Allgemeine Geschäftsbedingungen

PureCloud Service – Allgemeine Geschäftsbedingungen

Diese Geschäftsbedingungen wurden zuletzt im Jänner 2019 aktualisiert.

Dieser Vertrag über das PureCloud Service sowie die darin genannten Dokumente (der „**Vertrag**“) enthalten Bedingungen und Bestimmungen, die Ihren Zugang zum PureCloud Service (wie nachstehend definiert) und dessen Nutzung regeln. Es handelt sich hierbei um einen Vertrag zwischen Genesys Telecommunications Laboratories B.V., eingetragen bei der niederländischen Handelskammer unter der Nummer 24293219, mit Sitz in Naarden, Niederlande, und Geschäftsadresse in Gooimeer 6 – 02, 1411 DD Naarden, Niederlande („**Genesys**“, „**wir**“, „**uns**“ bzw. „**unser**“) und Ihnen bzw. dem Unternehmen, das Sie vertreten („**Sie**“ oder „**Kunde**“). Gegenüber Verbrauchern werden keine PureCloud Services angeboten. Dieser Vertrag wird mit Unterfertigung durch den Kunden wirksam („**Datum des Inkrafttretens**“). Sie sichern zu, rechtmäßig in der Lage zu sein, Verträge abzuschließen und rechtmäßig dazu befugt zu sein, dies im Namen des Kunden zu tun.

ABONNEMENTDIENSTE

1. **Abonnementdienste.** Wir räumen Ihnen das Recht ein, das PureCloud Service gemäß diesem Vertrag und den entsprechenden Servicebeschreibungen (verfügbar unter https://help.mypurecloud.com) zu nutzen.

    1. Die zur Betreibung des PureCloud Service verwendete Software befindet sich (i) auf Servern, die von Amazon Web Services, Inc. („**AWS**“) kontrolliert werden, und (ii) auf dem PureCloud Bridge Server an Ihren Standorten. Sie sind befugt auf die Software zugreifen und sie zu verwenden, nicht jedoch berechtigt, eine Kopie des Objektcodes oder Quellcodes zur Software zu erhalten.

    2. Die Richtlinien zur angemessenen Nutzung von AWS (*AWS Acceptable Use Policy*) verfügbar unter https://aws.amazon.com/aup/) sind einzuhalten. Sie nehmen zur Kenntnis, dass AWS die Richtlinien zur angemessenen Nutzung von Zeit zu Zeit ändern kann und dass Sie bei einer Verlängerung des PureCloud Service dafür verantwortlich sind, die Richtlinien zur angemessenen Nutzung von AWS auf etwaige Änderungen zu überprüfen. Durch die weitere Nutzung des PureCloud Service nach Vertragsverlängerung erklären Sie sich mit den geänderten Bestimmungen einverstanden.

    3. PureCloud Edge-Geräte, andere Komponenten von Drittanbietern und/oder von Dritten erbrachte Dienstleistungen können Ihnen von unseren Geschäftspartnern im Zusammenhang mit Ihrer Nutzung des PureCloud Service zur Verfügung gestellt werden; dies erfolgt im jeweils vorliegenden Zustand (*as is*). Die für die Verwendung derartiger Hardware von Drittanbietern geltenden Bedingungen sind die Bedingungen der in dieser Hardware inkludierten *Shrink-Wrap-*, *Click-Wrap-* oder sonstigen Lizenzen von Drittanbietern. Sie sind dafür verantwortlich, den Ort, an dem die Installation der Hardware erfolgt, so vorzubereiten und instand zuhalten, dass damit allen Spezifikationen für Versorgungs-, Klima-, Verdrahtungs-, Netzwerk- und Kommunikationsschnittstellen entsprochen wird. Sie sind ebenfalls für die Durchführung regelmäßiger Wartungsarbeiten verantwortlich.

4. Sofern zutreffend erbringen wir die in einem Bestellformular oder in einer von Ihnen und uns unterfertigten Leistungsbeschreibung (*Statement of Work, SOW*) spezifizierten professionellen Dienstleistungen.

2. **Nutzungsbedingungen.** Das Recht auf Nutzung des Ihnen zur Verfügung gestellten PureCloud Service ist nicht exklusiv, auf die Vertragslaufzeit beschränkt, nicht übertragbar (außer für zuvor genehmigte Übertragungen, wie nachstehend beschrieben) und ausschließlich Ihren internen geschäftlichen Zwecken vorbehalten. Wir behalten uns alle Rechte, Titel- und Nutzungsansprüche im Zusammenhang mit dem PureCloud Service vor. Sie und Ihre Endnutzern werden es unterlassen sowie unterlassen zu versuchen: (i) das PureCloud Service oder einen ähnlichen Dienst an Nicht-Abonnenten zu lizenzieren, zu verkaufen, an solche zu leasen oder auf andere Weise für Nicht-Abonnenten verfügbar zu machen; (ii) das PureCloud Service auf eine Art und Weise einzusetzen, die gegen Gesetze, Verordnungen oder Vorschriften verstößt oder die Bestimmungen dieses Vertrags verletzt; und (iii) Handlungen vorzunehmen, die unsere vertraulichen oder geschützten Informationen gefährden, oder jegliche Rechte am PureCloud Service oder einer anderen Sache, die wir mit Ihnen geteilt oder Ihnen zur Verfügung gestellt haben, zu erwerben. Darüber hinaus kann eine ungewöhnlich hohe Nutzung des PureCloud Service unter Umständen unsere Fähigkeit beeinträchtigen, qualitativ hochwertige Dienste für andere Parteien zu erbringen und/oder auf eine unbefugte Nutzung der PureCloud Services hinweisen. In diesem Fall können wir die Nutzung durch Sie aussetzen oder beenden. Sie bestätigen und stimmen zu, dass Sie allein den Inhalt und Zeitpunkt Ihrer Telefonanrufe bestimmen.

