Auftragsverarbeitungsvertrag

(Art. 28 Abs. 3 DSGVO)

Fujitsu Technology Solutions GmbH

Mies-van-der-Rohe-Straße 8

80807 München

als "**Auftragnehmer**" oder "**Auftragsverarbeiter**" stellt folgenden Auftragsverarbeitungsvertrag zur Verfügung:

Diese Vereinbarung ("**Vereinbarung**") soll für jede Verarbeitung personenbezogener Daten gelten, die der Auftragnehmer im Auftrag des Auftraggebers ausführt.

1. DEFINITIONEN, AUSLEGUNG

1.1 In dieser Vereinbarung gelten folgende Definitionen (sofern nicht ausdrücklich anderweitig angegeben):

1.1.1 Die Begriffe "**Verantwortlicher**", "**betroffene Personen**", "**personenbezogene Daten**", "**Verarbeitung**" und "**Verarbeiter**" haben dieselbe Bedeutung wie in der DSGVO (verwandte Begriffe sind entsprechend auszulegen).

1.1.2 "**Verbundenes Unternehmen**" ist, in Bezug auf eine juristische oder natürliche Person ("**Referenzperson**"), jede andere Person,

(a) die direkt oder indirekt die Referenzperson kontrolliert; oder

(b) die direkt oder indirekt unter derselben Kontrolle wie die Referenzperson steht; oder

(c) die von der Referenzperson kontrolliert wird.

1.1.3 "**Kontrolle**" ist die Fähigkeit einer Person (oder gemeinschaftlich handelnder Personen), direkt oder indirekt die Angelegenheiten einer anderen Person nach ihren Vorstellungen zu bestimmen, indem sie

(a) im Fall einer Kapitalgesellschaft: wirtschaftlich Berechtigter von mehr als 50% (in Worten: fünfzig Prozent) des Stammkapitals oder der Stimmrechte ist, oder ihr durch Gesellschaftsvertrag, Gesellschaftervereinbarung oder eine andere Vereinbarung, durch die die Angelegenheiten der jeweiligen Kapitalgesellschaft geregelt werden, die Fähigkeit eingeräumt wird, die Mehrheit der Vorstandsmitglieder/ Geschäftsführer zu ernennen oder zu entlassen oder aufgrund anderer Einflussmöglichkeiten die Entscheidungen der Gesellschafterversammlungen der Kapitalgesellschaft zu bestimmen;

(b) im Fall einer Personengesellschaft: wirtschaftlich Berechtigter von mehr als 50% (in Worten: fünfzig Prozent) des Kapitals ist oder ihr durch Gesellschaftsvertrag oder andere Vereinbarung, durch die die Angelegenheiten der Personengesellschaft geregelt werden, die Fähigkeit eingeräumt wird, die Zusammensetzung der Geschäftsführung oder das Abstimmungsverhalten einer Mehrheit der Geschäftsführung der Personengesellschaft zu bestimmen.

Der Begriff "**kontrollieren**" ist entsprechend zu verstehen. In diesem Zusammenhang bedeutet "**gemeinschaftlich handelnde Personen**", dass mehrere Personen gemäß einer Vereinbarung oder Absprache (formell oder informell) in Bezug auf eine Person aktiv zusammenwirken, um Kontrolle zu erlangen oder zu festigen.

1.1.4 "**Anwendbare Gesetze**" sind alle Gesetze und Verordnungen, die im Zusammenhang mit den Leistungen entweder auf den Auftraggeber oder auf den Auftragnehmer (oder auf beide) Anwendung finden.

1.1.5 "**Anwendbare Datenschutzgesetze**" sind Anwendbare Gesetze in Bezug auf den Schutz personenbezogener Daten oder der Privatsphäre, einschließlich der DSGVO (soweit anwendbar).

1.1.6 "**Angemessene Maßnahmen**" sind, vor dem Hintergrund der Verarbeitung personenbezogener Daten, solche technischen und organisatorischen Maßnahmen zum Schutz dieser Daten vor unbeabsichtigter oder unrechtmäßiger Löschung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff, die den unterschiedlichen Risiken - je nach Eintrittswahrscheinlichkeit und Schwere - für die Rechte und Freiheiten natürlicher Personen, deren Daten verarbeitet werden, Rechnung tragen, wobei der jeweilige Stand der Technik, die Kosten für die Umsetzung sowie Art, Umfang, Zweck und Rahmen der Verarbeitung zu berücksichtigen sind.

1.1.7 "**Vertraglich Vereinbarte Sicherheitsmaßnahmen**" bezeichnen die in Anlage 2 vereinbarten technischen und organisatorischen Maßnahmen, die den Schutz der Verarbeiteten Personenbezogenen Daten gewährleisten.

1.1.8 "**Auftraggeber**" ist der Nutzer der Securon Light (Cloud only) Plattform.

1.1.9 "**DSGVO**" bezeichnet die Datenschutz-Grundverordnung (EU 2016/679), einschließlich etwaiger Änderungen, Neufassungen oder Nachfolgebestimmungen.

1.1.10 **"Verletzung des Schutzes personenbezogener Daten"** bezeichnet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

1.1.11 "**Verarbeitete Personenbezogene Daten**" sind personenbezogene Daten, die vom Auftragnehmer oder seinen Subunternehmern im Rahmen der Erbringung der Leistungen verarbeitet werden.

1.1.12 "**Leistungen**" meint die Lieferungen und / oder Leistungen, die der Auftragnehmer erbringt.

1.1.13 "**Subunternehmer**" ist jede Person (mit Ausnahme von Arbeitnehmern), die für den Auftragnehmer (direkt oder indirekt) Leistungen (oder Teile hiervon) erbringt. Personen, die lediglich Hilfsaufgaben erfüllen (einschließlich insbesondere Telekommunikationsdienstleistungen und Reinigungsleistungen) gelten nicht als Subunternehmer.

1.1.14 "**Auftragnehmer**" ist auf dem Deckblatt definiert.

