NUTZUNGSBESTIMMUNGEN FÜR NUTZUNG DER INSIDERS CLOUD ZU TESTZWECKEN

INSIDERS TECHNOLOGIES

Nutzungsbestimmungen für Nutzung der Insiders Cloud zu Testzwecken

(nachfolgend „Vertrag“ genannt); Stand 01.02.2024

Die Insiders Technologies GmbH (nachfolgend „Insiders“ genannt) ermöglicht die Nutzung aller vertragsgegenständlichen cloudbasierten Services zu Testzwecken ausschließlich auf Grundlage dieses Vertrages. Die nachfolgenden Bedingungen gelten ausschließlich für den Geschäftsverkehr mit Unternehmern, juristischen Personen des öffentlichen Rechts oder öffentlich-rechtlichem Sondervermögen; **Insiders bietet die vertragsgegenständlichen Leistungen gegenüber Verbrauchern nicht an.** Abweichende Geschäftsbedingungen des Auftraggebers werden nicht Vertragsbestandteil, auch wenn Insiders ihrer Geltung nicht widerspricht, es sei denn, sie werden von Insiders ausdrücklich schriftlich anerkannt. Die Ausführung von Leistungen durch Insiders bedeutet keine Anerkennung von Vertragsbedingungen des Auftraggebers.

Die gegebenenfalls bestehende Leistungsbeschreibung des / der zu Testzwecken zugänglich gemachten Services sowie die Vereinbarung über Auftragsverarbeitung werden gemeinsam mit dem vorliegenden Vertrag abgeschlossen. Sie bilden einen wesentlichen Bestandteil des Vertrages und gelten im Fall von Widersprüchen oder Unklarheiten vorrangig.

---

1 Definitionen

1.1 „Autorisierte Nutzer“ sind die Nutzer, die die Cloud-Lösung für den Auftraggeber zu Testzwecken nutzen. Als autorisierte Nutzer kommen ausschließlich Arbeitnehmer, Leiharbeitnehmer sowie zur Berufsbildung Beschäftigte des Auftraggebers in Betracht. Andere Dritte gelten nicht als autorisierte Nutzer.

1.2 „Cloud-Lösung“ bezeichnet die von Insiders bereitgestellte Cloud-Computing-Plattform Insiders Cloud, über die Insiders die in der jeweiligen Leistungsbeschreibung näher definierten cloudbasierten Services erbringt. Die Cloud-Lösung wird dem Auftraggeber mittels SaaS zur Verfügung gestellt. Die Cloud-Lösung umfasst nicht die Applikationen (Apps), über die der Auftraggeber bzw. die von ihm autorisierten Nutzer über mobile oder stationäre Endgeräte auf die Cloud-Lösung zugreifen.

1.3 „Insiders“ meint die Insiders Technologies GmbH, Brüsseler Straße 1, 67657 Kaiserslautern, Deutschland.

1.4 “Kundendaten” sind alle Daten und Informationen, gleich welcher Art, die durch den Auftraggeber bzw. die von ihm autorisierten Nutzer bei der Nutzung der Services der Cloud-Lösung zu Testzwecken in die Cloud-Lösung eingespielt und dort verarbeitet und genutzt werden. Die Kundendaten können auch personenbezogene Daten im Klartext oder pseudonymisiert enthalten.

1.5 „SaaS“ ist die Abkürzung für Software-as-a-Service und bedeutet, dass dem Auftraggeber die Funktionen der Cloud-Lösung mit der ihr zugrunde liegenden Software als reiner Service über das Internet zur Nutzung zur Verfügung gestellt werden, ohne dass die Software dem Auftraggeber oder Nutzern überlassen wird. Weder der Auftraggeber noch die von ihm autorisierten Nutzer erhalten also eine Kopie der Software und können sie daher auch nicht auf eigenen Systemen installieren und betreiben.

1.6 „Verarbeitungsergebnis“ ist das durch die Nutzung der Services der Cloud-Lösung erzeugte Ergebnis, das die Cloud-Lösung dem Auftraggeber bzw. den von ihm autorisierten Nutzern zu Testzwecken anzeigt. Der Inhalt des Verarbeitungsergebnisses (z.B. Darstellung eines Datenextraktes) ergibt sich aus der jeweiligen Leistungsbeschreibung.

2 Vertragsgegenstand und Nutzungsrechte

2.1 Insiders gewährt dem Auftraggeber während der Laufzeit dieses Vertrages und nach Maßgabe der darin getroffenen Vereinbarungen das beschränkte, nicht-ausschließliche und kostenfreie Recht, die Services der Cloud-Lösung mit dem in der einschlägigen Leistungsbeschreibung vereinbarten Funktionsumfang ausschließlich zu Testzwecken zu nutzen bzw. durch seine autorisierten Nutzer nutzen zu lassen. Eine Nutzung für den produktiven Einsatz und insbesondere die Verarbeitung von Kundendaten für den regulären Geschäftsbetrieb ist ausdrücklich nicht gestattet.

2.2 Der Auftraggeber ist nicht berechtigt, die Cloud-Lösung oder einzelne Services der Cloud-Lösung an Dritte weiter zu verleihen, zu vermieten oder sie anderen Nutzern als den zulässigen autorisierten Nutzern zugänglich zu machen.

2.3 Der Zugriff des Auftraggebers bzw. seiner autorisierten Nutzer erfolgt über eine Internetverbindung. Diese Netzanbindung sowie die für den Zugriff notwendigen Geräte und Applikationen sind nicht Bestandteil der Cloud-Lösung und obliegen der Verantwortung des Auftraggebers.

2.4 Die technische Umgebung des Testsystems für die vereinbarten Services wird als virtualisierte Infrastruktur von Insiders betrieben und in einem in der EU, dem EWR oder der Schweiz gelegenen Rechenzentrum gehostet.

3 Änderungen der Cloud-Lösung

Insiders betreibt die Cloud-Lösung und ist berechtigt, ihre Funktionen und ihre Schnittstellen jederzeit nach eigenem Ermessen zu aktualisieren, um die Cloud-Lösung zu verbessern, weiter zu entwickeln oder an neue oder geänderte Anforderungen anzupassen.

4 Umgang mit Kundendaten

4.1 Insiders ist befugt, im Rahmen der Vertragsdurchführung und -erfüllung mittels der Cloud-Lösung die durch den Auftraggeber bzw. die von ihm autorisierten Nutzer in die Cloud-Lösung eingespielten Kundendaten dort zu verarbeiten und zu nutzen. Der Auftraggeber übernimmt die volle Verantwortung dafür, dass alle betroffenen Kundendaten von Insiders im Rahmen der Vertragsdurchführung und -erfüllung verarbeitet und genutzt werden dürfen. Insiders erkennt an, dass die Kundendaten im Verhältnis zum Auftraggeber jederzeit dem Auftraggeber zustehen. Soweit Kundendaten personenbezogene Daten enthalten und Insiders diese als Auftragsverarbeiter verarbeitet, ist der Auftraggeber gegenüber Insiders Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

4.2 Die Cloud-Lösung von Insiders basiert auf maschinellen Lernverfahren. Eine Weiterentwicklung und Verbesserung der Cloud-Lösung erfordert ein Training der zugrundeliegenden Software mit Echtdaten. Sogenannte Dummy-Daten sind für solche Trainingszwecke ungeeignet. Deshalb verarbeitet Insiders die vom Auftraggeber in die Cloud-Lösung eingespielten Kundendaten auch für die rechtmäßige Geschäftstätigkeit von Insiders und damit für die nachfolgend eingeschränkten eigenen Zwecke. Diese rechtmäßige Geschäftstätigkeit von Insiders umfasst (i) die Verbesserung der Funktionalität der Cloud-Lösung, (ii) das Training und die Optimierung der Cloud-Lösung

sowie (iii) die Nutzung von während der Verarbeitung der Kundendaten generierten Statistikdaten. Insiders nutzt die im Rahmen ihrer rechtmäßigen Geschäftstätigkeit verarbeiteten Kundendaten ausschließlich zu den vorstehend unter (i) bis (iii) genannten Zwecken und in keiner Weise, um die Kundendaten für vertriebliche oder andere kommerzielle Zwecke zu verarbeiten oder zu verwerten, Personen zu kontaktieren oder deren Daten an Dritte weiterzugeben. Insbesondere findet keinerlei Profiling im Sinne von Art. 4 Nr. 4 DSGVO statt. Personenbezogene Daten besonderer Kategorien werden von Insiders im Rahmen der rechtmäßigen Geschäftstätigkeit nicht verarbeitet. Bei den unter (iii) aufgeführten Statistikdaten handelt es sich um anonymisierte Daten, die keinen Rückschluss auf Personen zulassen. Soweit Kundendaten personenbezogene Daten enthalten und Insiders diese für ihre rechtmäßige Geschäftstätigkeit verarbeitet, ist Insiders gegenüber den betroffenen Personen Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

