschlossen werden kann, legt SISW dem Kunden auf Anforderung eine Liste vor, in der die Unterauftragsverarbeiter und deren Standorte verzeichnet sind. SISW aktualisiert diese Liste nach Bedarf, bevor einem neuen Unterauftragsverarbeiter Zugriff auf die personenbezogenen Daten des Kunden gewährt wird. Der Kunde setzt SISW in Kenntnis, wenn er begründete Einwände gegen einen neuen Unterauftragsverarbeiter hat. Besteht SISW auf dem neuen Unterauftragsverarbeiter, kann der Kunde aus wichtigem Grund von dieser Vereinbarung zur Datenverarbeitung zurücktreten. Soweit mit der Beauftragung eines solchen Unterauftragsverarbeiters die grenzüberschreitende Übermittlung personenbezogener Daten verbunden ist, bemüht sich SISW um Gewährleistung eines angemessenen Schutzniveaus in Bezug auf diese personenbezogenen Daten seitens des Unterauftragsverarbeiters.

SISW prüft regelmäßig, ob die anwendbaren technischen und organisatorischen Maßnahmen eingehalten werden, und bestätigt dem Kunden auf dessen begründetes Ersuchen, dass die anwendbaren technischen und organisatorischen Maßnahmen eingehalten werden. Hat der Kunde Grund zu der Annahme, dass die Bestätigung seitens SISW nicht den Tatsachen entspricht, kann der Kunde nach rechtzeitiger vorheriger Ankündigung bei SISW prüfen, ob die technischen und organisatorischen Maßnahmen eingehalten werden. Die Kosten für die Durchführung einer solchen Prüfung trägt der Kunde.

SISW und der Kunde vereinbaren, dass die Übermittlung von personenbezogenen Daten des Kunden aus Ländern der Europäischen Union (EU) in Länder außerhalb der EU, in denen personenbezogene Daten nach Auffassung der EU nicht ausreichend geschützt sind, in Einklang mit den Bestimmungen der EU-Standardvertragsklauseln in Anlage A, die Bestandteil diese Vereinbarung sind, erfolgt. Im Falle eines Widerspruchs zwischen den Bestimmungen dieser Vereinbarung zur Datenverarbeitung und den Bestimmungen der Standardvertragsklauseln haben die Bestimmungen der

Standardvertragsklauseln Vorrang. Die Standardvertragsklauseln unterliegen dem Recht des EU-Mitgliedstaats, in dem der Datenexporteur (gemäß der Definition in Anlage A) niedergelassen ist.

Anlage A
EU-STANDARDVERTRAGSKLAUSELN

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

durch und zwischen

Der Kunde und/oder ein verbundenes Unternehmen des Kunden mit Sitz in der EU

(im Folgenden als „**Datenexporteur**“ bezeichnet)

und

Siemens Product Lifecycle Management Software Inc. bzw. Siemens Industry Software sowie verbundene Unternehmen, die sich direkt oder indirekt im Besitz der Konzernmuttergesellschaft von Siemens Product Lifecycle Management Software Inc. befinden oder von dieser kontrolliert werden und von Siemens Product Lifecycle Management Software Inc. zur Durchführung von Datenverarbeitungsleistungen in deren Auftrag autorisiert sind

(im Folgenden als „**Datenimporteur**“ bezeichnet)

(die „Partei“, wenn eine dieser Organisationen gemeint ist, die „Parteien“, wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln“), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Abschnitt 1. Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

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

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

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

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

(e) der Begriff „anwendbares Datenschutzrecht“ bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung

personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

(f) der Ausdruck „technische und organisatorische Sicherheitsmaßnahmen“ bezeichnet Maßnahmen zum Schutz personenbezogener Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung.

Abschnitt 2. Einzelheiten der Übermittlung

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

Abschnitt 3. Drittbegünstigtenklausel

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

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

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

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

Abschnitt 4. Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

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

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

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

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

(e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

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

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

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

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

(j) er für die Einhaltung des Abschnitts 4 Buchstaben (a) bis (i) sorgt.