1.2 Auslegungsregeln

1.2.1 In dieser Vereinbarung gilt, sofern nicht ausdrücklich anderweitig festgelegt,

(a) eine Bezugnahme auf eine andere Vereinbarung oder auf ein anderes Dokument als eine Bezugnahme auf die andere Vereinbarung oder das andere Dokument in der jeweils gültigen Fassung und

(b) eine Bezugnahme auf die Präambel, eine Ziffer, einen Anhang oder eine Anlage als eine Bezugnahme auf die Präambel, Ziffer, den Anhang oder auf die Anlage zu dieser Vereinbarung.

(c) Der Auftragnehmer übernimmt mit dieser Vereinbarung keine Garantien im Sinne der §§ 276, 442, 443, 479 oder 639 des Bürgerlichen Gesetzbuchs (BGB).

1.2.2 Den Parteien bleibt es vorbehalten, diese Vereinbarung einvernehmlich zu ergänzen oder zu beenden. Hiervon sind auch, soweit vorhanden, Rechte Dritter umfasst. Es ist keine Zustimmung Dritter in diesem Zusammenhang erforderlich.

2. VERHÄLTNIS ZWISCHEN VERANTWORTLICHEM UND AUFTRAGSVERARBEITER

Die Parteien stellen fest, dass in den Fällen, in denen der Auftragnehmer oder sein Subunternehmer Verarbeitete Personenbezogene Daten verarbeiten, der Auftragnehmer bzw. sein Subunternehmer, vorbehaltlich der Bestimmungen in Ziffer 9, im Auftrag des Auftraggebers tätig werden. Der Auftraggeber bleibt, vorbehaltlich der Bestimmungen in Ziffer 9, in diesen Fällen Verantwortlicher für die Verarbeitung der Verarbeiteten Personenbezogenen Daten.

Anlage 1 (*Beschreibung der Datenverarbeitungstätigkeiten*), die Bestandteil dieses Vertrages ist, enthält die Beschreibung dieser Verarbeitungstätigkeit.

3. PFLICHTEN DES AUFTRAGNEHMERS IN BEZUG AUF VERARBEITETE PERSONENBEZOGENE DATEN

3.1 Der Auftragnehmer wird:

3.1.1 vorbehaltlich der Bestimmungen in Ziffer 6.2 jederzeit technische und organisatorische Maßnahmen bereithalten, die den Vertraglich Vereinbarten Sicherheitsmaßnahmen entsprechen, um die Verarbeiteten Personenbezogenen Daten zu schützen, solange sie sich im Besitz oder in der Kontrolle des Auftragnehmers oder seiner Subunternehmer befinden; und

3.1.2 gewährleisten, dass alle Arbeitnehmer des Auftragnehmers und seiner Subunternehmer, die zum Zugang zu (oder anderweitig zum Verarbeiten der) Verarbeiteten Personenbezogenen Daten berechtigt sind, sich angemessen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.2 Der Auftragnehmer wird Verarbeitete Personenbezogene Daten nur gemäß den dokumentierten Weisungen des Auftraggebers verarbeiten und insbesondere Verarbeitete Personenbezogene Daten, die in den Anwendungsbereich der Anwendbaren Datenschutzgesetze des Europäischen Wirtschaftsraums fallen, nur in

ein Land oder Hoheitsgebiet außerhalb dieses Territoriums übermitteln oder eine solche Übermittlung vom Auftraggeber bei Empfang der Leistungen verlangen, wenn eine dokumentierte Weisung des Auftraggebers vorliegt oder er gemäß Anwendbarer Gesetze hierzu verpflichtet ist (der Auftragnehmer wird den Auftraggeber hierüber unverzüglich informieren, soweit ihm dies im Rahmen der Anwendbaren Gesetze gestattet ist).

3.3 Der Auftraggeber beauftragt den Auftragnehmer (und bevollmächtigt den Auftragnehmer dazu, im Namen des Auftraggebers wiederum seine Subunternehmer zu beauftragen), in seinem Namen bei der Verarbeitung der Verarbeiteten Personenbezogenen Daten solche Maßnahmen zu ergreifen, die der Auftragnehmer (oder die entsprechenden Subunternehmer) vernünftigerweise zur Bereitstellung der Leistungen oder anderweitig zur Erfüllung der Verpflichtungen des Auftragnehmers gemäß dieser Vereinbarung für notwendig erachten. Dies schließt die Befugnis ein, vorbehaltlich der Bestimmungen in Ziffer 7 internationale Datenübermittlungen selbst vorzunehmen oder dies von den entsprechenden Subunternehmern zu verlangen.

3.4 Der Auftragnehmer wird den Auftraggeber bei den nachfolgenden Pflichten unter dieser Ziffer 3.4 insoweit unterstützen, als der Auftraggeber dies angemessenerweise verlangt und der Auftragnehmer in angemessener Weise hierzu in der Lage ist, wobei die Art der Verarbeitung der Verarbeiteten Personenbezogenen Daten zu berücksichtigen ist. Der Auftragnehmer

3.4.1 wird, soweit dies möglich ist, angemessene technische und organisatorische Maßnahmen bereithalten, um den Auftraggeber bei der Bearbeitung von Anfragen betroffener Personen in Hinblick auf Zugang zu Verarbeiteten Personenbezogenen Daten oder deren Berichtigung, Löschung oder Übertragbarkeit, sowie auf Beschränkung oder Widerspruch gegen die Verarbeitung der Verarbeiteten Personenbezogenen Daten im Rahmen der DSGVO zu unterstützen; und

3.4.2 achtet auf die Einhaltung der Pflichten des Auftraggebers hinsichtlich Sicherheit, Folgenabschätzung und Anhörungspflichten gegenüber der Aufsichtsbehörde im Rahmen der DSGVO, soweit dem Auftragnehmer hierzu Informationen vorliegen.

Für die vorstehende Unterstützung kann der Auftragnehmer eine Vergütung nach Aufwand (Zeit und Material) verlangen.

