

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen

gemäß Art. 28 Datenschutzgrundverordnung (DSGVO)

Präambel

- a) Die Trust Call GmbH, Lurgiallee 12, 60439 Frankfurt am Main (im Folgenden als „Auftragnehmer“ oder „Auftragsverarbeiter“ bezeichnet) und der Kunde (im Folgenden Auftraggeber“ oder „Verantwortlicher“ genannt) haben einen Vertrag zur Nutzung eines Dienstes der Trust Call GmbH geschlossen (nachfolgend: „Hauptvertrag“).
- b) Aufgrund des automatisierten Dienstes erhält der Auftragnehmer grundsätzlich keine Kenntnis vom Inhalt der von dem Auftraggeber bereitgestellten Daten. Allerdings ist es im Rahmen des Dienstes gemäß Hauptvertrag einschließlich des Supportes und des Hostings zumindest technisch nicht ausgeschlossen, dass ein Zugriff erfolgen könnte.
- c) Da aus diesem Grund eine Identifikation einer natürlichen Person und damit eine Verarbeitung von personenbezogenen Daten nicht ausgeschlossen werden kann, werden mit diesem Vertrag die Regelungen zur Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber im Rahmen der Nutzung des Dienstes gemäß Hauptvertrag geregelt (nachfolgend „AVV“ genannt).
- d) Dieser AVV bildet einen integralen Bestandteil der AGB und der Nutzungsbedingungen des jeweiligen Dienstes. Mit Zustimmung des Nutzers/Kunden zu den AGB und den Nutzungsbedingungen wird auch der AVV zwischen den Parteien wirksam. Er gilt aber auf Grund Abs. (b) nur dann und nur so weit, wie der Auftraggeber tatsächlich den Anforderungen des Art. 28 DSGVO unterliegt.
- e) Bei Widersprüchen oder einer Unstimmigkeit zwischen dem AVV und den AGB sowie den einzelnen Nutzungsbedingungen hat dieser AVV Vorrang in dem Umfang, in dem ein solcher Konflikt oder eine solche Unstimmigkeit besteht.
- f) Der Auftragsverarbeiter erbringt die Vertragsleistungen ausschließlich auf Grundlage der Regelungen dieses Auftragsverarbeitungsvertrages, etwaige Geschäftsbedingungen des Kunden finden keine Anwendung, auch wenn der Auftragsverarbeiter ihnen nicht ausdrücklich widersprochen hat.

Gegenstand / Anwendung der EU Standardvertragsklauseln

Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber in dessen Auftrag im Sinne der in der Präambel aufgeführten Dienstleistungen gemäß Hauptvertrag. Die Vertragsparteien vereinbaren hierzu, da die Datenverarbeitung durch den Auftragnehmer in der EU stattfinden wird, entsprechend des Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates, folgenden AVV, bestehend aus folgenden Teilen:

- Teil I:** Standardvertragsklauseln zur Einhaltung von Art. 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 (DSGVO)
- Teil II:** Ergänzungen und weitere Klauseln gemäß Klausel 2 a) und b) der Standardvertragsklauseln
- Teil III:** Anhänge I-IV

Teil I: Standardvertragsklauseln

Abschnitt I

Klausel 1

Zweck und Anwendungsbereich

- a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)] sichergestellt werden.
- b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
- c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- d) Die Anhänge I bis IV sind Bestandteil der Klauseln.
- e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

- a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
- b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 Auslegung

- a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen besneidet.

Klausel 4 Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ Kopplungsklausel

- bewusst freigelassen –

Abschnitt II Pflichten der Parteien

Klausel 6 Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 Pflichten der Parteien

7.1. Weisungen

- a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

- b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

- a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
- b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

- a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der

Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

- d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

- a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 7 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.
- b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.
- e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den

Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

- a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.
- b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

- a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
- b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:
 - 1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
 - 2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
 - 3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

- 4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679].
- d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
- b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
- 1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - 2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - 3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

- c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679], die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679] zu unterstützen.