Abschnitt 5. Pflichten des Datenimporteurs

Der Datenimporteur erklärt sich bereit und garantiert, dass:

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

(b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Abschnitte bieten sollen, dem

Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

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

(d) er den Datenexporteur unverzüglich informiert über

(i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;
(ii) jeden zufälligen oder unberechtigten Zugang und
(iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

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

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

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

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

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

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

Abschnitt 6. Haftung

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

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Abschnitte 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person

Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

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

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

Abschnitt 7. Schlichtungsverfahren und Gerichtsstand

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

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

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

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

Abschnitt 8. Zusammenarbeit mit Kontrollstellen

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

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

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

Abschnitt 9. Anwendbares Recht

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

Abschnitt 10. Änderung des Vertrags

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

Abschnitt 11. Vergabe eines Unterauftrags

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

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

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

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

Abschnitt 12. Pflichten nach Beendigung der Datenverarbeitungsdienste

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

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

ANHANG 1 ZU DEN STANDARDVERTRAGSKLAUSELN

Datenexporteur
Der Datenexporteur ist (bitte erläutern Sie kurz Ihre Tätigkeiten, die für die Übermittlung von Belang sind):

Der Kunde ist Abonnent eines von SISW bereitgestellten Cloud-Service, der es den vom Kunden autorisierten Endbenutzern gestattet, Kundendaten einzugeben, zu ändern, zu verwenden, zu entfernen, herunterzuladen und auf andere Art zu verarbeiten. Diese Kundendaten können personenbezogene Daten gemäß der Beschreibung in der Vereinbarung und in der relevanten Dokumentation für den Cloud-Service beinhalten.

Datenimporteur
Der Datenimporteur ist (bitte erläutern Sie kurz die Tätigkeiten, die für die Übermittlung von Belang sind):

Siemens Product Lifecycle Management Software Inc. stellt selbst und/oder über ihre Unterauftragsverarbeiter den Cloud-Service bereit, der Folgendes umfasst: Unterhalt der Recheninfrastruktur, auf der der Cloud-Service betrieben wird, in den USA und in der Europäischen Union, Speicherung der vom Kunden in den Cloud-Service hochgeladenen Kundendaten in der Infrastruktur, Überwachung der Verfügbarkeit und des laufenden Betriebs des Cloud-Service und der Infrastruktur sowie Gewährleistung der Sicherheit der Infrastruktur gemäß der Vereinbarung und der relevanten Dokumentation für den Cloud-Service.

Betroffene Personen
Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen (bitte genau angeben):

Sofern vom Datenexporteur nicht ausdrücklich schriftlich anders festgelegt, kann die Gruppe der betroffenen Personen Endbenutzer umfassen, die vom Kunden zur Nutzung des Cloud-Service autorisiert wurden, sowie andere Mitarbeiter des Kunden, deren personenbezogene Daten im Cloud-Service gespeichert sind.

Kategorien von Daten
Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):

Die spezifischen, im Cloud-Service zu speichernden Datenkategorien, werden weitgehend vom Kunden konfiguriert. Die folgenden Beispiele für allgemeine Kategorien von Daten, die im Cloud-Service gespeichert werden können, sind daher als nicht erschöpfende Liste zu verstehen: Name, E-Mail-Adresse, Name des Unternehmens, Telefonnummer, Arbeitsort, Staatsangehörigkeit oder Nationalität und Informationen betreffenden den Zugang zum und die Nutzung des Cloud-Service. Je nachdem, wie der Cloud-Service vom Kunden konfiguriert wird, können die Kundendaten zahlreiche weitere Datenkategorien umfassen.

Besondere Datenkategorien (falls zutreffend)
Die übermittelten personenbezogenen Daten umfassen folgende besondere Datenkategorien (bitte genau angeben):

Besondere, im Cloud-Service zu speichernde Datenkategorien werden von den an der Vereinbarung oder einem Auftrag beteiligten Parteien oder in einer Leistungsbeschreibung der professionellen Services, die dem Kunden im Rahmen seiner Implementierung des Cloud-Service bereitzustellen sind, festgelegt.

Verarbeitung
Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen (bitte genau angeben):

Die personenbezogenen Daten können wie folgt verarbeitet werden: im Rahmen des regulären Betriebs des Cloud-Service entsprechend der Konfiguration des Kunden, durch Speicherung und/oder Archivierung in der vom Datenexporteur unterhaltenen Recheninfrastruktur, in Einzel- oder Mehrmandantenumgebungen, durch Zugriff oder Übermittlung seitens eines vom Kunden zur Nutzung des Cloud-Service autorisierten Endbenutzers gemäß den für den Cloud-Service erteilten Anweisungen und im Rahmen der vom Datenexporteur durchgeführten Eingriffe zur Wartung des Cloud-Service.