4.3 Insiders ist verpflichtet, mit wirtschaftlich angemessenem Aufwand dafür zu sorgen, dass die Integrität der Kundendaten und Verarbeitungsergebnisse geschützt und diese sorgfältig verarbeitet werden. Dabei wird Insiders mindestens branchenübliche Sicherheitsstandards verwenden. Die Kundendaten und Verarbeitungsergebnisse müssen logisch von den Kundendaten aller anderen Kunden getrennt werden.

4.4 Insiders ist verpflichtet, alle Kundendaten und Verarbeitungsergebnisse auf den Systemen der Cloud-Lösung unwiederbringlich und vollständig innerhalb von vierzehn (14) Tagen zu löschen. Der Auftraggeber hat keinen Anspruch auf eine darüber hinausgehende Speicherung der Kundendaten und Verarbeitungsergebnisse durch Insiders. Insiders wird die Kundendaten und Verarbeitungsergebnisse jedoch über das Vertragsende hinaus speichern, soweit und solange sie dazu verpflichtet ist (z. B. im Rahmen gesetzlicher Aufbewahrungspflichten); die Kundendaten und Verarbeitungsergebnisse werden in solchen Fällen für die Verarbeitung zu anderen Zwecken jedoch gesperrt.

4.5 Der Auftraggeber darf keine Informationen, Programme oder andere datenschutzrechtlich, urheberrechtlich oder anderweitig durch gewerbliche, persönlichkeitsrechtliche oder sonstige Schutzrechte geschützten Materialien oder Daten in die Cloud-Lösung einspielen oder seinen autorisierten Nutzern gestatten, solche einzuspielen, ohne hierzu über die erforderlichen Rechte zu verfügen. Gleichermaßen ist es dem Auftraggeber untersagt, verbotene Informationen, Programme, Materialien oder Daten (z.B. terroristische, kinderpornographische oder rassistische Inhalte) in die Cloud-Lösung einzuspielen oder den von ihm autorisierten Nutzern dies zu gestatten.

5 Sperrung

Wenn der Auftraggeber oder irgendein Dritter (insbesondere ein autorisierter Nutzer), der die Infrastruktur oder Zugangsdaten (Credentials) des Auftraggebers nutzt, die Cloud-Lösung für (Distributed) Denial-of-Service-Angriffe, Spamming oder sonstige rechts- oder vertragswidrige Aktivitäten (nachfolgend zusammenfassend „schädigende Aktivitäten“ genannt) verwendet oder sie darüber veranlasst, darf Insiders den Zugang des Auftraggebers oder von ihm autorisierter Nutzer zur Cloud-Lösung sperren, bis der

Auftraggeber Maßnahmen zur Unterbindung der fortgesetzten schädigenden Aktivitäten ergriffen und damit für die Beendigung der schädigenden Aktivitäten gesorgt hat. Der Auftraggeber verpflichtet sich gegenüber Insiders in Bezug auf von ihm und seinen autorisierten Nutzern zu vertretende schädigende Aktivitäten zum Schadensersatz und zur Schadloshaltung.

6 Sach- und Rechtsmängelhaftung

6.1 Insiders haftet im Rahmen der kostenfreien Zugänglichmachung der Cloud-Lösung für Testzwecke nur auf Ersatz des Schadens, der dem Auftraggeber aus Mängeln entsteht, wenn Insiders den jeweiligen Mangel der zugänglich gemachten Cloud-Lösung arglistig verschwiegen hat.

6.2 Alle anderen Ansprüche auf Sach- und Rechtsmängelhaftung sind ausdrücklich ausgeschlossen.

7 Haftung

7.1 Insiders haftet im Rahmen der kostenfreien Zugänglichmachung der Cloud-Lösung für Testzwecke nur für Vorsatz und grobe Fahrlässigkeit.

7.2 UNTER KEINEN UMSTÄNDEN HAFTET INSIDERS GEGENÜBER DEM AUFTRAGGEBER FÜR SCHÄDEN, DIE ÜBER DIE IN ZIFFER 7.1 VEREINBARTE HAFTUNG HINAUSGEHEN.

7.3 Die in dieser Ziffer 7 vereinbarten Haftungsbeschränkungen gelten auch zu Gunsten der gesetzlichen Vertreter und Erfüllungsgehilfen von Insiders.

7.4 Die vorstehenden Regelungen dieser Ziffer 7 finden entsprechend Anwendung, wenn Insiders an Stelle von Schadensersatz Aufwendungsersatz zu leisten hat.

8 Vertragslaufzeit und Kündigung

8.1 Der Vertrag wird für einen bestimmten Zeitraum, welcher in der Leistungsbeschreibung definiert wird, abgeschlossen und endet danach automatisch.

8.2 Das Recht auf außerordentliche fristlose Kündigung aus wichtigem Grund bleibt unberührt.

9 Geheimhaltung

9.1 Mit der Cloud-Lösung verarbeitete Kundendaten und Verarbeitungsergebnisse gelten als vertrauliche Informationen, mit Ausnahme von Informationen, (i) die ohne Geheimhaltungspflicht und ohne Verschulden von Insiders, ihrer Erfüllungs- oder Verrichtungsgehilfen oder Vertreter allgemein für die Öffentlichkeit zugänglich sind, (ii) die unabhängig von Insiders, ihren Erfüllungs- oder Verrichtungsgehilfen oder Vertretern ohne Nutzung der Kundendaten entwickelt wurden, (iii) die ohne Geheimhaltungspflicht rechtmäßig aus anderen Quellen stammen, (iv) die aufgrund einer gesetzlichen Regelung oder gerichtlichen bzw. behördlichen Anordnung bekannt gegeben werden müssen oder (v) deren Bekanntgabe vom Auftraggeber gestattet wurde. Insiders wird vertrauliche Informationen nicht an Dritte weitergeben, angemessene Sicherheitsmaßnahmen zum Schutz vertraulicher Informationen ergreifen und deren unberechtigte Bekanntgabe verhindern.

9.2 Der Auftraggeber verpflichtet sich, alle vertraulichen Informationen, die ihm Insiders im Zusammenhang mit dem Vertrag zugänglich macht (z.B. Zugangsdaten, Dokumentationen, Reports, Beschreibungen technisch-organisatorischer Maßnahmen, Sicherheitskonzepte), vertraulich zu behandeln und ausschließlich zur Erfüllung des Vertrages zu verwenden. Für den Missbrauch der dem Auftraggeber überlassenen Zugangsdaten trägt der Auftraggeber gegenüber Insiders die Verantwortung.

9.3 Die Geheimhaltungspflichten gelten auch über das Ende dieses Vertrages hinaus.

10 Sonstige Bestimmungen

10.1 Dieser Vertrag, einschließlich seiner Leistungsbeschreibungen für die zu Testzwecken bereitgestellten Services und der Vereinbarung über Auftragsverarbeitung, die zusammen einen integralen Bestandteil des Vertrages bilden, decken in Bezug auf den Vertragsgegenstand sämtliche vertraglichen Vereinbarungen zwischen den Vertragspartnern vollständig ab.