Abschnitt III Schlussbestimmungen

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

- a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - 1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 - 2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;
 - 3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der

Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

- 4) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
- 5) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Teil II: Ergänzungen und weitere Klauseln gemäß Klausel 2 a) und b) der Standardvertragsklauseln

In diesem Teil folgen Ergänzungen gemäß Klausel 2 a) und weitere Klauseln gemäß Klausel 2 b). Hierbei handelt es sich um Ergänzungen und Präzisierungen.

Ergänzung zu 7.1:

- a) Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen nach Überprüfung bestätigt oder geändert werden. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien bzw. einer Haftungsfreistellung für den Auftragsverarbeiter durch den Verantwortlichen auszusetzen.
- b) Weichen die weiteren Weisungen des Verantwortlichen im Sinne der Klausel 7.1.a) Satz 3 von den im Hauptvertrag festgelegten Vereinbarungen ab und führen diese zu einem im Verhältnis zur Vergütung entsprechend dem Hauptvertrag unverhältnismäßigen Mehraufwand beim Auftragsverarbeiter, so kann der Auftragsverarbeiter vom Verantwortlichen eine dem Aufwand entsprechende Vergütung zu den jeweils aktuellen Sätzen verlangen.

Ergänzung zu 7.5:

- a) Da der Auftragnehmer auch Dienste anbietet /anbieten könnte, im Rahmen derer es generell möglich wäre, dass sensible Daten, wie z.B. politische Meinungen, religiöser oder weltanschauliche Überzeugungen enthalten sind, wird generell bei der Verarbeitung aller personenbezogener Daten im Rahmen der unterschiedlichen angebotenen Dienste ein erhöhter Sicherheitsstandard angewandt. Dies ist in den ToMs berücksichtigt (siehe Anhang III).
- b) Die Verantwortung für die rechtmäßige Erhebung und Übermittlung der dieser Daten liegt beim Auftraggeber.

Ergänzung zu 7.6:

Der Verantwortliche und der Auftragsverarbeiter sind sich einig, dass

- a) eine Überprüfung nach c) höchstens (1) mal pro Kalenderjahr angemessen ist, wenn nicht ein Verstoß des Auftragsverarbeiters dazu Anlass gegeben hat.
- b) Prüfungen im Sinne d) mindestens 14 Tage im Voraus anzukündigen sind und zu den jeweils üblichen Geschäftszeiten ohne übermäßige Störung des Betriebsablaufes vorzunehmen sind.
- c) der Auftragsverarbeiter die Prüfung von der Unterzeichnung einer Verschwiegenheitserklärung - auch hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen - abhängig machen kann. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn der Prüfer einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.
- d) der Auftragsverarbeiter den Einsatz eines externen Prüfers ablehnen kann, wenn dieser in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht.
- e) der Auftragsverarbeiter für die Unterstützung bei der Durchführung der Prüfung eine angemessene Vergütung verlangen kann, die sich nach dem Aufwand und den jeweils aktuellen Tagessätzen richtet.

Ergänzung zu Klausel 8:

Für Aufwendungen im Rahmen der Klausel 8 kann der Auftragsverarbeiter vom Verantwortlichen eine angemessene Vergütung beanspruchen, wenn diese Unterstützungsleistung nicht in der Leistungsbeschreibung des Hauptvertrages enthalten und nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen ist.

Weitere Klausel: Rechtswahl / Gerichtsstand

- a) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- b) Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.
- c) Gerichtsstand ist Frankfurt am Main.

Anhang I

zum

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen

Liste der Parteien

1. Verantwortliche(r):

Der Verantwortliche ist der Nutzer/Kunde entsprechend der Trust Call Nutzungsbedingungen des beauftragten/gebuchten Dienstes gemäß Hauptvertrag sowie der Allgemeinen Geschäftsbedingungen (AGB) der Trust Call GmbH.

Name: Ergibt sich aus den Vertragsunterlagen (Hauptvertrag) entsprechend der Beauftragung/Buchung bzw. Anmeldung des Nutzers/Kunden.