ANHANG 2 ZU DEN STANDARDVERTRAGSKLAUSELN

Für einige Cloud-Service-Angebote gelten abweichenden Bestimmungen, die ggf. in einem Auftrag festgelegt werden. Andernfalls führt der Datenimporteur für die im System gespeicherten personenbezogenen Daten die nachstehend beschriebenen technischen und organisatorischen Maßnahmen gemäß Abschnitt 4 Buchstabe (d) und Abschnitt 5 Buchstabe (c) dieser Klauseln durch.

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Abschnitt 4 Buchstabe (d) und Abschnitt 5 Buchstabe (c) eingeführt hat:

1. Zutrittskontrolle. Unbefugten wird der Zutritt zu Geländen, Gebäuden oder Räumlichkeiten verwehrt, in denen sich Datenverarbeitungssysteme, die personenbezogene Daten verarbeiten und/oder nutzen, befinden.

   Maßnahmen: Für alle Rechenzentren gelten strenge Sicherheitsvorkehrungen. Diese werden u. a. durch Wachpersonal oder mithilfe von Überwachungsgeräten, Bewegungsmeldern und Zutrittskontrollmechanismen umgesetzt, um Verletzungen der Sicherheit von Geräten und Rechenzentrumsanlagen zu verhindern. Zu den Systemen und der Infrastruktur der Rechenzentrumsanlagen hat ausschließlich autorisiertes Personal Zutritt. Sicherheitseinrichtungen (z. B. Bewegungsmelder, Kameras usw.) werden regelmäßig gewartet, um ihre ordnungsgemäße Funktion zu gewährleisten. Im Einzelnen werden in allen Rechenzentren die folgenden physischen Sicherheitsmaßnahmen getroffen:

   a. Im Allgemeinen sind Gebäude durch Zutrittskontrollsysteme gesichert (Zutrittssysteme mit Smartcard).
   b. Autorisierte Mitarbeiter erhalten Autorisierungsnachweise, z. B. eine (mitarbeiter-, anbieter- oder auftragnehmerspezifische) elektronische Ausweiskarte und eine PIN, die ihnen den Zutritt zu den Rechenzentrumsanlagen gestatten.
   c. Der Zutritt zu den Rechenzentren innerhalb der Systemgrenze wird mittels eines elektronischen Zutrittskontrollsystems kontrolliert. Dieses umfasst Kartenlesegeräte und PIN-Tastenfelder für den Zutritt zu Gebäuden und Räumen sowie Kartenlesegeräte, die ausschließlich für das Verlassen von Gebäuden und Räumen gedacht sind.
   d. Je nach Sicherheitsklassifizierung werden Gebäude, einzelne Bereiche und die Umgebung mit zusätzlichen Schutzmaßnahmen gesichert. Dazu gehören bestimmte Zutrittsprofile, Videoüberwachung, Einbruchmeldesysteme und biometrische Zutrittskontrollsysteme.
   e. Die Erteilung der Zutrittsberechtigungen für autorisierte Personen erfolgt auf individueller Basis gemäß den nachstehenden Zugangs- und Zugriffskontrollmaßnahmen. Dies gilt auch für den Zutritt von Besuchern. Gäste und Besucher in Gebäuden von SISW müssen sich namentlich am Empfang anmelden und von autorisiertem SISW-Personal begleitet werden. SISW und alle Drittanbieter von Rechenzentren protokollieren die Namen der Personen, die die nicht öffentlichen Bereiche von SISW in den Rechenzentren betreten, sowie die betreffenden Zutrittszeiten.
   f. Mitarbeiter von SISW und externe Mitarbeiter müssen ihre Ausweise an allen SISW-Standorten tragen.

2. Zugangskontrolle. Die zur Bereitstellung des Cloud-Service verwendeten Datenverarbeitungssysteme sind vor unbefugter Nutzung zu schützen.