10.2 Sollten einzelne Bestimmungen dieses Vertrages, der Leistungsbeschreibungen oder der Vereinbarung über Auftragsverarbeitung unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt. Die unwirksame Bestimmung ist durch eine wirksame zu ersetzen, die den mit der unwirksamen Bestimmung verfolgten Zweck am ehesten erreicht. Wenn bei Vertragsdurchführung eine regelungsbedürftige bzw. ergänzungsbedürftige Lücke offenbar wird, ist diese durch Vereinbarung einer Bestimmung zu schließen, die den verfolgten Zweck am ehesten erreicht.

10.3 Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (Convention on Contracts for the International Sale of Goods vom 11.4.1980, UNCITRAL-Kaufrecht).

10.4 Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Kaiserslautern.

Leistungsbeschreibung

1. Funktionsumfang

Der autorisierte Nutzer erhält nach dem Login-Prozess auf dem Insiders Marketplace [https://insiders-marketplace.com/de/] die Möglichkeit verschiedenste Services zu testen. Der Funktionsumfang beinhaltet das Hochladen eines Dokumentes innerhalb eines bestimmten Services und die Anzeige/visuelle Darstellung der Verarbeitungsergebnisse zur einmaligen Ansicht.

2. Verarbeitungsergebnis

Die angezeigten Verarbeitungsergebnisse unterscheiden sich je nach gewähltem Service. Sie sind mit allen auszulesenden Feldern auf der jeweiligen Seite auf dem Insiders Marketplace beschrieben, auf der der Service dargestellt wird.

3. Leistungszeitraum

Der Leistungszeitraum richtet sich nach der jeweiligen offenen und aktiven Login-Session des Benutzers im Insiders Marketplace. Es erfolgt eine automatische Abmeldung aus dem Marketplace eine Stunde nach Login, somit endet nach diesem Zeitraum die Geltung der zugrundeliegenden Nutzungsbestimmungen.

Vereinbarung über Auftragsverarbeitung

Diese Vereinbarung über Auftragsverarbeitung konkretisiert die Verpflichtungen der Vertragspartner zum Datenschutz, die sich aus der Nutzung der Cloud-Lösung durch den Auftraggeber im Hinblick auf die damit verbundene Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der testweisen Nutzung der Cloud-Lösung durch den Auftraggeber in Zusammenhang stehen und bei denen Beschäftigte von Insiders oder durch von Insiders Beauftragte mit personenbezogenen Daten aus der Sphäre des Auftraggebers und der von ihm autorisierten Nutzer in Berührung kommen können.

1 Definitionen

Begriffsdefinitionen aus den Nutzungsbestimmungen Insiders Cloud und den Leistungsbeschreibungen des / der beauftragten Services (nachfolgend zusammenfassend „Hauptvertrag“ genannt) gelten auch für diese Vereinbarung über Auftragsverarbeitung, soweit hierin nicht ausdrücklich etwas anderes bestimmt ist. Wenn in dieser Vereinbarung über Auftragsverarbeitung der Begriff „Daten“ verwendet wird, sind stets personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO gemeint. Im Übrigen sind die in dieser Vereinbarung über Auftragsverarbeitung verwendeten Begriffe so zu verstehen, wie sie in der DSGVO oder in anderen Gesetzen (z.B. § 2 BDSG, § 3 TTDSG) definiert sind.

2 Gegenstand und Dauer der Verarbeitung

2.1 Insiders stellt dem Auftraggeber zu Testzwecken die im Hauptvertrag vereinbarte Cloud-Lösung zur Nutzung zur Verfügung, mit der der Auftraggeber unter anderem personenbezogene Daten verarbeitet bzw. verarbeiten lässt und Verarbeitungsergebnisse erzeugt bzw. erzeugen lässt. Dabei kann nicht ausgeschlossen werden, dass Insiders Zugriff auf personenbezogene Daten erhält, die der Auftraggeber oder der jeweilige von ihm autorisierte Nutzer in die Cloud-Lösung einspielt. Insiders verarbeitet die im Zusammenhang mit dem Auftrag stehenden personenbezogenen Daten ausschließlich im Rahmen der in dieser Vereinbarung über Auftragsverarbeitung getroffenen Bestimmungen. Insiders verarbeitet die betreffenden personenbezogenen Daten für keine anderen und insbesondere nicht für eigene Zwecke.

2.2 Die Zwecke und Mittel der Verarbeitung bestimmt alleine der Auftraggeber. Änderungen des Verarbeitungsgegenstandes und Verarbeitungsänderungen sind gemeinsam abzustimmen und schriftlich durch Änderung dieser Vereinbarung über Auftragsverarbeitung festzulegen.

2.3 Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

3 Konkretisierung des Auftrags

3.1 Der Inhalt des Auftrags wird in Bezug auf die Auftragsverarbeitung wie folgt konkretisiert:

Art und Zweck der Verarbeitung	Die in der jeweiligen Leistungsbeschreibung vereinbarten Services der Cloud-Lösung ermöglichen dem Auftraggeber bzw. den von ihm autorisierten Nutzern (z.B. Mitarbeiter) zu Testzwecken die Verarbeitung der Kundendaten sowie die Betrachtung der Verarbeitungsergebnisse in der Cloud-Lösung. Art und Zweck der Verarbeitung ergeben sich (i) aus dem Testfunktionsumfang der Cloud-Lösung, der in der jeweiligen Leistungsbeschreibung dokumentiert ist, (ii) den vom Auftraggeber bzw. den autorisierten Nutzern in die Cloud-Lösung eingespielten Kundendaten und (iii) deren konkrete, vom Auftraggeber bzw. den autorisierten Nutzern veranlasste Verarbeitung durch die Cloud-Lösung.
Art der Verarbeitung	☐ Erheben ☐ Erfassen ☒ Organisation ☒ Ordnen ☐ Speicherung ☐ Anpassung oder Veränderung ☒ Auslesen ☐ Abfragen ☐ Verwendung ☐ Offenlegung durch Übermittlung ☒ Verbreitung oder eine andere Form der Bereitstellung ☒ Abgleich oder Verknüpfung ☐ Einschränkung ☐ Löschen oder Vernichtung ☐ Sonstige: .....
Art der personenbezogenen Daten	☐ Personenstammdaten (Vertragsdaten, Geburtsdatum o. ä.) ☐ private Kontaktdaten (Name, Rufnummer, Adresse, E-Mail o. ä.) ☐ berufliche Kontaktdaten (Name, Funktion, Rufnummer, Adresse, E-Mail o. ä.) ☐ Kontodaten / Umsatzdaten / Kontobewegungsdaten ☐ Abrechnungs- und Zahlungsdaten ☐ Versicherungsdaten ☐ Rechnungseingangsdaten

	☒ Sonstige: siehe Leistungsbeschreibung
Besondere Kategorien personenbezogener Daten	☐ rassische oder ethnische Herkunft ☐ politische Meinungen ☐ religiöse oder weltanschauliche Überzeugungen ☐ Gewerkschaftszugehörigkeit ☐ Verarbeitung genetischer Daten ☐ Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person ☐ Gesundheitsdaten ☐ Daten zum Sexualleben ☐ Daten zur sexuellen Orientierung einer natürlichen Person
Kategorien der betroffenen Personen	☒ Privatkunden ☒ Versicherungsnehmer ☒ Geschäfts- / Unternehmenskunden ☒ Beschäftigte i. S. d. § 26 BDSG ☒ Lieferanten ☒ Handelsvertreter ☒ Ansprechpartner ☐ Sonstige: .....

4 Weisungsgebundenheit

4.1 Insiders verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern Insiders nicht durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem sie unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt Insiders dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung in Textform (z.B. per E-Mail oder Fax) mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2 Der Auftraggeber hat das Recht, Insiders im Rahmen des Auftragsgegenstandes (siehe Ziffer 2) Weisungen hinsichtlich der Art, des Umfangs und des Verfahrens der Verarbeitung der personenbezogenen Daten zu erteilen. Seine Weisungen kann er durch Einzelweisungen konkretisieren. Mündlich erteilte Weisungen sind vom Auftraggeber unverzüglich schriftlich oder in Textform zu bestätigen. Als Weisung ist dabei die auf einen bestimmten datenschutzmäßigen Umgang (z.B. Anonymisierung, Berichtigung, Einschränkung der Verarbeitung, Löschung, Herausgabe) von Insiders mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers zu verstehen.