3.5 Vorbehaltlich Ziffer 3.6 informiert der Auftragnehmer den Auftraggeber schriftlich und unverzüglich (jedoch ohne Verpflichtung, eine rechtliche Beratung vorzunehmen), wenn nach seiner Auffassung eine Weisung des Verantwortlichen nach Ziffer 3.2 gegen Anwendbare Datenschutzgesetze verstößt. Der Auftragnehmer ist in diesem Fall berechtigt, die Durchführung der entsprechenden Weisung ganz oder teilweise so lange auszusetzen, bis der Auftraggeber die Weisung nach sorgfältiger Prüfung bestätigt oder ändert.

3.6 Der Auftragnehmer leistet keine Gewähr und haftet nicht für Inhalt einer Information nach Ziffer 3.5 (oder etwaiges Vertrauen hierauf), auch wenn eine solche Stellungnahme unrichtig, unvollständig oder irreführend ist, es sei denn, es liegt ein

Fall von Arglist, Vorsatz, grober Fahrlässigkeit oder eine Verletzung des Lebens, des Körpers oder der Gesundheit vor.

4. SICHERHEITSRELEVANTE VORFÄLLE

4.1 Jede Partei teilt der anderen schriftlich, unverzüglich und unter Angabe der erforderlichen Details mit, wenn sie Kenntnis davon erlangt, dass eine Verletzung des Schutzes personenbezogener Daten hinsichtlich der Verarbeiteten Personenbezogenen Daten, die sich in ihrem Besitz oder in ihrer Kontrolle befinden (ein "**sicherheitsrelevanter Vorfall**"), eingetreten ist.

4.2 Der Auftragnehmer unternimmt in Bezug auf sämtliche sicherheitsrelevanten Vorfälle, die auf die Verletzung einer Pflicht des Auftragnehmers nach dieser Vereinbarung zurückzuführen sind, und von denen der Auftragnehmer Kenntnis erlangt, angemessene Schritte zur Erforschung und Behebung der dem sicherheitsrelevanten Vorfall zugrundeliegenden Ursache, um so das Risiko einer Wiederholung und das Auftreten ähnlicher sicherheitsrelevanter Vorfälle einzudämmen bzw. zu beseitigen.

5. PRÜF- UND AUSKUNFTSRECHTE

5.1 Der Auftragnehmer wird

5.1.1 regelmäßig eine angemessene Überprüfung der technischen und organisatorischen Maßnahmen, die er zum Schutz der Daten des Auftraggebers, einschließlich der Verarbeiteten Personenbezogenen Daten, bereitgestellt hat, vornehmen oder durch einen erfahrenen und qualifizierten Dritten in Auftrag geben; und

5.1.2 dem Auftraggeber auf Anfrage eine Zusammenfassung der jeweiligen Prüfberichte und Prüfungsergebnisse zur Verfügung stellen. Dabei dürfen Informationen geschwärzt oder entfernt werden, die der Auftragnehmer im Hinblick auf andere Auftraggeber vertraulich zu behandeln hat.

5.2 Falls der Auftraggeber dem Auftragnehmer schriftlich darlegt, dass er ernstlich befürchtet, dass der Auftragnehmer eine Pflicht aus Ziffer 3 dieser Vereinbarung in erheblichem Maße verletzt, und die Bedenken sich nicht durch Prüfberichte gemäß Ziffer 5.1 oder durch andere Informationen seitens des Auftragnehmers ausräumen lassen, gilt Folgendes:

5.2.1 Der Auftragnehmer wird dem Auftraggeber unverzüglich die schriftlich angeforderten Informationen zur Verfügung stellen, sofern ihm dies angemessenerweise möglich ist (ohne dabei vertrauliche Informationen von anderen Kunden des Auftragnehmers offenzulegen).

5.2.2 Wenn sich die Bedenken des Auftraggebers (auch nach Ablauf eines angemessenen Zeitraums) nicht durch die Bereitstellung der Informationen nach Ziffer 5.2.1 ausräumen lassen, muss der Auftragnehmer vorbehaltlich der Bestimmungen in Ziffer 5.3 dem Auftraggeber (oder einem vom Auftraggeber benannten Prüfer, dem der Auftragnehmer zugestimmt hat, wobei der Auftragnehmer diese Zustimmung nicht unbillig verweigern oder verzögern darf) die Durchführung einer Überprüfung oder Inspektion der zur Erbringung

der Leistungen eingesetzten Räumlichkeiten, Systeme und Mitarbeiter des Auftragnehmers und der mit ihm Verbundenen Unternehmen gestatten. Dies ist auf Maßnahmen beschränkt, die erforderlich sind, um die Bedenken des Auftraggebers auszuräumen.

5.3 Der Auftraggeber wird

5.3.1 dem Auftragnehmer jegliche Überprüfung oder Inspektion, die gemäß Ziffer 5.2.2 durchgeführt wird, mit angemessener Frist vorankündigen;

5.3.2 angemessene Anstrengungen unternehmen (und sicherstellen, dass jeder Prüfer alle ihm zumutbaren Anstrengungen unternimmt), um Schäden, Verletzungen bzw. Störungen der Räumlichkeiten, Systeme, Mitarbeiter und des Geschäftsbetriebs des Auftragnehmers oder der mit ihm Verbundenen Unternehmen zu vermeiden (oder, falls dies nicht möglich ist, diese zu minimieren), während sich seine Mitarbeiter zum Zwecke einer Prüfung oder Inspektion in diesen Räumlichkeiten befinden oder auf diese Systeme zugreifen; und

5.3.3 dem Auftragnehmer und den mit ihm Verbundenen Unternehmen solche Kosten oder Aufwendungen erstatten, die in Folge solcher Schäden, Verletzungen oder Störungen entstanden sind, auch wenn die nach Ziffer 5.3.2 erforderlichen Anstrengungen unternommen wurden.

5.4 Der Auftragnehmer ist in folgenden Fällen nicht verpflichtet, Zugang zu seinen Räumlichkeiten oder Systemen für die Zwecke der Überprüfung oder Inspektion gemäß Ziffer 5.2.2 zu gewähren:

5.4.1 an Einzelpersonen, sofern er oder sie keinen angemessenen Nachweis hinsichtlich Identität und Befugnis erbringt, oder

5.4.2 in den entsprechenden Räumlichkeiten außerhalb der üblichen Geschäftszeiten.