   Maßnahmen:
   a. SISW bzw. ihre Unterauftragsverarbeiter gewährleisten bei der Verwaltung der Umgebung, dass die Anforderungen von NIST SP 800-53 Rev 4 „Access Control (AC) and Identification and Authentication (IA)“ des National Institute of Standards and Technology (NIST) in den USA eingehalten werden.
   b. Der Zugang zu sensiblen Systemen einschließlich der Systeme zur Speicherung und Verarbeitung personenbezogener Daten wird über mehrere Autorisierungsstufen gewährt. Mit entsprechenden Prozessen wird gewährleistet, dass nur autorisierte Benutzer über die entsprechende Berechtigung zum Hinzufügen, Löschen oder Ändern von Benutzern verfügen.
   c. Alle Benutzer benötigen für den Zugang zu den Systemen von SISW einen eindeutigen Benutzernamen und ein Kennwort, das bestimmte Mindestkriterien in Bezug auf die Komplexität erfüllen muss.
   d. SISW und ihre Unterauftragsverarbeiter gewährleisten mit entsprechenden Verfahren, dass angeforderte Autorisierungsänderungen nur in Übereinstimmung mit den Leitlinien durchgeführt werden (z. B. werden keine Berechtigungen ohne entsprechende Autorisierung erteilt). Wenn ein SISW-Benutzer eine andere Rolle übernimmt oder aus dem Unternehmen ausscheidet, werden die Zugangsberechtigungen für die Umgebung aufgehoben.
   e. SISW und ihre Unterauftragsverarbeiter haben eine Kennwortrichtlinie festgelegt, die die Weitergabe von Kennwörtern untersagt, das Vorgehen bei Weitergabe eines Kennworts regelt, die regelmäßige Änderung aller

Benutzerkennwörter vorschreibt und die Änderung der vorgegebenen Kennwörter verlangt. Zur Authentifizierung werden personalisierte Benutzerkennungen zugewiesen. Alle Kennwörter müssen Mindestanforderungen an die Komplexität erfüllen und werden in verschlüsselter Form gespeichert. Im Fall von Domänenkennwörtern erzwingt das System alle 60 Tage eine Kennwortänderung, bei der die Mindestanforderungen an die Komplexität erfüllt werden müssen. Auf jedem SISW-Rechner ist ein kennwortgeschützter Bildschirmschoner installiert.

f. Bei den folgenden Account-Ereignissen führen SISW oder ihre Unterauftragsverarbeiter automatisch eine Prüfung durch: Erstellung, Änderung, Aktivierung, Deaktivierung und Entfernung. Die Protokolle werden regelmäßig von einem Systemadministrator geprüft.
g. Firewalls schotten die Netzwerke von SISW und ihren Unterauftragsverarbeitern vom öffentlichen Internet ab.
h. SISW und ihre Unterauftragsverarbeiter setzen an den Zugangspunkten zum Firmennetzwerk, für E-Mail-Konten sowie auf allen Dateiservern und Workstations aktuelle Antivirensoftware ein.
i. SISW und ihre Unterauftragsverarbeiter gewährleisten mit einer Sicherheitspatch-Verwaltung die Anwendung relevanter Sicherheitsupdates.
j. Der Remote-Vollzugriff auf das Unternehmensnetzwerk und die kritische Infrastruktur wird durch eine effiziente, mehrstufige Authentifizierung geschützt.

3. Zugriffskontrolle. Personen, die zur Nutzung von Datenverarbeitungssystemen berechtigt sind, erhalten nur auf die personenbezogenen Daten Zugriff, für die sie zugriffsberechtigt sind. Die personenbezogenen Daten dürfen im Rahmen der Verarbeitung, Nutzung und Speicherung nur mit entsprechender Autorisierung gelesen, kopiert, geändert und entfernt werden.

   Maßnahmen:

   a. Der Zugriff auf personenbezogene, vertrauliche oder sensible Informationen wird nur bei entsprechender Notwendigkeit gewährt („Need-to-know"-Prinzip). Mit anderen Worten, Mitarbeiter bzw. externe Dritte können auf die Informationen zugreifen, die sie für ihre Arbeit benötigen. SISW verwendet Autorisierungskonzepte, die dokumentieren, wie und welche Autorisierungen zugewiesen werden. Alle personenbezogenen, vertraulichen oder sonstigen sensiblen Informationen sind durch die SISW-Sicherheitsrichtlinien und -vorgaben geschützt.
   b. Alle Produktionsserver eines SISW-Cloud-Service werden in den betreffenden Rechenzentren betrieben. Die Sicherheitsmaßnahmen zum Schutz der Anwendungen zur Verarbeitung personenbezogener, vertraulicher oder sonstiger sensibler Informationen werden regelmäßig überprüft. Dazu sieht SISW auch regelmäßige externe Prüfungen vor, die die ordnungsgemäße Anwendung dieser Maßnahmen bestätigen sollen.
   c. SISW untersagt die Installation persönlicher oder anderer, nicht von SISW genehmigter Software auf Systemen, die für einen Cloud-Service genutzt werden.
   d. Sollte der Ausfall zugrunde liegender Datenspeichermedien die Übermittlung von Daten erforderlich machen, werden die fehlerhaften Medien nach der Übermittlung entmagnetisiert (Magnetspeicher) oder vernichtet (Solid-State-Speicher oder optischer Speicher).

4. Datenübertragungskontrolle. Personenbezogene Daten dürfen während der Übermittlung nur mit entsprechender Autorisierung gelesen, kopiert, geändert oder entfernt werden.

   Maßnahmen:

   a. SISW bzw. ihre Unterauftragsverarbeiter gewährleisten bei der Verwaltung der Infrastruktur und der Konfiguration, dass die Anforderungen von NIST SP 800-53 Rev 4 „Systems and Communication Protection (SC)" des National Institute of Standards and Technology (NIST) in den USA eingehalten werden. Dies schließt netzwerkbasierte Eindringschutzsysteme und Firewalls an den Systemgrenzen ein, die an der Außengrenze der Infrastruktur Schutz vor schädlichen Mitteilungen bieten. Netzwerkbasierte Eindringschutzsysteme werden über DISA STIG-Vorgaben konfiguriert. Die Daten werden bei der Übermittlung mithilfe von FIPS 140-2 entsprechenden kryptografischen Modulen verschlüsselt.
   b. SISW ergreift geeignete Maßnahmen, um beim physischen Transport von Datenträgern die Einhaltung der vereinbarten Service-Level (z. B. Verschlüsselung und mit Blei ausgekleidete Behälter) zu gewährleisten.
   c. Personenbezogene Daten sind, wie auch andere vertrauliche Daten, gemäß den Sicherheitsrichtlinien von SISW bei der Übertragung über interne SISW-Netzwerke geschützt.
   d. Bei der Übermittlung personenbezogener Daten zwischen SISW und dem Kunden kommen die in der Vereinbarung oder in der relevanten Dokumentation für den Cloud-Service festgelegten Schutzmaßnahmen zur Anwendung. Dies gilt für die physische ebenso wie für die netzwerkbasierte Datenübermittlung. Der Kunde übernimmt die Verantwortung für die Datenübermittlung ab dem Übergabepunkt von SISW (z. B. ausgehende Firewall des Rechenzentrums, in dem der Cloud-Service gehostet wird).

5. Dateneingabekontrolle. Der Cloud-Service bietet die Möglichkeit, im Nachhinein festzustellen, ob und von wem personenbezogene Daten in der zur Bereitstellung des Cloud-Service verwendeten Infrastruktur eingegeben, geändert oder entfernt wurden.

   Maßnahmen:
   a. SISW erlaubt ausschließlich autorisiertem Personal, im Rahmen seiner Arbeit nach Bedarf auf personenbezogene Daten zuzugreifen. SISW hat ein Protokollierungssystem implementiert, das die Eingabe, Änderung und Löschung bzw. Sperrung personenbezogener Daten durch SISW oder ihre Unterauftragsverarbeiter im größten vom Cloud-Service unterstützten Umfang ermöglicht.
   b. Audit-Trails liefern ausreichend detaillierte Informationen zur Rekonstruktion der Ereignisse, wenn eine unberechtigte Aktivität oder eine Störung auftritt oder vermutet wird. Jeder Eintrag im Ereignisprotokoll des Betriebssystems enthält den Ereignistyp, einen Zeitstempel, die Ereignisquelle, die Ereignisposition, die Auswirkungen des Ereignisses und den mit dem Ereignis verknüpften Benutzer.

6. Auftragskontrolle. Personenbezogene Daten werden ausschließlich in Übereinstimmung mit den Bestimmungen der Vereinbarung und den diesbezüglichen Anweisungen des Kunden verarbeitet.