4.3 Der Auftraggeber hat alle Weisungen, die er Insiders erteilt, zu dokumentieren. Die Dokumentation stellt er Insiders für jede erteilte Weisung zur Verfügung. Für die Dokumentation der Umsetzung der vom Auftraggeber erteilten Weisungen ist dagegen Insiders verantwortlich.

4.4 Den entsprechenden Weisungen des Auftraggebers hat Insiders jederzeit Folge zu leisten. Solange und soweit Insiders personenbezogene Daten aus dem Auftrag über das Auftragsende hinaus verarbeitet, gilt die Weisungsgebundenheit gegenüber dem Auftraggeber auch nach der Beendigung dieser Vereinbarung über Auftragsverarbeitung weiter; Aufwendungen und Kosten, die Insiders hierdurch entstehen, trägt der Auftraggeber.

4.5 Insiders unternimmt alle erforderlichen Schritte, um sicherzustellen, dass die ihr unterstellten natürlichen Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Auftraggebers verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4.6 Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen. Falls Weisungen die in Ziffer 3 getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn vorher eine entsprechende Änderung dieser Vereinbarung über Auftragsverarbeitung in Text- oder Schriftform erfolgt ist.

4.7 Insiders wird den Auftraggeber unverzüglich informieren, wenn eine vom Auftraggeber erteilte Weisung nach Auffassung von Insiders gegen gesetzliche Vorschriften und insbesondere gegen die DSGVO, das BDSG oder gegen andere anwendbare Datenschutzbestimmungen der Europäischen Union oder ihrer Mitgliedstaaten verstößt. Insiders ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch eine weisungsberechtigte Person vom Auftraggeber bestätigt oder geändert wird.

5 Verpflichtung zur Vertraulichkeit

5.1 Insiders gewährleistet, dass sie bei der Verarbeitung personenbezogener Daten nur Mitarbeiter beschäftigt, die sie mit den für sie maßgebenden Bestimmungen des Datenschutzrechtes vertraut gemacht und schriftlich - auch über die Beendigung ihrer Tätigkeit hinaus - zur Vertraulichkeit verpflichtet hat. Einer Verpflichtung bedarf es nicht, wenn Mitarbeiter einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.2 Insiders überwacht die Einhaltung der datenschutzrechtlichen Vorschriften durch die ihr unterstellten Personen, die Zugang zu personenbezogenen Daten haben. Ihre mit der Verarbeitung von personenbezogenen Daten betrauten Mitarbeiter wird Insiders regelmäßig in angemessenem Umfang und in angemessenen Abständen schulen und für den Datenschutz sensibilisieren.

5.3 Der Auftraggeber ist verpflichtet, alle im Rahmen des Auftrags erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie Daten- und andere IT-

Sicherheitsmaßnahmen von Insiders, insbesondere die technischen und organisatorischen Maßnahmen von Insiders, streng vertraulich zu behandeln und diese weder weiterzugeben noch auf sonstige Art zu verwerten oder zu offenbaren. Dies gilt gegenüber jeglichen unbefugten Dritten, d.h. auch gegenüber eigenen unbefugten Mitarbeitern, sofern die Weitergabe bzw. sonstige Verwertung oder Offenbarung von solchen Informationen nicht zur ordnungsgemäßen Erfüllung der vertraglichen oder gesetzlichen Verpflichtungen des Auftraggebers erforderlich ist. In Zweifelsfällen ist der Auftraggeber verpflichtet, vor einer solchen Weitergabe bzw. sonstigen Verwertung oder Offenbarung die schriftliche Zustimmung von Insiders einzuholen.

5.4 Ungeachtet der in Ziffer 5.3 vereinbarten Verschwiegenheitspflichten des Auftraggebers darf dieser technische und organisatorische Maßnahmen von Insiders, die den Auftrag betreffen, im Rahmen der dem Auftraggeber gesetzlich auferlegten Rechenschaftspflicht gegenüber berechtigten Personen und Stellen (z.B. Aufsichtsbehörden) offenbaren, soweit sie dazu gesetzlich verpflichtet ist.

6 Technische und organisatorische Maßnahmen

6.1 Insiders setzt für den Auftrag unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Vereinbarung über Auftragsverarbeitung erfolgt.

6.2 Die als Anlage 1 (Technische und organisatorische Maßnahmen) beigefügten Datenschutzvorkehrungen von Insiders, die die Festlegungen gemäß Art. 32 DSGVO enthalten, werden für die Durchführung des Auftrags als verbindliches Minimum festgelegt, das zu keiner Zeit unterschritten werden darf. Insiders verpflichtet sich zur Einhaltung der in Anlage 1 niedergelegten technischen und organisatorischen Maßnahmen.

6.3 Stellt der Auftraggeber während der Laufzeit des Auftrages fest, dass sich die Risiken für die Rechte und Freiheiten der Betroffenen verändert haben, teilt er dies Insiders unverzüglich mit, damit Insiders ihre technischen und organisatorischen Maßnahmen so anpassen kann, dass das für den Auftrag erforderliche Datenschutzniveau weiterhin gewährleistet bleibt; die Insiders durch die Anpassung entstehenden einmaligen und wiederkehrenden Aufwendungen und Kosten trägt der Auftraggeber. Sobald Insiders in Anlage 1 die aktualisierten technischen und organisatorischen Maßnahmen festgelegt hat, ersetzt diese neue Anlage 1 die bis dahin gültige Anlage 1. Sollte eine entsprechende Anpassung der technischen und organisatorischen Maßnahmen Insiders nicht möglich, nicht zumutbar oder gar für sie unzulässig sein, stellt dies für beide Vertragspartner einen wichtigen Grund dar, der zur außerordentlichen Kündigung des Hauptvertrages einschließlich der vorliegenden Vereinbarung über Auftragsverarbeitung berechtigt.

6.4 Insiders stellt sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten von sonstigen Datenbeständen strikt getrennt werden. Nähere Anforderungen und Maßnahmen zur Trennung sind in den technischen und organisatorischen Maßnahmen in Anlage 1 festgelegt.

6.5 Wenn und soweit Insiders gegenüber dem Auftraggeber zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen verpflichtet ist, kann sie Nachweise über die Einhaltung genehmigter Verhaltensregelungen gemäß Art. 40 DSGVO oder über aktuelle Zertifizierung gemäß Art. 42 DSGVO vorlegen, um ihren Nachweis zu stützen. Des Weiteren kann sie diesen Nachweis auch über aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch ein Informationssicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, als Bestandteil einer ISO 27001-Zertifizierung) führen.

6.6 Die technischen und organisatorischen Maßnahmen müssen im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Dazu werden die in Anlage 1 vereinbarten technischen und organisatorischen Maßnahmen vom Auftraggeber und von Insiders im Lichte der Ziffer 6.1 sowie unter Berücksichtigung des Stands der Technik mindestens einmal im Kalenderjahr überprüft. Aus solchen Überprüfungen resultierende Änderungen sind schriftlich festzulegen. Stellt Insiders während der Laufzeit des Auftrages von sich aus fest, dass die von ihr getroffenen Maßnahmen die Risiken für die Rechte und Freiheiten der Betroffenen nicht oder nicht mehr angemessen abdecken, benachrichtigt sie den Auftraggeber. Für die Anpassung der Anlage 1 gelten die in Ziffer 6.3 vereinbarten Bestimmungen entsprechend.

7 Einbeziehung weiterer Auftragsverarbeiter

7.1 Der Auftraggeber erteilt hiermit ihre allgemeine Zustimmung zur Inanspruchnahme weiterer Auftragsverarbeiter.

7.2 Im Falle der Beauftragung von weiteren Auftragsverarbeitern (Kettenauftragsverarbeitung) oder der Ersetzung von weiteren Auftragsverarbeitern wird Insiders den Auftraggeber informieren. Will der Auftraggeber gegen derartige Änderungen Einspruch erheben, hat er diesen gegenüber Insiders innerhalb von zwei (2) Wochen nach Zugang der Information bzw. unverzüglich nach Kenntniserlangung von einem sich später ergebenden Einspruchsgrund schriftlich zu erklären. Die Bestimmungen dieser Ziffer 7 gelten entsprechend für jede Hinzuziehung bzw. Ersetzung von weiteren Auftragsverarbeitern im Rahmen einer mehrstufigen Kettenauftragsverarbeitung.