Darüber hinaus muss der Auftragnehmer dem Auftraggeber oder seinen Prüfern zum Zwecke der Überprüfung oder Inspektion keine Informationen bereitstellen, die im Hinblick auf andere Kunden des Auftragnehmers vertraulich sind.

5.5 Der Auftragnehmer kann vom Auftraggeber für die Zeit, die er im Zusammenhang mit der Durchführung einer Überprüfung oder Inspektion nach Ziffer 5.2.2 aufwendet, eine Vergütung nach Aufwand (Zeit und Material) verlangen. Dies gilt nicht, wenn die Überprüfung oder Inspektion ergibt, dass der Auftragnehmer eine Pflicht aus Ziffer 3 dieser Vereinbarung in wesentlichem Umfang verletzt hat.

6. PFLICHTEN DES AUFTRAGGEBERS IN HINBLICK AUF VERARBEITETE PERSONENBEZOGENE DATEN

6.1 Der Auftraggeber wird

6.1.1 sich vor der Offenlegung von personenbezogenen Daten gegenüber dem Auftragnehmer oder einem seiner Subunternehmer selbst davon überzeugen, dass die technischen und organisatorischen Maßnahmen, die den Vertraglich Vereinbarten Sicherheitsanforderungen entsprechen, Angemessene

Maßnahmen zum Schutz der Verarbeiteten Personenbezogenen Daten darstellen,

6.1.2 selbst Angemessene Maßnahmen ergreifen, um die Verarbeiteten Personenbezogenen Daten zu schützen, soweit diese sich in seinem Besitz oder unter seiner Kontrolle befinden, und

6.1.3 die vom Auftragnehmer als Vertragliche Vereinbarte Sicherheitsmaßnahmen eingerichteten Sicherheitsmaßnahmen einhalten, wenn er auf die Verarbeiteten Personenbezogenen Daten, die sich im Besitz oder unter der Kontrolle des Auftragnehmers oder seiner Subunternehmer befinden, zugreift oder diese verarbeitet.

6.2 Sollte sich trotz Ziffer 6.1 herausstellen, dass die zum Schutz der Verarbeiteten Personenbezogenen Daten, solange sie sich im Besitz oder unter der Kontrolle des Auftragnehmers befinden, ergriffenen technischen und organisatorischen Maßnahmen nicht (oder vermeintlich nicht) Angemessenen Maßnahmen zum Schutz dieser Daten entsprechen, obwohl die Vertraglich Vereinbarten Sicherheitsmaßnahmen eingehalten wurden (eine "**sicherheitsrelevante Abweichung**"), sind die Parteien auf schriftliches Verlangen des Auftraggebers verpflichtet, nach Treu und Glauben über eine Anpassung der Vertraglich Vereinbarten Sicherheitsmaßnahmen zu verhandeln, um der sicherheitsrelevanten Abweichung Rechnung zu tragen.

6.3 Der Auftraggeber ist für sicherheitsrelevante Abweichungen verantwortlich und wird dem Auftragnehmer und den mit dem Auftragnehmer Verbundenen Unternehmen alle Kosten und Aufwendungen erstatten, die diesen im Zusammenhang mit einer Inanspruchnahme (einschließlich der Inanspruchnahme durch eine Aufsichtsbehörde oder eine andere Datenschutzbehörde) in Folge einer sicherheitsrelevanten Abweichung oder einer Verletzung der Pflichten des Auftraggebers nach Ziffer 6.1 entstehen.

7. INTERNATIONALE DATENÜBERMITTLUNG / ERMÄCHTIGUNG DES AUFTRAGGEBERS

7.1 Der Auftraggeber erklärt sich damit einverstanden, dass der Auftragnehmer im Rahmen der Bestimmungen der Ziffern 3.3 und 8zum Zweck der Verarbeitung von Verarbeiteten Personenbezogenen Daten Subunternehmer, einschließlich mit ihm Verbundener Unternehmen, innerhalb und außerhalb des Europäischen Wirtschaftsraums einsetzen darf.

7.2 Bevor der Auftragnehmer oder einer seiner Subunternehmer Verarbeitete Personenbezogene Daten an einen Subunternehmer in einem Land oder Hoheitsgebiet außerhalb dieses Territoriums übermittelt (oder dies vom Auftraggeber bei Erhalt der Leistungen verlangt), muss der Auftragnehmer darauf achten, dass vorbehaltlich der Anwendbaren Datenschutzgesetze des europäischen Wirtschaftsraums:

7.2.1 ein Beschluss vorliegt, wonach das betreffende Land oder Hoheitsgebiet über ein angemessenes Schutzniveau für die Verarbeiteten Personenbezogenen Daten (bzw. Kategorien personenbezogener Daten, die Verarbeitete Personenbezogene Daten beinhalten) im Einklang mit der DSGVO verfügt; oder

7.2.2 der Auftragnehmer in Bezug auf die Übermittlung im eigenen Namen und (soweit relevant und vorbehaltlich der Ziffern 7.3 und 9.2.1) im Namen des Auftraggebers geeignete Garantien gemäß § 46 Abs. 2 DSGVO vorgesehen hat.

7.3 Der Auftraggeber ermächtigt hiermit den Auftragnehmer dazu, Standarddatenschutzklauseln gemäß § 46 Abs. 2 lit. c) oder d) DSGVO als Vertreter im Namen des Auftraggebers abzuschließen; dies umfasst auch die Genehmigung von bereits vor dem Abschluss dieser Vereinbarung abgeschlossenen Vereinbarungen.

7.4 Die Parteien vereinbaren im Hinblick auf Standarddatenschutzklauseln gemäß § 46 Abs. 2 lit. c) oder d) DSGVO, die zwischen dem Auftragnehmer und seinen Subunternehmern außerhalb des Europäischen Wirtschaftsraums geschlossen werden, das Folgende:

7.4.1 Die Erfüllung der Pflichten des Auftragnehmers nach Ziffer 5 entspricht der Verpflichtung des Datenimporteurs unter den Standarddatenschutzklauseln, dem Auftraggeber Prüfrechte einzuräumen.