Anschrift: Ergibt sich aus den Vertragsunterlagen (Hauptvertrag) entsprechend der Beauftragung/Buchung bzw. Anmeldung des Nutzers/Kunden.

Unterschrift und Beitrittsdatum:

Erfolgt durch Zustimmung zu den Allgemeinen Geschäftsbedingungen (AGB) und Zustimmung zu dem AVV in Form der EU-Standardvertragsklausel durch den Nutzer/Kunden.

2. Auftragsverarbeiter:

Name: Trust Call GmbH

Anschrift: Lurgiallee 12, 60431 Frankfurt am Main, Deutschland

Name, Funktion und Kontaktdaten der Kontaktperson: Axel Reddehase, Geschäftsführer, Lurgiallee 12, 60431 Frankfurt am Main, Deutschland

Name, Kontaktdaten des Datenschutzbeauftragten: Harald Eul, HEC Harald Eul Consulting GmbH, Datenschutz + Datensicherheit, Auf der Höhe 34, 50321 Brühl, E-Mail: datenschutz@trustcall.de

Unterschrift und Beitrittsdatum:

Erfolgt durch Zustimmung zu den Allgemeinen Geschäftsbedingungen (AGB) und Zustimmung zu dem AVV in Form der EU-Standardvertragsklausel durch den Kunden.

Anhang II

zum

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen

Beschreibung der Verarbeitung

1. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Nutzer/Administratoren des Dienstes gemäß Hauptvertrag
- Kunden und Interessenten/Geschäftspartner des Auftraggebers bzw. Kunden und Interessenten/Geschäftspartner von Auftraggebern des Auftraggebers
- Dritte, sonstige Personen, die in SMS oder Bestätigungstexten erwähnt werden

2. Kategorien personenbezogener Daten, die verarbeitet werden:

- Identifikationsdaten, wie Name, E-Mail-Adresse, Nutzer-ID der Administratoren/Nutzer und gegebenenfalls Telefonnummern im Rahmen der Verifizierung sowie Softwarenutzungsdaten
- Technische SMS-Daten: Zielrufnummer, Versand- bzw. Empfangszeitpunkte (Start, Ende), Zustellungsinformationen
- Vom Nutzer eingegebene oder via REST-Schnittstelle übermittelte Daten von Kunden und Interessenten/Geschäftspartner (Telefonnummern, individualisierte Parameter wie z. B. Adress- und Kommunikationsdaten, Vornamen, Namen, Anschriften, Vertragsdaten, Bank- und Kreditkartenverbindung oder andere kundenspezifische Daten).
- Da die Nutzer in ConfirmationCheck SMS- oder Bestätigungstexte mit beliebigen Parametern erstellen und verarbeiten können, kann nicht ausgeschlossen werden, dass auch sensible Daten im Sinne von § 9 DSGVO (siehe unter 3.) verarbeitet werden, wie z. B. Gesundheitsdaten.

3. Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen, Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:

- Da die Nutzer in ConfirmationCheck SMS- oder Bestätigungstexte mit beliebigen Parametern erstellen und verarbeiten können, kann nicht ausgeschlossen werden, dass auch sensible Daten im Sinne von § 9 DSGVO, wie
 - Genetische Daten
 - Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
 - Gesundheitsdaten
 - Rassistische und ethnische Herkunft
 - Politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder
 - Gewerkschaftszugehörigkeit
 - Daten zum Sexualleben oder der sexuellen Orientierung

verarbeitet werden.

4. Art der Verarbeitung:

- Die Verarbeitung erfolgt wie im Hauptvertrag einschließlich der Dienstbeschreibung beschrieben.

5. Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

- Ergibt sich aus dem Hauptvertrag.

6. Dauer der Verarbeitung

- Entsprechend der Dauer des Hauptvertrages.