7.3 Insiders erlegt weiteren Auftragsverarbeitern im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats geeignete Pflichten zur Einhaltung des Datenschutzes auf. Dabei ist sicherzustellen, dass geeignete technische und organisatorische Maßnahmen auch von dem

weiteren Auftragsverarbeiter so durchgeführt werden, dass die Verarbeitung den gesetzlichen Anforderungen des Datenschutzrechtes entspricht.

7.4 Bei Abschluss dieser Vereinbarung über Auftragsverarbeitung hat der Auftraggeber der Inanspruchnahme der in Anlage 2 (Weitere Auftragsverarbeiter) mit Namen und konkretisiertem Auftragsinhalt bezeichneten weiteren Auftragsverarbeitern mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang zugestimmt.

7.5 Der Auftraggeber kann gegen den Einsatz eines weiteren Auftragsverarbeiters durch Insiders nur dann Einspruch erheben, wenn er begründete Zweifel daran hat, dass der weitere Auftragsverarbeiter die datenschutzrechtlichen Bestimmungen oder die Bedingungen dieser Vereinbarung über Auftragsverarbeitung einhalten wird.

7.6 Nicht als Inanspruchnahme weiterer Auftragsverarbeiter im Sinne dieser Ziffer 7 sind solche Dienstleistungen zu verstehen, die Insiders bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Reinigungskräfte, Telekommunikationsleistungen und Postdienste.

8 Unterstützung des Auftraggebers

8.1 Insiders unterstützt den Auftraggeber bei dessen Pflicht, Anträge auf Wahrnehmung der in Art. 12 bis 23 DSGVO sowie in §§ 32 bis 37 BDSG genannten Rechte der betroffenen Person zu bearbeiten und zu beantworten. Dazu wird sie dem Auftraggeber auf Anfrage alle zweckdienlichen Informationen bereitstellen, die Insiders im Einzelfall vorliegen. Wendet sich ein Betroffener mit Anträgen auf Wahrnehmung der in Art. 12 bis 23 DSGVO und in §§ 32 bis 37 BDSG genannten Rechten unmittelbar an Insiders, wird diese den Betroffenen an den Auftraggeber verweisen.

8.2 Auskünfte an Dritte oder den Betroffenen darf Insiders nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

8.3 Insiders ergreift geeignete technische und organisatorische Maßnahmen, um den Auftraggeber gemäß Ziffer 8.1 unterstützen zu können.

8.4 Des Weiteren unterstützt Insiders mit den ihr zur Verfügung stehenden Informationen den Auftraggeber bei dessen Einhaltung der ihm gemäß Art. 32 bis 36 DSGVO obliegenden Pflichten.

8.5 Der Auftraggeber hat Insiders alle Aufwendungen und Kosten zu erstatten, die Insiders im Rahmen der Unterstützung des Auftraggebers entstehen.

9 Rückgabe und Löschung von Daten

Nach Beendigung der vertraglichen Arbeiten hat Insiders sämtliche im Zusammenhang mit dem Auftrag in ihren Besitz gelangten Unterlagen und erstellten Verarbeitungsergebnisse, die personenbezogene Daten enthalten, sowie alle im Rahmen der Cloud-Lösung vom bzw. für den Auftraggeber verarbeiteten personenbezogenen Daten datenschutzgerecht zu löschen.

10 Nachweis der Einhaltung der datenschutzrechtlichen Pflichten

10.1 Insiders stellt dem Auftraggeber auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten zur Verfügung.

10.2 Außerdem ermöglicht und unterstützt Insiders Überprüfungen einschließlich Inspektionen und Untersuchungen, die von dem Auftraggeber oder einem anderen von diesem beauftragten Prüfer oder von Aufsichtsbehörden durchgeführt werden. Insiders erklärt sich insbesondere damit einverstanden, dass der Auftraggeber oder ein von diesem beauftragten Prüfer nach angemessener Vorankündigung berechtigt ist, während der üblichen Bürozeiten von Insiders die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen dieser Vereinbarung über Auftragsverarbeitung im erforderlichen Umfang und ohne Störung des Betriebsablaufs von Insiders vor Ort zu kontrollieren.

10.3 Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu Insiders stehen, hat Insiders gegen diesen Prüfer ein Einspruchsrecht.

10.4 Der Auftraggeber hat Insiders alle Aufwendungen und Kosten zu erstatten, die Insiders im Rahmen der Durchführung und Unterstützung einer Überprüfung bzw. Inspektion entstehen.

11 Verfahrensverzeichnisse

Insiders führt das gemäß Art. 30 Abs. 2 DSGVO von ihr zu führende Verzeichnis und stellt dieses der Aufsichtsbehörde auf Anfrage zur Verfügung.

12 Sonstige Pflichten von Insiders

12.1 Insiders arbeitet auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

12.2 Insiders hat einen Datenschutzbeauftragten benannt und teilt dem Auftraggeber dessen Kontaktdaten auf Anfrage mit. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage von Insiders leicht zugänglich hinterlegt.

12.3 Ist für eine geplante Verarbeitung personenbezogener Daten eine Datenschutz-Folgeabschätzung erforderlich, unterstützt Insiders den Auftraggeber auf Anforderung und gegen Vergütung ihres damit verbundenen Aufwandes bei der Abschätzung und stellt ihm alle erforderlichen Dokumentationen und zweckdienlichen Informationen zur Verfügung.

12.4 Insiders wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO sowie über Ermittlungen, die eine zuständige Behörde nach Art. 83 DSGVO und §§ 42, 43 BDSG bei Insiders durchführt, informieren, soweit diese Kontrollhandlungen, Maßnahmen oder Ermittlungen Bezüge zur Auftragsverarbeitung aufweisen.

13 Mitzuteilende Verstöße

13.1 Insiders benachrichtigt den Auftraggeber unverzüglich, wenn ihr eine Verletzung des Schutzes von dem Auftraggeber zugewiesenen personenbezogenen Daten bekannt

wird. Meldungen erfolgen in Textform und müssen mindestens die in Art. 33 Abs. 3 DSGVO aufgezählten Informationen umfassen.

13.2 Insiders ist bekannt, dass nach Art. 33 und 34 DSGVO Melde- und Benachrichtigungspflichten im Falle der Verletzung des Schutzes personenbezogener Daten gegenüber der Aufsichtsbehörde und den betroffenen Personen bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Insiders hat in Abstimmung mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

13.3 Soweit den Auftraggeber Pflichten nach Art. 33 und 34 DSGVO treffen, hat Insiders ihn hierbei gegen Vergütung des für Insiders damit verbundenen Aufwandes zu unterstützen. Ungeachtet dessen bleibt der Auftraggeber für die Erfüllung der ihn gemäß Art. 33 und 34 DSGVO treffenden Melde- und Benachrichtigungspflichten selbst verantwortlich.

14 Anlagen

Die folgenden Anlagen bilden einen wesentlichen Bestandteil dieser Vereinbarung über Auftragsverarbeitung und haben im Fall von Widersprüchen oder Unklarheiten Vorrang vor den Bestimmungen der vorliegenden Vereinbarung über Auftragsverarbeitung:

Anlage 1: Technische und organisatorische Maßnahmen - Insiders Technologies GmbH einschließlich Cloud-Betrieb

Anlage 1a: AWS Security Standards

Anlage 1b: Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Open Telekom Cloud

Anlage 2: Weitere Auftragsverarbeiter

Anlage 1: Technische und organisatorische Maßnahmen – Insiders Technologies GmbH einschließlich Cloud-Betrieb

1 Vorbemerkung

Insiders setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den getroffenen Vereinbarungen erfolgt.