7.4.2 Die Erfüllung der Pflichten des Auftragnehmers nach Ziffer 8 entspricht den Verpflichtungen des Datenimporteurs unter den Standarddatenschutzklauseln, den Auftraggeber über die Einschaltung von Unterauftragsverarbeitern zu informieren und seine Zustimmung hierzu einzuholen.

7.4.3 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage eine Kopie der Vereinbarungen zwischen dem Datenimporteur und dem Unterauftragsverarbeiter nach Ziffer 7.2.2 zur Verfügung, aus der alle sensiblen Geschäftsinformationen entfernt wurden. Die Erfüllung dieser Verpflichtung entspricht der Verpflichtung des Datenimporteuers nach den Standarddatenschutzklauseln, dem Auftraggeber Kopien von Vereinbarungen mit Unterauftragsverarbeitern zur Verfügung zu stellen.

7.4.4 Die Haftung des Datenimporteurs oder Auftragnehmers gegenüber dem Auftraggeber aus oder im Zusammenhang mit den Standarddatenschutz-klauseln gilt als Haftung des Auftragnehmers aus oder im Zusammenhang mit dieser Vereinbarung.

8. UNTERAUFTRAGSVERARBEITER

8.1 Der Auftraggeber erklärt sich damit einverstanden, dass der Auftragnehmer andere Personen beauftragen kann, um die Verarbeiteten Personenbezogenen Daten in seinem Namen zu verarbeiten ("**Unterauftragsverarbeiter**"), wenn:

8.1.1 der Unterauftragsverarbeiter (i) ein mit dem Auftragnehmer Verbundenes Unternehmen oder (ii) als Subunternehmer in Anhang 3 genannt ist oder sonst dem Auftraggeber schriftlich vor Abschluss dieser Vereinbarung als für diesen Zweck eingesetzt mitgeteilt wurde; oder

8.1.2 der Auftragnehmer (i) dem Auftraggeber frühzeitig eine schriftliche Mitteilung über den geplanten Einsatz gemacht hat, einschließlich solcher Informationen, anhand derer die Auswirkungen dieses Einsatzes auf die

Erfüllung der Pflichten aus Ziffer 3 abgeschätzt werden können; und (ii) der Auftragnehmer vor Beauftragung des Unterauftragsverarbeiters etwaige Anmerkungen oder Einwände des Auftraggebern angemessen berücksichtigt hat.

Sollten diese Voraussetzungen nicht vorliegen, ist die Beauftragung eines Unterauftragsverarbeiters nicht zulässig.

8.2 Der Auftragnehmer haftet, unabhängig vom Einsatz von Unterauftragsverarbeitern, weiterhin für die Erfüllung seiner Pflichten im Rahmen dieser Vereinbarung.

8.3 Der Auftragnehmer stellt sicher, dass jeder Unterauftragsverarbeiter einen Vertrag abschließt, der in Bezug auf den Verantwortlichen verbindlich ist und dem Unterauftragsverarbeiter Verpflichtungen auferlegt, die im Wesentlichen denen entsprechen, die dem Auftragnehmer gemäß Ziffer 3 auferlegt werden.

8.4 Nicht als Leistungen eines Unterauftragsverarbeiter im Sinne dieser Vereinbarung gelten solche Leistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Erbringung der Leistungen in Anspruch nimmt (darunter fallen insbesondere, aber nicht abschließend Telekommunikationsleistungen und Reinigungsarbeiten). Der Auftragnehmer ist jedoch verpflichtet, auch in Hinblick auf diese Unterauftragsverarbeiter zur Gewährleistung des Schutzes und der Sicherheit der Verarbeiteten Personenbezogenen Daten des Auftraggebers angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9. DRITTE ALS VERANTWORTLICHE

Ist anstelle des Auftraggebers ein mit diesem Verbundenes Unternehmen oder ein Dritter für die Verarbeitung der Verarbeiteten Personenbezogenen Daten verantwortlich ("**Drittverantwortlicher**"), gilt das Folgende:

9.1 Der Auftraggeber gewährleistet, dass der Drittverantwortliche die Pflichten des Auftraggebers nach Ziffer 6 in Hinblick auf Verarbeitete Personenbezogene Daten erfüllt, als wäre der Drittverantwortliche anstelle des Auftraggebers Partei dieser Vereinbarung.

9.2 Bezugnahmen auf den Auftraggeber in Ziffer 3 sollen, soweit einschlägig, als Bezugnahmen auf den Drittverantwortlichen anstelle des Auftraggebers oder gemeinsam mit dem Auftragnehmer ausgelegt werden. Allerdings

9.2.1 übt der Auftraggeber alle auf den Drittverantwortlichen übertragenen Rechte in Ziffer 3 in dessen Namen aus und stellt sicher, dass der Drittverantwortliche diese nicht selbst geltend macht und

9.2.2 muss der Auftraggeber gewährleisten, dass er zu allen maßgeblichen Zeitpunkten autorisiert ist, im Namen des Drittverantwortlichen die in dieser Vereinbarung aufgeführten Weisungen, Erklärungen und Berechtigungen zu erteilen (und seinerseits den Auftragnehmer zur Erteilung zu bevollmächtigen).

10. VERTRAGSLAUFZEIT UND BEENDIGUNG

10.1 Diese Vereinbarung tritt mit Nutzung der Securon Light (Cloud only) Plattform in Kraft. Die relevanten Bestimmungen dieser Vereinbarung bestehen fort, bis alle übermittelten Verarbeiteten Personenbezogenen Daten gemäß dieser Vereinbarung gelöscht, zerstört oder zurückgegeben wurden.

10.2 Der Auftragnehmer soll nach Wahl des Auftraggebers unverzüglich nach dem Ende der Erbringung der erbrachten Leistungen alle Verarbeiteten Personenbezogenen Daten, welche sich in seinem Besitz oder in seiner Kontrolle befinden, löschen, zerstören oder zurückgeben. Auf schriftliche Anfrage hin soll der Auftragnehmer dem Auftraggeber die Löschung der Verarbeiteten Personenbezogenen Daten bestätigen.