   Maßnahmen:
   a. SISW nutzt Kontrollen und Prozesse, um die Einhaltung der Verträge zwischen SISW und ihren Kunden, Unterauftragsverarbeitern oder anderen Serviceanbietern zu gewährleisten.
   b. Kundendaten werden gemäß dem SISW-Informationsklassifizierungsstandard im gleichen Umfang geschützt wie vertrauliche Informationen.
   c. Sämtliche Mitarbeiter und Vertragspartner von SISW werden vertraglich verpflichtet, die Geheimhaltungspflicht in Bezug auf alle sensiblen Informationen einschließlich Geschäftsgeheimnissen von SISW-Kunden und -Partnern einzuhalten.

7. Verfügbarkeitskontrolle. Personenbezogene Daten werden vor versehentlicher oder unberechtigter Zerstörung oder vor Verlust geschützt.

   Maßnahmen:
   a. SISW verfügt über Sicherungsprozesse und weitere Maßnahmen, um die Verfügbarkeit geschäftskritischer Systeme bei Bedarf kurzfristig wiederherzustellen.
   b. SISW greift auf globale Cloud-Service-Anbieter zurück, um die Stromversorgung für die Rechenzentren zu gewährleisten.
   c. SAP hat Notfallpläne sowie Strategien zur Betriebs- und Notfallwiederherstellung für Cloud-Services ausgearbeitet.

8. Datentrennungskontrolle. Personenbezogene Daten, die für unterschiedliche Zwecke erfasst werden, können getrennt verarbeitet werden.

   Maßnahmen:
   a. SISW nutzt ggf. die technischen Möglichkeiten der implementierten Software (z. B. Mehrmandanten- oder getrennte Systemlandschaften), um die Trennung der personenbezogenen Daten einzelner Kunden zu gewährleisten.
   b. SISW richtet dedizierte Instanzen (mit logischer oder physischer Trennung) für jeden Kunden ein.
   c. Der Kunde (einschließlich der verbundenen Unternehmen) hat ausschließlich auf die eigene(n) Instanz(en) Zugriff.

9. Datenintegritätskontrolle. Die Datenintegritätskontrolle gewährleistet, dass personenbezogene Daten während der Verarbeitungsschritte intakt, vollständig und aktuell bleiben.

   Maßnahmen: SISW hat zum Schutz vor unberechtigten Änderungen eine mehrere Schichten umfassende Sicherheitsstrategie umgesetzt. Dies bezieht sich auf die in den obigen Abschnitten zu Kontrollen und Maßnahmen beschriebenen Kontrollen. Durch die Konfiguration der Firewalls entstehen mehrere Netzwerksegmente, die öffentlichen und privaten Zugriff voneinander trennen. Jeder Firewall-Regelsatz umfasst spezifische Zugriffskontrollen, die die zulässige Kommunikation zwischen diesen Segmenten bestimmen.

a. Sicherheitsüberwachungszentrum: Automatisierte Angriffserkennungssoftware wird in Verbindung mit sonstiger präventiver Sicherheitssoftware und Forensiksoftware sowie entsprechenden Prozessen für folgende Zwecke eingesetzt: Meldung und Untersuchung eines Sicherheitsvorfalls sowie, falls erforderlich, Übermittlung von Benachrichtigungen und Unterstützung bei der Behebung des Sicherheitsvorfalls.
b. Antivirensoftware: Auf allen Systemen werden aktuelle Virendefinitionen zum Schutz vor Viren, Würmern, Trojanern und sonstiger Malware konfiguriert.
c. Sicherung und Wiederherstellung: Für alle Systeme existieren grundlegende Sicherungsmomentaufnahmen der Daten und der Konfiguration. Ggf. unterhalten SISW und ihre Unterauftragsverarbeiter auch eine Kundeninstanz mit Hochverfügbarkeitskonfiguration, um zu gewährleisten, dass die Daten in zwei separaten, ausreichend weit voneinander entfernten Rechenzentren gespeichert werden.
d. Regelmäßige externe Prüfungen zur Validierung der Sicherheitsmaßnahmen. SISW und ihre Unterauftragsverarbeiter unterziehen sich regelmäßig externen Prüfungen, bei denen die oben genannten Sicherheitsmaßnahmen überprüft werden.