AWS unterhält ein Informationssicherheitsprogramm (einschließlich der Einführung und Durchsetzung interner Richtlinien und Verfahren), das dazu dient,

1. Insiders dabei zu unterstützen, seine Daten vor versehentlichem oder unrechtmäßigem Verlust, Zugriff oder Offenlegung zu schützen,

2. vernünftigerweise vorhersehbare und interne Risiken für die Sicherheit und den unbefugten Zugriff auf das AWS-Netzwerk zu ermitteln und

3. Sicherheitsrisiken zu minimieren, unter anderem durch Risikobewertung und regelmäßige Tests.

Von AWS umgesetzte technische und organisatorische Maßnahmen werden im Dokument AWS Security Standards beschrieben. Von der Telekom umgesetzte technische und organisatorische Maßnahmen werden im Dokument Anlage zu Ergänzende Bedingungen Auftragsdatenverarbeitung personenbezogener Daten für Open Telekom Cloud beschrieben.

2 Spezielle Maßnahmen für Rechenzentrumsbetrieb der Cloud-Lösungen

2.1 Insiders nutzt für den Betrieb der Cloud-Lösungen und die Erbringung der damit verbundenen Services die Leistungen externer Rechenzentren (siehe auch Anlage 2). Für diese Rechenzentren hat Insiders Vereinbarungen über Auftragsverarbeitung abgeschlossen, in der auf den Rechenzentrumsbetrieb ausgerichtete technische und organisatorische Maßnahmen festgelegt sind.

2.2 Die für Amazon Web Services bei Abschluss der vorliegenden Vereinbarung über Auftragsverarbeitung geltenden technischen und organisatorischen Maßnahmen sind im DPA (AWS GDPR Data Protection Addendum) von AWS unter https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf zu finden (siehe auch Anlage 1a). Die für die OpenTelekom Cloud geltenden technischen und organisatorischen Maßnahmen sind in Anhang III der „Ergänzenden Bedingungen Auftragsverarbeitung (ErgB-AV) für die Open Telekom Cloud“ zu finden (siehe auch Anlage 1b).Auf die übrige Verarbeitung personenbezogener Daten durch Insiders finden die in den folgenden Ziffern 3 bis 8 beschriebenen technischen und organisatorischen Maßnahmen Anwendung.

2.3 Die technischen und organisatorischen Maßnahmen beziehen sich auf die Maßnahmen bei Insiders, jeweils erforderlichenfalls ergänzt um umgesetzte Maßnahmen im

externen Rechenzentrum für Colocation/Housing und/oder um umgesetzte Maßnahmen in der Cloud-Umgebung bei Insiders.

3 Kundendaten

3.1 Für den Support der Cloud-Lösung kann es erforderlich sein, dass Kunden Insiders Beispieldokumente (Rechnungen, Lieferscheine, Formulare etc.) und Stammdaten zur Verfügung stellen.

3.2 Alle Insiders von Kunden im Sinne von Ziffer 3.1 überlassenen Daten werden zentral im Support verwaltet. Datenträger und Dokumente in Papierform werden zugriffssicher verschlossen gelagert. Elektronische Dokumente werden zentral und logisch getrennt abgelegt. Für die Ablage von Kundendaten stehen dedizierte Fileserver und Datenbankserver in einem externen Rechenzentrum zur Verfügung.

3.3 Die Ablage dieser Daten erfolgt zu Sicherheitszwecken in pseudonymisierter Form. Die Zuordnung von Daten zu Kunden erfolgt hierbei über Supportmitarbeiter. Als weitere Sicherheitsmaßnahme werden die Kundendaten Fileserver-basiert auf einem hardwareverschlüsselten Plattensystem abgelegt.

3.4 Zugriff auf die Kundendaten erhalten nur autorisierte Mitarbeiter und auch diese ausschließlich für die jeweils benötigten Kundendaten. Hierzu werden für elektronische Dokumente auf Dateiebene Rechte für die entsprechenden Benutzer festgelegt. Papierdokumente werden nur gegen Unterschrift herausgegeben. Für Mitarbeiter, die Zugriff auf Kundendaten benötigen, existiert ein dezidiertes Berechtigungskonzept, das im Falle sich ändernder Anforderungen angepasst wird.

4 Betriebsstätten

Insiders verarbeitet Daten im Rahmen des mobilen Arbeitens auch außerhalb der Betriebsstätten Kaiserslautern, München und Berlin. Dabei sind alle beschriebenen technischen und organisatorischen Maßnahmen angemessen zu beachten. Insbesondere erfolgt der Zugriff auf die Daten der Kunden nur über eine gesicherte VPN-Verbindung, die Verarbeitung der Daten nur auf gegen Fremdzugriff gesicherten Endgeräten und die Mitarbeiter haben sicher zu stellen, dass Dokumente in Papierform, die Daten der Kunden enthalten, wirksam vor dem Zugriff Unbefugter geschützt sind. Insiders ergreift geeignete Maßnahmen, um die Einhaltung dieser Vorgaben durch seine Mitarbeiter zu ermöglichen, zu fördern und zu überwachen.

5 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

5.1 Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

Es existieren folgende Maßnahmen zur Zutrittskontrolle in den Gebäuden bei Insiders:

- Alarmanlage
- Bewegungsmelder
- Schlüsselregelung (Schlüsselausgabe etc.)

- Protokollierung der Besucher / Tragen von Besucherausweisen
- Begleitung von Besuchern
- Transponder-Schließsystem
- Manuelles Schließsystem
- Videoüberwachung der Zugänge
- Sicherheitsschlösser
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Dienstleistern, insbesondere von Reinigungspersonal
- Zutrittsbeschränkung zu Sicherheitszonen

Zusätzlich zu den vorstehenden Maßnahmen im externen Rechenzentrum für Colocation/Housing umgesetzte Maßnahmen:

- Mehrstufiges Zugangskontrollsystem
- Videoüberwachung im Eingangsbereich zum und im Rechenzentrum
- Einbruchmeldeanlage und Einsatz eines Sicherheitsdienstes
- Überwachtes Betriebsgelände und Leitstelle

5.2 Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

Es existieren folgende Maßnahmen zur Zugangskontrolle bei Insiders:

- Zuordnung von Benutzerrechten
- Verwendung von Benutzerrollen
- Passwortvergabe
- Automatische Sperrung von Accounts nach mehrfacher Fehleingabe
- Automatische Bildschirmsperre
- Verwendung von Passwort-Richtlinien
- Authentifikation mit Benutzername/Passwort
- Einsatz von Intrusion-Prevention-Systemen
- Einsatz von Anti-Viren-Software
- Einsatz eines Extended Detection and Response (XDR) Systems
- Einsatz von Hardware-/Software-Firewalls
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie mit mehrstufiger Authentifizierung
- Protokollierung von Benutzeranmeldungen

- Verwendung von Netzwerksicherheitszonen

In den Cloud-Umgebungen von AWS und OTC bei Insiders existieren die folgenden Maßnahmen:

- Rollenbasiertes Berechtigungskonzept
- Verwendung von Passwort-Richtlinien
- Mehrfaktor-Authentifizierung
- Verwendung von IP-Filtern
- Automatisches Ausloggen von Benutzern nach Inaktivität
- Automatisches Ausloggen von Benutzern nach Ablauf der maximalen Sessiondauer
- Multi-Account-Architektur ermöglicht Isolation von Benutzern und Systemen
- Verschlüsselung personenbezogener Daten At-Rest (außer smart FLOW) und In-Transit
- Aufbewahrung der Master-Keys zur Verschlüsselung der Daten in AWS in einem Schlüsselverwaltungssystem der OTC
- Verschlüsselung von Laufwerken, Fileshare und Object-Storage
- Applikationsseitige, kundenindividuelle Verschlüsselung von datenschutzrelevanten Daten (außer smart FLOW)
- Einsatz von Network Access Control Lists und Security Groups
- Einsatz von Next-Generation Anti-Viren-Software
- Einsatz einer Next-Generation Firewall
- Einsatz eines Extended Detection and Response Systems (XDR)

5.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Es existieren folgende Maßnahmen zur Zugriffskontrolle bei Insiders:

- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Einsatz eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von An-/Abmeldungen am Active Directory
- Einsatz eines Intrusion-Prevention-System (IPS)
- Hardware-/softwareverschlüsselte Platten bei allen PCs und Laptops außerhalb von Sicherheitszonen

- Sichere Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399, Schutzklasse 2, Sicherheitsstufe H4)
- Ordnungsgemäße Vernichtung von Papierunterlagen (DIN 66399, Schutzklasse 3, Sicherheitsstufe P4)
- Protokollierung der Vernichtung

In den Cloud-Umgebungen von AWS und OTC bei Insiders existieren die folgenden Maßnahmen:

- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Rollenbasiertes Berechtigungskonzept
- Mehrfaktor-Authentifizierung
- Einhaltung des "Least-Privilege"-Prinzips bei der Vergabe von Rechten
- Konfiguration von Zugriffsrichtlinien
- Protokollierung und Überwachung von An-/Abmeldungen am Active Directory
- Multi-Account-Architektur ermöglicht Isolation von Benutzern und Systemen
- Regelmäßige Reviews der Rollen und Berechtigungen
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Regelmäßige Penetrationstests aller Insiders Cloud Anwendungen
- Absicherung der Daten In-Use durch virtualisierte Recheninstanzen mit geschütztem Hypervisor. Bei AWS kommt ein Nitro Hypervisor zum Einsatz.