11. SCHLUSSBESTIMMUNGEN

11.1 Diese Vereinbarung unterliegt deutschem Recht.

11.2 Für den Fall, dass eine Bestimmung dieser Vereinbarung ganz oder teilweise nichtig oder unwirksam sein sollte oder werden sollte oder falls sich in dieser Vereinbarung eine Regelungslücke offenbart, bleibt die Vereinbarung im Übrigen hiervon unberührt.

11.3 Diese Vereinbarung kann auch mittels einer elektronischen Zustimmung wirksam geschlossen werden. Für diesen Fall verpflichten sich der Auftraggeber, dass er ein autorisierter Vertreter der Schule / des Schulträgers ist.

ANLAGE 1
BESCHREIBUNG DER DATENVERARBEITUNGSTÄTIGKEITEN

1. Gegenstand und Dauer der Verarbeitung

Fujitsu stellt der Schule für die Dauer des Testzeitraumes eine Cloudplattform zur Kollaboration und Kommunikation zur Verfügung.

2. Name und Kontaktdaten des Auftragverarbeiters und seines Datenschutzbeauftragten (Artikel 30 (1) a) und 30 (2) a) DSGVO)

Partei	Name	Funktion	Telefon	E-Mail
Fujitsu Technology Solutions GmbH	Frank Kuß	Head of SITC	+49 40 5120 3200	frank.kuss@ts.fujitsu.com
Fujitsu Technology Solutions GmbH	Stefan Strobel	Datenschutzbeauftragter	+49 89 62060 2111	Datenschutzbeauftragter@ts.fujitsu.com

3. Art und Zweck der Verarbeitung (Artikel 30 (1) b) DSGVO)

Zurverfügstellung eines Cloud-Services im pädagogischen Umfeld.

4. Arten der Verarbeiteten Persönlichen Daten (Artikel 30 (1) c) DSGVO)

Datenkategorien [1]			
☒	Persönliche Stammdaten	☒	Kommunikationsdaten (z.B. Telefon, Email)
☐	Vertragsstammdaten (vertragliche Beziehung, Interesse am Produkt und Vertragserfüllung)	☐	Kundenhistorie
☐	Vertragsabrechnungs- und Zahlungsdaten	☐	Planungs- und Steuerungsdaten
☐	Informationen von Drittparteien (z.B. Auskunfteien oder öffentlichen Registern)		
☐	Andere:		

[1] Mehrfachnennung ist möglich!

Besondere Kategorien personenbezogener Daten nach Artikel 9 DSGVO[2]			
☒	Keine Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 DSGVO **oder** eine oder mehrere der folgenden Kategorien:		
☐	Gesundheitsdaten/ Daten zum Sexualleben oder zur sexuellen Orientierung	☐	Gewerkschaftszugehörigkeit / Betriebsratszugehörigkeit
☐	Religiöse oder weltanschauliche Überzeugungen	☐	Politische Meinungen
☐	Rassische und ethnische Herkunft	☐	Genetische/ biometrische Daten (Fingerabdruck))
☐	Gesichtsbilder zur eindeutigen Identifizierung (z.B. Fotos)		
☐	Andere:		

5. **Kategorien betroffener Personen (Artikel 30 (1) c) DSGVO)**

Auflistung betroffener Personen[3]			
☐	Kunden	☐	Interessenten
☐	Abonnenten	☐	Mitarbeiter / Beschäftigte / Bewerber
☐	Lieferanten	☐	Handelsvertreter
☐	Kontaktdaten		
☒	Andere: Schüler, Lehrer, Systemadministratoren		

6. **Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offen gelegt werden, einschließlich Empfänger Drittländern oder internationalen Organisationen (sofern einschlägig) (Artikel 30 (1) d) DSGVO)**

Auflistung von Empfängerkategorien [4]					
☒	Direkte Unterauftragnehmer (Sub)	☐	Indirekte Unterauftragnehmer Sub-Sub		
☐	Firmen der Fujitsu Gruppe	☐	Fujitsu GDC's	☐ ☐	EU Drittland
☐	Nicht Fujitsu GDC's	☐	Lieferanten/Partner		
☐	Andere:				

[2] Mehrfachnennung ist möglich!

[3] Mehrfachnennung ist möglich!

[4] Mehrfachnennung ist möglich!

7. **Fristen für die Löschung der verschiedenen Datenkategorien (Artikel 30 (1) f) DSGVO)**

Nach Ablauf des Testzeitraumes werden die Daten der Plattform dem Auftraggeber übergeben und auf der Plattform gelöscht.

8. **Kategorien der Verarbeitung (Artikel 30 (2) b) DSGVO)**

☐	Erhebung	Falls zutreffend: Bei der betroffenen Person direkt	☐	oder: Bei Dritten	☐
☒	Speicherung				
☐	Übermittlung				
☐	Veränderung				
☐	Sperrung				
☒	Nutzung				
☐	Prüfung, Wartung oder Bereitstellung automatisierter Verfahren oder Datenverarbeitungsanlagen durch andere Stellen im Auftrag, bei welchen ein Zugriff auf personenbezogene Daten oder Kundendaten nicht ausgeschlossen werden kann.				

9. **Technische und organisatorische Sicherheitsmaßnahmen (Artikel 30 (1) g) und 30 (2) d) DSGVO)**

Siehe **Anlage 2**.

ANLAGE 2
VERTRAGLICH VEREINBARTE SICHERHEITSMAßNAHMEN

1. Der Auftraggeber wird für die Verarbeitung der personenbezogenen Daten die in der Vereinbarung festgelegten technischen und organisatorischen Maßnahmen treffen. Auf schriftliche Anfrage wird der Auftragnehmer einen Nachweis dafür erbringen, dass diese Maßnahmen bereitgestellt wurden.