Anhang III

zum

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Daten

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen Beispiele für mögliche Maßnahmen:

1. Präambel

Unter Berücksichtigung des Standes der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung – ebenso wie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere möglicher Risiken für die Rechte und Freiheiten natürlicher Personen – vereinbaren der Auftraggeber und der Auftragnehmer nachfolgend die erforderlichen technischen und organisatorischen Maßnahmen (TOM). Diese gelten für die im Hauptvertrag spezifizierten IT-Leistungen, die in den unter Ziffer 2 aufgeführten Rechenzentren erbracht werden.

Bei der Auswahl und Ausgestaltung der Maßnahmen wurden die in Art. 32 Abs. 1 lit. b DSGVO definierten Schutzziele – Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der Systeme und Dienste – umfassend berücksichtigt. Darüber hinaus ist gewährleistet, dass im Falle eines physischen oder technischen Zwischenfalls eine zeitnahe Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten erfolgen kann. Die Angemessenheit und Wirksamkeit sämtlicher technischer und organisatorischer Maßnahmen wird regelmäßig gemäß Art. 32 Abs. 1 lit. d DSGVO überprüft und bei Bedarf angepasst.

2. Geltungsbereich

Umfasst die Haupt-Infrastrukturbestandteile, die für den Betrieb der Plattform genutzt werden. Diese befinden sich primär bei der Trust Call GmbH am Standort Frankfurt (Lurgiallee 12, 60439 Frankfurt/Main), sowie dem Rechenzentrumsbetreiber PlusServer GmbH an den Standorten CGN 3.1/3.2 (Welserstr. 14, 51149 Köln) und DUS 6.1 (In der Steele 33a, 40599 Düsseldorf).

Darüber hinaus werden weitere Rechenzentrumsbetreiber zur Unterstützung, Lastverteilung, Ausfallsicherheit und Bereitstellung besonderer Dienste genutzt, die der Anlage B „Trust Call_Liste Unterauftragnehmer_AV SAAS_tt_de.pdf“ entnommen werden können.

3. Technische und organisatorische Maßnahmen

3.1. Pseudonymisierung

Konzept:

Verarbeitung personenbezogener Daten in der Weise, dass die Daten ohne Hinzuziehung zusätzlicher, gesondert aufbewahrter und gesicherter Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Umsetzung:

- Sofern notwendig und weitestgehend systemisch unterstützt, werden Identifikationsmerkmale (z.B. Name durch ein Kennzeichen) ersetzt oder gar anonymisiert.
- Sorgfältige Auswahl datenschutzfreundlicher IT-Systeme.
- Nutzung datenschutzfreundlicher Voreinstellungen der sich im Einsatz befindlichen IT-Systeme.
- Einsatz entsprechender Verschlüsselungsmechanismen im Zusammenhang mit Pseudonymisierung.

3.2. Verschlüsselung

Konzept:

Transformation von Klartext in Geheimtext mittels Schlüssel, um Unentzifferbarkeit für Unbefugte zu gewährleisten.

Umsetzung:

- Administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen (z.B. HTTPS, SFTP).
- Daten auf den Server-Systemen werden auf verschlüsselten Datenträgern gespeichert; entsprechende Festplattenverschlüsselungssysteme sind im Einsatz.
- Bei der Kommunikation zwischen Mandanten und der Plattform werden relevante Daten stets verschlüsselt übertragen.
- Remote-Zugriffe auf IT-Systeme erfolgen stets über verschlüsselte Verbindungen.

3.3. Fähigkeit der Vertraulichkeit

Konzept:

- Personenbezogene Daten sind vor unbefugter Preisgabe geschützt.

3.3.1 Zutrittskontrolle

Unbefugten wird der „körperliche“ Zutritt zu Datenverarbeitungsanlagen verwehrt.