5.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

Es existieren folgende Maßnahmen zur Trennungskontrolle bei Insiders:

- Einsatz eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Verwendung dedizierter File- und Datenbankserver
- Ablage bereitgestellter Supportdaten in pseudonymisierter Form
- Logische Mandantentrennung (softwareseitig)

In den Cloud-Umgebungen von AWS und OTC bei Insiders existieren die folgenden Maßnahmen:

- Rollenbasiertes Berechtigungskonzept

- Ablage bereitgestellter Supportdaten in pseudonymisierter Form
- Logische Mandantentrennung (softwareseitig)
- Multi-Account Architektur zur vollständigen Trennung von Test- und Produktivsystemen
- Bereitstellung eines Sandbox-Accounts zu Testzwecken
- Kundenspezifische Verschlüsselung von Anwendungsdaten (außer smart FLOW)
- Verwendung von Row-Level-Security auf Datenbankebene

6 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

6.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

Es existieren folgende Maßnahmen zur Weitergabekontrolle bei Insiders:

- Transportverschlüsselung beim E-Mail-Versand (TLS-Verschlüsselung)
- SMIME Signierung und Verschlüsselung von E-Mails bei Bedarf
- Absicherung der Online-Datentransfers durch geschützte Übertragungswege (HTTPS, VPN)
- Regelungen (u.a. arbeitsrechtliche) für den Umgang mit Daten und IT-Strukturen
- Weitergabe von Kundendaten ausschließlich auf Weisung des Kunden

Zusätzlich zu den vorstehenden Maßnahmen in den Cloud-Umgebungen von AWS und OTC von Insiders umgesetzte Maßnahmen:

- Einsatz von VPN-Tunneln
- Verschlüsselung In-Transit aller personenbezogener Daten gemäß Empfehlungen des BSI
- Clientseitige Verschlüsselung At-Rest aller personenbezogener Daten gemäß Empfehlungen des BSI (außer smart FLOW)
- Aufbewahrung der Schlüssel in einem von AWS getrennten, externen Key Management System

6.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

Es existieren folgende Maßnahmen zur Eingabekontrolle bei Insiders:

- Für Support- und Entwicklungszwecke für Kunden findet keine Eingabekontrolle statt, weil hierbei nur Test- und Entwicklungssysteme eingesetzt werden.

Zusätzlich zu den vorstehenden Maßnahmen in den Cloud-Umgebungen von AWS und OTC bei Insiders umgesetzte Maßnahmen:

- Trennung von Produktiv-, Entwicklungs- und Testsystemen
- Protokollierung der Eingabe, Änderung und Löschung von Daten im Produktivsystem
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Nachvollziehbarkeit durch Schreiben und Überwachen von Audit Logs
- Schutz der Logdateien

7 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

7.1 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle bei Insiders:

- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans
- Verwendung von Hardwareredundanzen
- Verwendung von Clustern (VMWare, Datenbanken etc.)
- Regelmäßige Verteilung von Windows- und Software-Updates auf allen internen PC, Servern und VMs über Patch Management Tool
- Verwendung von Virenscannern
- Einsatz eines Extended Detection and Response (XDR) Systems
- Verwendung von Firewalls
- Asynchron gespiegelte Storage-Systeme
- Rauchmelder

Zusätzlich zu den vorstehenden Maßnahmen im externen Rechenzentrum für Colocation/Housing umgesetzte Maßnahmen:

- Unterbrechungsfreie Stromversorgung (USV)
- Notstromversorgung über Dieselgenerator
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Redundante Kälte- und Klimaversorgung
- Brandmeldesysteme mit Früherkennung
- Gaslöschanlage
- Schutzsteckdosenleisten in Serverräumen
- Anbindung über redundante, dedizierte Glasfaserstrecken

In den Cloud-Umgebungen von AWS und OTC bei Insiders existieren die folgenden Maßnahmen:

- Regelmäßige, automatisierte Backups aller produktiven Datenspeicher
- Ablage von Backups in einem gesicherten, hochverfügbaren Backuptresor
- Durchführen von Wiederherstellungstests
- Durchführen von Ausfalltests
- Einsatz von Next-Generation Anti-Viren-Software
- Einsatz einer Next-Generation Firewall
- Einsatz eines Extended Detection and Response Systems (XDR)
- Einsatz eines Security Operation Center (SOC) zur 24/7 Überwachung
- Synchron gespiegelte Dateispeicher
- Hochverfügbare Produktivumgebung
- Dreifache Redundanz und Aufteilung der Produktivumgebung auf drei getrennte Rechenzentren bei AWS, zweifache Redundanz bei OTC

7.2 Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c) DS-GVO)

Es existieren folgende Maßnahmen zur raschen Wiederherstellung:

- Tägliche automatische Snapshoterstellung
- Bei Changes: gesonderte, manuelle Snapshoterstellung
- Automatische Erstellung von Datenbankdumps

Zusätzlich zu allen vorstehenden Maßnahmen in den Cloud-Umgebungen von AWS und OTC bei Insiders umgesetzte Maßnahmen:

- Regelmäßige, automatisierte Backups aller produktiven Datenspeicher
- Bei Changes: gesonderte, manuelle Backups
- Automatisiertes Einrichten der Infrastruktur durch Infrastructure-As-Code

8 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Insiders trifft folgende Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung bei Insiders:

- Datenschutz-Management
  - Prüfung der vertraglichen Regelungen mit Mitarbeitern und ggf. Mitarbeitern externer Dienstleister
    - Vertraulichkeitsvereinbarung;
    - Belehrung und Verpflichtung auf das Datengeheimnis sowie das Sozialgeheimnis gemäß Sozialgesetzbuch (§ 35 SGB I und § 80 SGB X);
    - Vereinbarung über die Nutzung der IT- und TK-Infrastruktur;
    - Sicherung der Urheberrechte bei Insiders bzw. beim Kunden, sofern dies vereinbart ist;
    - Belehrung und Verpflichtung auf weitere datenschutzrelevante Vorschriften und Gesetze, insbesondere das Postgeheimnis gemäß Postgesetz (§§ 39, 41 PostG), das Fernmeldegeheimnis gemäß Telekommunikation-Telemedien-Datenschutz-Gesetz (§ 3 TTDSG) sowie § 203 StGB.
  - Regelmäßige Datenschutzschulungen
  - Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der getroffenen Maßnahmen
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle

  Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.
  - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
  - dokumentierte Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
  - Auftragnehmer hat Datenschutzbeauftragten bestellt
  - Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
  - vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Überprüfung des Auftragnehmers und seiner Tätigkeiten

9 Veränderungen der Sicherheitsstruktur

Insiders passt seine Sicherheitsstruktur regelmäßig dem technischen Fortschritt sowie den rechtlichen und vertraglichen Erfordernissen an. Das Datensicherheitskonzept mit den hier referenzierten Inhalten wird mindestens jährlich aktualisiert. Bei wesentlichen Änderungen der Systeme und/oder der angewendeten Maßnahmen erfolgt die Aktualisierung zum Zeitpunkt der erfolgten Änderungen.