2. Der Auftragnehmer wird mindestens die folgenden technischen und organisatorischen Maßnahmen treffen, soweit diese in Bezug auf die Leistungen in die Verantwortlichkeit des Auftragnehmers fallen und seiner Kontrolle unterliegen:

2.1 **Zugangskontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um Unbefugten den Zugang zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, zu verwehren. Unbefugte Personen dürfen keinen Zugang zum Gelände, den Gebäuden oder Räumlichkeiten haben, in denen sich Verarbeitungsanlagen befinden, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden. Externen Prüfern darf der Zugang ausnahmsweise gewährt werden, solange sie vom Auftragnehmer überwacht werden und keinen Zugriff auf die Verarbeiteten Personenbezogenen Daten erhalten.

Der Auftragnehmer wird insbesondere

(a) berechtigte Personen benennen
(b) einen Prozess zur Zugangskontrolle einrichten, um unbefugten Zugang zu Räumlichkeiten zu vermeiden
(c) einen Prozess zur Zugangskontrolle einrichten, um den Zugang zu Rechenzentren / Serverräumen zu beschränken
(d) Videoüberwachung und Alarmanlagen in Bezug auf Zugangsbereiche verwenden
(e) Drittpersonal ohne Zugangsberechtigung (z.B. Techniker oder Reinigungspersonal) durchgängig begleiten

2.2 **Datenträgerkontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verhindern.

Der Auftragnehmer wird insbesondere

(a) Datenträger in gesicherten Bereichen verwahren
(b) Regeln für die sichere und dauerhafte Zerstörung von nicht mehr benötigten Datenträgern aufstellen
(c) Zugang zu Datenträgern nur seinem Personal und dem Personal seiner Subunternehmer sowie deren Organen, Angestellten, Vertretern und zulässigen Subunternehmern und Rechtsnachfolgern gewähren, jeweils mit der zur Erfüllung ihrer Aufgabe erforderlichen Berechtigung.

2.3 **Speicherkontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um eine unbefugte Eingabe von personenbezogenen Daten sowie eine unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten zu verhindern. Für ein

Datenverarbeitungssystem berechtigte Personen sollen nur solche Daten eingeben und nur auf solche Daten Zugriff haben, für die sie ein Recht zur Eingabe oder zum Zugriff haben, und Verarbeitete Personenbezogene Daten dürfen im Rahmen der Verarbeitung nicht ohne Berechtigung gelesen, kopiert, verändert oder gelöscht werden.

Der Auftragnehmer wird insbesondere

(a) den Zugriff auf Dateien und Programme auf einer "Need-to-Know-Basis" beschränken
(b) Datenträger in gesicherten Bereichen verwahren
(c) die Nutzung/Installation nicht freigegebener Hardware und/oder Software verhindern
(d) Regeln für die sicher und dauerhafte Zerstörung von nicht mehr benötigten Daten aufstellen
(e) Zugang zu Daten nur seinem Personal und dem Personal seiner Subunternehmer sowie deren Organen, Angestellten, Vertretern und zulässigen Subunternehmern und Rechtsnachfolgern gewähren, jeweils mit der zur Erfüllung ihrer Aufgabe erforderlichen Berechtigung.

2.4 **Benutzerkontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte zu verhindern.

Der Auftragnehmer wird insbesondere

(a) angemessene Maßnahmen ergreifen, um Systeme, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, vor unbefugtem Zugriff mit Hilfe von Einrichtungen zur Datenübertragung zu schützen; dies beinhaltet den Einsatz von Firewalls und Intrusion Detection-Systemen
(b) den Fernzugriff auf Systeme, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, protokollieren
(c) für den Fernzugriff auf Systeme, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, Authentifizierungssysteme einsetzen
(d) Fernzugriff auf Applikationen, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, nur seinem Personal und dem Personal seiner Subunternehmer sowie deren Organen, Angestellten, Vertretern und zulässigen Subunternehmern und Rechtsnachfolgern gewähren, jeweils mit der zur Erfüllung ihrer Aufgabe erforderlichen Berechtigung
(e) Einen Prozess zur Deaktivierung von Fernzugriffsberechtigungen für den Fall etablieren, dass ein Benutzer das Unternehmen verlässt oder sich seine Aufgabe ändert

2.5 **Zugriffskontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Der Auftragnehmer wird insbesondere

(a) gewährleisten, dass alle Rechner, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden (auch bei Fernzugriff)
- nach der Boot-Sequenz und
- wenn sie für einen kurzen Zeit nicht genutzt wurden

mit einem Passwort geschützt sind, um den unbefugten Zugriff auf Verarbeitete Personenbezogene Daten zu verhindern

(b) für jede Person eine dedizierte Benutzerkennungen zur Authentifizierung gegenüber der Benutzerverwaltung des Systems verwenden

(c) individuelle Passwörter zur Authentifizierung zuweisen

(d) gewährleisten, dass für die Zugriffskontrolle eine Authentifizierungssystem eingesetzt wird, einschließlich des Fernzugriffs und der Fernnutzung von Systemen

(e) Zugriff auf Applikationen, mit denen Verarbeitete Personenbezogene Daten verarbeitet werden, nur seinem Personal und dem Personal seiner Subunternehmer sowie deren Organen, Angestellten, Vertretern und zulässigen Subunternehmern und Rechtsnachfolgern gewähren, jeweils mit der zur Erfüllung ihrer Aufgabe erforderlichen Berechtigung

(f) eine Passwortrichtlinie implementieren, die die Weitergabe von Passwörtern verbietet, einen geregelten Prozess für den Fall vorsieht, dass ein Passwort Dritten offengelegt wird und die eine regelmäßige Änderung von Passwörtern erfordert

(g) gewährleisten, dass jeder Rechner einen passwortgeschützten Bildschirmschoner hat, der sich spätestens nach 10-15 minütiger Inaktivität einschaltet

(h) gewährleisten, dass Passwörter immer verschlüsselt gespeichert werden

(i) einen Prozess zur Deaktivierung von Nutzerberechtigungen für den Fall etablieren, dass ein Benutzer das Unternehmen verlässt oder sich seine Aufgabe ändert

(j) einen Prozess zur Anpassung von Administratorberechtigungen für den Fall etablieren, dass ein Administrator das Unternehmen verlässt oder sich seine Aufgabe ändert

2.6 **Übertragungskontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

2.7 **Eingabekontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind. Es muss nachträglich möglich sein, zu untersuchen und festzustellen, ob und von wem Verarbeitete Personenbezogene Date in das Datenverarbeitungssystem eingegeben wurden bzw. in dem Datenverarbeitungssystem verändert oder gelöscht wurden (soweit dies unter der Kontrolle des Auftragnehmers steht).