Umsetzung:

- Einsatz von Magnet- / Chipkarten, Schlüssel.
- Dienstanweisung zur Handhabung von Zutrittskontrollkarten.
- Überwachungseinrichtung und Alarmanlage.
- Server befinden sich in verschlossenen Räumen.
- Festlegung von Sicherheitsbereichen.
- Sicherung des Serverraums mittels Sicherheitsschlösser und Überwachungseinrichtung.
- Server in abschließbaren Serverschränken untergebracht.
- Serverschrankschlüssel gesichert durch Schlüsselsafe.
- Aufbewahrung von Sicherungen im zutrittsgeschützten Safe.
- Zutrittsberechtigungen werden erst erteilt, wenn dies durch Vorgesetzten und/oder Personalabteilung angefordert wurde, nach dem Grundsatz der Erforderlichkeit.
- Schlüsselvergabe und -management erfolgt nach einem definierten Prozess (Erteilung/Entzug bei Beginn/Ende Arbeitsverhältnis).

3.3.2. Zugangskontrolle

Unbefugte Nutzung von Datenverarbeitungssystemen wird verhindert.

Umsetzung:

- Serversysteme nur nach mindestens passwortgestützter lokaler bzw. zentraler Authentifizierung nutzbar.
- Eindeutige Zuordnung von Benutzerkonten.
- Verbindliche Regelungen für das Passwortverfahren und Richtlinie zum sicheren Umgang mit Passwörtern, orientiert am BSI Maßnahmenkatalog (speziell Maßnahme 2.11).
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre bei vorübergehender Nichtbenutzung.
- Automatische Standardroutinen für regelmäßige Aktualisierungen von Schutzsoftware.
- Nutzung von Hardware- und Software-Firewalls und Virens Scanner auf Clients und Servern.
- Zugangsberechtigungen werden von Administratoren auf Antrag von Vorgesetzten vergeben.
- Fremdpersonal hat keinen Zugang zu diesen Systemen.
- Alle relevanten Server verfügen über Virenschutzsoftware mit tagesaktueller Versorgung mit Signaturupdates.
- Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.
- Zugriff von Servern auf das Internet und Zugriff auf diese Systeme über das Internet sind durch Firewalls gesichert, nur erforderliche Ports sind nutzbar.

3.3.3. Zugriffskontrolle

Berechtigte können ausschließlich auf Daten zugreifen, für die sie Zugriffs-berechtigung haben.

Umsetzung:

- Authentisierung auf Betriebssystemebene erforderlich.
- Separate Authentisierung und Berechtigungsvergabe auf Anwendungsebene.
- Anzahl der Administratoren auf das „Notwendigste“ reduziert.
- Passworrichtlinie inkl. Passwortlänge, Passwortwechsel.
- Authentisierung gegenüber zentralem Verzeichnisdienst, lokalem Betriebssystem, Applikation.
- Trennung von Berechtigungsbewilligung (organisatorisch durch Abteilungsleitung oder Geschäftsführung) und Berechtigungsvergabe (technisch durch IT-Abteilung).
- Verbindliches Konzept der Laufwerksnutzung und –zuordnung.
- Berechtigungen werden ausschließlich von Administratoren eingerichtet.
- Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben.
- Voraussetzung ist eine entsprechende Anforderung der Berechtigung durch einen Vorgesetzten.
- Rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen nach Aufgaben- und ggf. Projektgebiet.
- Nutzung systemisch unterstützter Authentisierungsmechanismen auf Anwendungsebene, sofern unterstützt (Zweifaktor-Authentifizierung).
- Mobile Datenträger / Geräte (Laptops) werden durch separate Verschlüsselungsmethoden geschützt (bis auf Betriebsebene).
- Verwendung von Sichtschutzfolien bei Laptops im Außeneinsatz.
- Installieren nicht genehmigter Software auf IT-Systemen ist grundsätzlich untersagt.
- Alle Server-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

3.3.4. Trennungskontrolle

Zu unterschiedlichen Zwecken erhobene Daten werden getrennt voneinander verarbeitet.