AWS führt regelmäßige Überprüfungen der Sicherheit seines AWS-Netzwerks und der Angemessenheit seines Informationssicherheitsprogramms durch, gemessen an den Sicherheitsstandards der Branche und seinen Richtlinien und Verfahren. AWS wird die Sicherheit seines AWS-Netzes und der zugehörigen Dienste fortlaufend bewerten, um festzustellen, ob zusätzliche oder andere Sicherheitsmaßnahmen erforderlich sind, um auf neue Sicherheitsrisiken oder Erkenntnisse aus den regelmäßigen Überprüfungen zu reagieren.

10 Zertifizierungen

Zum Zeitpunkt der Erstellung dieses Dokumentes können die folgenden Zertifizierungen nachgewiesen werden:

- ISO/IEC 27001:2017, Zertifikat-Registrier-Nr. 73 121 6688 (Insiders Technologies GmbH)
- ISO/IEC 27001:2017, Zertifikat-Registrier-Nr. 2209/Z3407 (Externes Rechenzentrum für Colocation/Housing)
- ISO/IEC 27001:2013, Zertifikat-Nr. 2013-009 (Amazon Web Services, Inc.)
- ISO/IEC 27017:2015, Zertifikat-Nr. 2015-015 (Amazon Web Services, Inc.)
- ISO/IEC 27018:2019, Zertifikat-Nr. 2015-016 (Amazon Web Services, Inc.)
- ISO/IEC 27701:2019, Zertifikat-Nr. 2021-035 (Amazon Web Services, Inc.)
- ISO/IEC 27001:2017, Zertifikat-Nr. DS-1215044/2 (Deutsche Telekom AG)
- ISO/IEC 22301:2020, Zertifikat-Nr. DS1215046/2 (Deutsche Telekom AG)
- Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) (T-Systems International GmbH für den Dienst Open Telekom Cloud, Zertifikats Registrier-Nr.: DS-0817020/1-4

Anlage 1a: AWS Security Standards

Capitalised terms not otherwise defined in this document have the meanings assigned to them in the Agreement [https://aws.amazon.com/agreement/].

1 Information Security Program.

AWS will maintain an information security program designed to (a) enable Customer to secure Customer Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable risks to the security and availability of the AWS Network, and (c) minimize physical and logical security risks to the AWS Network, including through regular risk assessment and testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. AWS's information security program will include the following measures:

1.1 Logical Security.

A. **Access Controls.** AWS will make the AWS Network accessible only to authorized personnel, and only as necessary to maintain and provide the Services. AWS will maintain access controls and policies to manage authorizations for access to the AWS Network from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain access controls designed to (i) restrict unauthorized access to data, and (ii) segregate each customer's data from other customers' data.

B. **Restricted User Access.** AWS will (i) provision and restrict user access to the AWS Network in accordance with least privilege principles based on personnel job functions, (ii) require review and approval prior to provisioning access to the AWS Network above least privileged principles, including administrator accounts; (iii) require at least quarterly review of AWS Network access privileges and, where necessary, revoke AWS Network access privileges in a timely manner, and (iv) require twofactor authentication for access to the AWS Network from remote locations.

C. **Vulnerability Assessments.** AWS will perform regular external vulnerability assessments and penetration testing of the AWS Network, and will investigate identified issues and track them to resolution in a timely manner.

D. **Application Security.** Before publicly launching new Services or significant new features of Services, AWS will perform application security reviews designed to identify, mitigate and remediate security risks.

E. **Change Management.** AWS will maintain controls designed to log, authorize, test, approve and document changes to existing AWS Network resources, and will document change details within its change management or deployment tools. AWS will test changes according to its change management standards prior to migration to production. AWS will maintain processes designed to detect unauthorized changes to the AWS Network and track identified issues to a resolution.

F. **Data Integrity.** AWS will maintain controls designed to provide data integrity during transmission, storage and processing within the AWS Network. AWS will provide Customer the ability to delete Customer Data from the AWS Network.

G. **Business Continuity and Disaster Recovery.** AWS will maintain a formal risk management program designed to support the continuity of its critical business functions ("Business Continuity Program"). The Business Continuity Program includes processes and procedures for identification of, response to, and recovery from, events that could prevent or materially impair AWS's provision of the Services (a "BCP Event"). The Business Continuity Program includes a three-phased approach that AWS will follow to manage BCP Events:

(i) **Activation & Notification Phase.** As AWS identifies issues likely to result in a BCP Event, AWS will escalate, validate and investigate those issues. During this phase, AWS will analyze the root cause of the BCP Event.

(ii) **Recovery Phase.** AWS assigns responsibility to the appropriate teams to take steps to restore normal system functionality or stabilize the affected Services.

(iii) **Reconstitution Phase.** AWS leadership reviews actions taken and confirms that the recovery effort is complete and the affected portions of the Services and AWS Network have been restored. Following such confirmation, AWS conducts a post-mortem analysis of the BCP Event.

H. **Incident Management.** AWS will maintain corrective action plans and incident response plans to respond to potential security threats to the AWS Network. AWS incident response plans will have defined processes to detect, mitigate, investigate, and report security incidents. The AWS incident response plans include incident verification, attack analysis, containment, data collection, and problem remediation. AWS will maintain an AWS Security Bulletin (as of the Effective Date, http://aws.amazon.com/security/security-bulletins/) which publishes and communicates security related information that may affect the Services and provides guidance to mitigate the risks identified.

I. **Storage Media Decommissioning.** AWS will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Data. Prior to final disposal, storage media that was used to store Customer Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Data cannot be retrieved from the applicable type of storage media.

1.2 Physical Security.

A. **Access Controls.** AWS will (i) implement and maintain physical safeguards designed to prevent unauthorized physical access, damage, or interference to the AWS Network, (ii) use appropriate control devices to restrict physical access to the

AWS Network to only authorized personnel who have a legitimate business need for such access, (iii) monitor physical access to the AWS Network using intrusion detection systems designed to monitor, detect, and alert appropriate personnel of security incidents, (iv) log and regularly audit physical access to the AWS Network, and (v) perform periodic reviews to validate adherence with these standards.

B. **Availability.** AWS will (i) implement redundant systems for the AWS Network designed to minimize the effect of a malfunction on the AWS Network, (ii) design the AWS Network to anticipate and tolerate hardware failures, and (iii) implement automated processes designed to move customer data traffic away from the affected area in the case of hardware failure.

1.3 AWS Employees.

A. **Employee Security Training.** AWS will implement and maintain employee security training programs regarding AWS information security requirements. The security awareness training programs will be reviewed and updated at least annually.

B. **Background Checks.** Where permitted by law, and to the extent available from applicable governmental authorities, AWS will require that each employee undergo a background investigation that is reasonable and appropriate for that employee's position and level of access to the AWS Network.

2 Continued Evaluation.

AWS will conduct periodic reviews of the information security program for the AWS Network. AWS will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.

Anlage 1b: Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Open Telekom Cloud

Anhang III aus Ergänzende Bedingungen Auftragsverarbeitung OTC. Ist unter dem Link

https://www.open-telekom-cloud.com/_Resources/Persistent/4/e/e/8/4ee848dc4ead2a3992eeb85035677d55e1b53936/open-telekom-cloud-ergaenzende-bedingungen-auftragsverarbeitung.pdf

zugänglich.

Anlage 2: Weitere Auftragsverarbeiter

Name / Firma, Anschrift des Vertragspartners	Auftragsinhalt	Standorte der Rechenzentren	Umfang der Auftragsverarbeitung
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855, Luxemburg	Rechenzentrum CLOUD-Betrieb	Local Zone eu-central-1 mit Standorten in Frankfurt am Main	AWS-Services zum Betrieb der Cloud-Lösung, insbesondere Cloud Computing, File System, Backup, Storage, System Management, Load Balancing
Telekom Deutschland GmbH Landgrabenweg 151, 53227 Bonn, Deutschland	Rechenzentrum CLOUD-Betrieb	Raum Magdeburg und Biere (D)	Envelope Encryption mit dem KMS Service der OTC Infrastruktur zum Betrieb der Microsoft OCR Instanz