Der Auftragnehmer wird insbesondere

(a) Administrator- und Nutzeraktivitäten protokollieren
(b) nur befugtem Personal die Eingabe und Änderung von Verarbeiteten Personenbezogenen Daten im Rahmen ihrer Aufgaben gestatten

2.8 **Transportkontrolle:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Verarbeitete Personenbezogene Daten dürfen während des Transfers oder während der Speicherung nur insoweit gelesen, kopiert, geändert oder gelöscht werden, wie das für die Erbringung der Leistungen erforderlich ist. Der Auftragnehmer trifft angemessene Maßnahmen, um die Vertraulichkeit und Integrität der Verarbeiteten Personenbezogenen Daten bei Übermittlung und Transport zu schützen.

Der Auftragnehmer wird insbesondere

(a) Daten für die Übermittlung verschlüsseln
(b) Datenträger in verschlossenen Containern transportieren
(c) Fracht- und Lieferpapiere nachhalten

2.9 **Wiederherstellbarkeit:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Der Auftragnehmer wird insbesondere

(a) Datensicherungen erstellen und diese in einer speziell geschützten Umgebung aufbewahren (soweit dies Teil der Leistungen ist)
(b) Regelmäßige Wiederherstellungstests mit solchen Datensicherungen durchführen
(c) Einen Notfall- und Wiederherstellungsplan für seinen eigenen Betrieb vorhalten
(d) Verarbeitete Personenbezogene Daten nicht von den Rechnern und aus den Räumlichlichkeiten des Auftragnehmers entfernen (sofern dies vom Auftraggeber nicht ausdrücklich zu Geschäftszwecken authorisiert wurde)
(e) keine private Ausrüstung für die Erbringung der Leistungen verwenden
(f) aktuelle Anti-Viren-Lösungen auf Computersystemen einsetzen

2.10 **Zuverlässigkeit:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass alle Funktionen eines Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

2.11 **Datenintegrität**: Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

2.12 **Auftragskontrolle**: Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass personenbezogene Daten,

die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftragnehmer erbringt die Leistungen und insbesondere die Verarbeitung von Verarbeiteten Personenbezogenen Daten, nur im Einklang mit den erteilten Weisungen und wird seine Subunternehmer, die in die Verarbeitung der Verarbeiteten Personenbezogenen Daten einbezogen sind, entsprechend anweisen.

Der Auftragnehmer wird insbesondere

(a) die Leistungserbringung überwachen
(b) gemäß den schriftlichen Weisungen und vertaglichen Vereinbarungen arbeiten
(c) personenbezogene Daten, die er von verschiedenen Kunden erhalten, so verarbeiten, dass bei jedem Verarbeitungsschritt der jeweilige Verantwortliche in Bezug auf die personenbezogenen Daten identifiziert werden kann (physische und logische Trennung der Daten)

2.13 **Verfügbarkeitskontrolle:** Verarbeitete Personenbezogene Daten werden gegen Offenlegung sowie gegen versehentliche oder unbefugte Zerstörung oder Verlust geschützt.

Der Auftragnehmer wird insbesondere

(a) Datensicherungen erstellen und diese in einer speziell geschützten Umgebung aufbewahren (soweit dies Teil der Leistungen ist)
(b) Regelmäßige Wiederherstellungstests mit solchen Datensicherungen durchführen
(c) Einen Notfall- und Wiederherstellungsplan für seinen eigenen Betrieb vorhalten
(d) Verarbeitete Personenbezoge Daten nicht zu anderen als den vertragsgemäßen Zwecken verwenden
(e) Verarbeitete Personenbezogene Daten nicht von den Rechnern und aus den Räumlichlichkeiten des Auftragnehmers entfernen (sofern dies vom Auftraggeber nicht ausdrücklich zu Geschäftszwecken authorisiert wurde)
(f) keine private Ausrüstung für die Erbringung der Leistungen verwenden
(g) gewährleisten, dass Nutzer, die ihren Arbeitsplatz während der Arbeitszeit verlassen oder nach Ende der Arbeitszeit verlassen, Dokumente, die Verarbeitete Personenbezogene Daten enthalten, in einem sicheren und gesicherten Umfeld verwahren, wie z.B. einer Schreibtischschublade, einem Aktenschrank oder einem gesicherten Aufbewahrungsort (Clean Desk)
(h) einen Prozess für die Zerstörung von Dokumenten und Datenträgern mit personenbezogenen Daten implementieren
(i) Firewalls auf Netzwerkebene verwenden, um unbefugten Zugriff auf Systeme und Services auf Netzwerkebene zu verhindern
(j) aktuelle Anti-Viren-Lösungen auf Computersystemen einsetzen

2.14 **Trennbarkeit:** Der Auftragnehmer trifft die angemessenen technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Verarbeitete Personenbezogene Daten getrennt verarbeitet werden können. Der Auftragnehmer darf sich insoweit auf die Weisungen und Informationen des Auftraggebers verlassen, insbesondere in Bezug auf die Art der Verarbeiteten Personenbezogenen Daten und den Zweck ihrer Erhebung. Soweit Maßnahmen zur

Trennung nicht unter die Pflichten des Auftragnehmers fallen, steht die Verpflichtung des Auftragnehmers zur Umsetzung solcher Maßnahmen unter dem Vorbehalt einer Vereinbarung, in der die Maßnahmen spezifiziert und eine angemessene Vergütung des Auftragnehmers vereinbart wird.

ANLAGE 3
SUBUNTERNEHMER

Subunter-nehmer	Land	Aufgaben	Kontaktdaten	Telefon	E-Mail
OTRS AG	Deutsch-land	Plattform-anbieter für ITSM	Zimmersmühlenweg 11 61440 Oberursel	+49 6172 681988 -0	security@otrs.com