Umsetzung:

- Interne Funktionstrennung durch Verarbeitung von unterschiedlichen Mitarbeitern bei unterschiedlichen Verarbeitungszwecken (z.B. Administration und User).
- Einsatz eines Berechtigungskonzepts, das der getrennten Verarbeitung der Daten Rechnung trägt.
- Jeder datenschutzrelevante Datenbestand wird nach Mandant und vertraglicher Relevanz in unterschiedlichen Schichten gelagert.
- Zugriffsrechte auf dem Filesystem und Rechtevergabe führen zu einer transparenten Trennung von Datenbeständen je nach Vertrag, Aktion, Mandant und Zugriffsnotwendigkeit durch die Anwender.
- Die Trennung von Daten verschiedener Kunden ist stets gewährleistet.
- Strikte Trennung der Netze zwischen Test-, Entwicklungsabteilung und Projektleitung, Support.

3.4. Fähigkeit der Integrität

Konzept:

Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen; Daten sind vollständig und unverändert.

3.4.1. Weitergabekontrolle

Verhindern unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern und Nachvollziehbarkeit der Datenübermittlung.

Umsetzung:

- Einsatz von verschlüsselten Datenleitungen (HTTPS, SFTP, VPN).
- Legitimationsprüfungen von (Empfangs-) Berechtigten.
- Datenschutzgerechte Vernichtung von Papierdokumenten (nach ISO/IEC 21964), Einsatz von Aktenvernichtern.
- Datenschutz- und datensicherheitsgerechte Vernichtung von elektronischen Datenträgern bei Entsorgung (nach ISO/IEC 21964, ggf. durch Spezialisten nach BSI-Empfehlung für höchste Anforderungen).
- Einsatz von Verschlüsselung von mobilen Datenträgern (Laptops, USB-Sticks usw.).
- Der Datenaustausch und die Kommunikation zwischen Mandanten und der Plattform erfolgen stets verschlüsselt.
- Begrenzte Kommunikation auf Basis von E-Mail zwischen Mandanten und Plattform.
- Der Zugriff auf die Daten im System obliegt nur den jeweiligen Mitarbeitern der Mandanten oder erfolgt auf Weisung des Auftragsgebers durch die Administratoren der Trust Call GmbH.
- Das Datenschutzkonzept ist durch Betriebsanweisungen geregelt und an die Mitarbeiter kommuniziert.

3.4.2. Eingabekontrolle

Gewährleistung der Nachprüfbarkeit von Datenverarbeitungsvorgängen (Wer, Wann, Was bei Eingabe/Änderung/Löschung).

Umsetzung

- Festlegung von Benutzerprofilen.
- Differenzierte Benutzerberechtigungen (Lesen, Ändern, Löschen; Nur Teilzugriffe auf Daten und Funktionen).
- Automatische Protokollierung von Änderungen in Anwendungen und Betriebssystemen.
- Die Eingabe, Änderung und Löschung personenbezogener Daten wird grundsätzlich protokolliert.
- Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten (Benutzeraccounts dürfen nicht geteilt/gemeinsam genutzt werden).
- Nutzung systemischer Protokollierungsmöglichkeiten der Anwendungen.

3.5. Fähigkeit der Verfügbarkeit

Konzept:

Gewährleistung, dass Dienstleistungen, IT-Systeme, Anwendungen oder Informationen stets wie vorgesehen genutzt werden können; Schutz gegen zufällige Zerstörung oder Verlust (z.B. Wasserschäden, Feuerschäden, Stromausfall).

Umsetzung:

- Einsatz von Schutzprogrammen (Virens Scanner, Hardware- und Software-Firewall, Verschlüsselungsprogramme, SPAM-Filter, Live-Guard Zero-Day-Protection).
- Abweisung von unberechtigten Benutzern.
- Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte in den Serverräumen und Büros.
- Klimaanlage in den Serverräumen.
- Daten auf Serversystemen werden mindestens täglich inkrementell und wöchentlich vollgesichert.
- Die Sicherungen werden verschlüsselt an einem physisch getrennten Ort gespeichert.
- Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung.
- Im Serverraum befindet sich eine Brandmeldeanlage.
- Im Serverraum befindet sich eine CO₂-Löschanlage.
- Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

3.6. Fähigkeit der Belastbarkeit

Konzept:

Systeme sind widerstandsfähig, so dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

Umsetzung:

- Die unter Ziffer 3.5. („Fähigkeit der Verfügbarkeit“) dargestellten Maßnahmen tragen maßgeblich zur Belastbarkeit der IT-Systeme bei.

3.7. Wiederherstellbarkeit der Verfügbarkeit und des Zugangs

Konzept:

Rasche Wiederherstellbarkeit der Daten nach einem eingetretenen Datenverlust oder Sicherheitsvorfall.

Umsetzung:

- Einsatz unterbrechungsfreier Stromversorgung.
- Vollständiges Backup- und Recoverykonzept mit täglichen Sicherungen.
- Tägliches Backup nach dem Generationsprinzip von relevanten Systemen.
- Es wird regelmäßig über den aktuellen Stand der Sicherungen informiert.
- Eine Rückspielung zum Test wird regelmäßig durchgeführt.

3.8. Verfahren zur regelmäßigen Überprüfung

Konzept:

Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen.

Umsetzung:

- Datenschutzhandbuch inklusive Incident-Response-Management.
- Notfallpläne für unterschiedliche Szenarien.
- Regelmäßige Schulungen der Beschäftigten.
- Regelmäßige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten.
- Im Datenschutzhandbuch sind die Regeln zum Umgang mit personenbezogenen Daten definiert.
- Die Ziele des Datenschutzes und die Einhaltung der DSGVO-Vorgaben sind in der Leitlinie zu Datenschutz und Informationssicherheit festgehalten. Die dort beschriebenen Maßnahmen werden regelmäßig geschult.
- Es ist sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich gemeldet werden.

3.9. Unrechtmäßiger Zugang zu personenbezogenen Daten

Konzept:

Verhinderung von unrechtmäßigem Zugang zu personenbezogenen Daten.

Umsetzung:

- Dies wird durch die unter Ziffer 4.3 („Fähigkeit der Vertraulichkeit“), insbesondere durch die Maßnahmen zur Zugangs- und Zugriffskontrolle, gewährleistet.

3.10. Verarbeitung personenbezogener Daten nur nach Anweisung

Konzept:

Gewährleistung, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden.

Umsetzung:

- (Es existieren Produkt bezogene Löschkonzepte; relevante, Mandanten bezogene Daten werden spätestens 14 Tage nach Beendigung des Vertragsverhältnisses datenschutzkonform gelöscht).
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer sind vereinbart (impliziert durch Audit und regelmäßige Kontrollen während des Vertragsverhältnisses).
- Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union. Sorgfältige Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere Datensicherheit).
- Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen (z.B. durch Audit durch den Datenschutzbeauftragten).

- Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers.
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis.
- Auftragnehmer hat Datenschutzbeauftragten bestellt (bei der Trust Callt GmbH ist ein externer Datenschutzbeauftragter benannt).
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

Anhang IV

zum

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen

Liste der Unterauftragsverarbeiter

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter (einschließlich Unterunterauftragsverarbeiter) genehmigt:

Name und Anschrift des Unterauftragnehmers / Unterunterauftragsverarbeiter	Beschreibung der Teilleistungen	Ort der Leistungserbringung
ttUnited GmbH Lurgiallee 12 60439 Frankfurt am Main	Betrieb, Wartung, Support der Cloud-Infrastruktur	Deutschland
Tribe Technologies GmbH Lurgiallee 12 60439 Frankfurt am Main	3d-Level Support	Deutschland
PlusServer GmbH Hohenzollernring 72 50672 Köln	Rechenzentrumsbetreiber	Standorte: Rechenzentrum CGN 3.1 / 3.2 Welserstr. 14 51149 Köln Rechenzentrum DUS 6.1 In der Steele 33a 40599 Düsseldorf
IONOS SE Elgendorfer Str. 57 56410 Montabaur	Rechenzentrumsbetreiber	Standorte: Rechenzentrum Berlin
Contabo GmbH Aschauer Straße 32a 81549 München	Rechenzentrumsbetreiber	Standorte: Rechenzentrum Nürnberg Rechenzentrum Karlsruhe Rechenzentrum Düsseldorf