3. **Kundendaten.**

    1. Kundendaten werden gemäß dem hier beigefügten Datenverarbeitungsdokument ("**Data Processing Schedule**", "**DPS**", "**Datenverarbeitungsdokument**") verarbeitet.

    2. Unsere Sicherheits- und Datenschutzrichtlinien sind als Bestandteil dieses Vertrags unter https://help.mypurecloud.com/articles/purecloud-security-compliance/ verfügbar.

    3. Sie sind berechtigt Kundendaten zur Verwendung mit dem PureCloud Service bereitstellen. Ungeachtet unserer Verpflichtungen im Rahmen des DPS sind Sie in Bezug auf Ihre Kundendaten der einzige für die Datenverarbeitung Verantwortliche (wie nach der anwendbaren Datenschutzgesetzgebung, einschließlich der Verordnung (EU) 2016/679, definiert), und tragen Sie die alleinige Verantwortung für den Inhalt und die rechtliche Zulässigkeit Ihrer Kundendaten. Wir erheben keinen Anspruch auf Eigentum an Kundendaten.

    4. Wir werden die Kundendaten in Einklang mit dem DPS, den in diesem Vertrag im Abschnitt zur Vertraulichkeit festgelegten Bestimmungen sowie unseren Sicherheits- und Datenschutzrichtlinien sicher und vertraulich aufbewahren. Sie bestätigen, dass Sie alle betroffenen Personen über unsere Verwendung von Kundendaten zur Bereitstellung des PureCloud Service an Sie informiert haben und über eine rechtmäßige Grundlage für unsere Verwendung von Kundendaten zur Bereitstellung des PureCloud Service an Sie verfügen, einschließlich unserer Nutzung von AWS zur Speicherung von Kundendaten in Übereinstimmung mit der AWS-Kundenvereinbarung (*AWS Customer Agreement*).

5. Sie stellen sicher, dass Sie angemessene Sicherheitsrichtlinien, darunter auch Richtlinien für die Datenarchivierung, implementiert haben. Sie sind für die Verteilung, laufende Verwaltung, Wartung, Sicherheit und ordnungsgemäße Verwendung aller gültigen Benutzernamen, Benutzer-IDs und Kennwörter, die in Verbindung mit dem PureCloud Service eingesetzt werden, verantwortlich.

4. **Gewährleistungen im Zusammenhang mit Abonnementdiensten.** Wir leisten Gewähr, dass das PureCloud Service im Wesentlichen so funktionieren wird, wie dies in den entsprechenden Servicebeschreibungen (verfügbar unter https://help.mypurecloud.com/?p=8858) im Detail beschrieben ist. Ihr einziger und ausschließlicher Rechtsbehelf bei einem Gewährleistungsfall ist folgendes: (i) Sie ermöglichen es uns, das PureCloud Service so zu modifizieren, dass es den Servicebeschreibungen entspricht, oder (ii) Sie ermöglichen es uns, eine Alternativlösung bereitzustellen, die Ihre Anforderungen angemessen erfüllt. Wenn keine dieser beiden Optionen wirtschaftlich vertretbar ist, können wir diesen Vertrag kündigen und Ihnen alle bereits bezahlten, noch nicht konsumierten Gebühren erstatten.

5. **Bereitstellung des PureCloud Service.** Wir stellen den PureCloud Service rund um die Uhr an sieben Tagen pro Woche bereit, mit Ausnahme von: (i) gelegentlichen geplanten Ausfallzeiten außerhalb von Spitzenzeiten (die wir im Vorfeld ankündigen werden); oder (ii) allen Fällen von Nichtverfügbarkeit, die durch Umstände verursacht werden, die sich unserer Kontrolle entziehen, einschließlich Ausfall oder Verzögerung Ihrer Internetverbindung, Fehlkonfiguration durch Sie oder Dritte, Probleme mit Ihrem Netzwerk oder mit Telekommunikationsdiensten, die von Ihnen oder für Sie vertraglich bezogen werden; oder (iii) Nichtverfügbarkeit aufgrund von Handlungen durch AWS, einschließlich (a) der Wartung oder geplanten Ausfallzeiten der AWS-Dienste, (b) eines Fehlers oder Ausfalls der AWS-Dienste oder (c) Beendigung der AWS-Kundenvereinbarung oder Suspendierung unserer oder Ihrer Nutzung von AWS-Diensten durch AWS. Ihre Nutzung des PureCloud Service unterliegt der Gesamtheit unserer PureCloud-Supportrichtlinien und Service Level Agreements ("**SLAs**"), die unter https://help.mypurecloud.com/articles/service-level-agreements/ verfügbar sind.

6. **Laufzeit und Zahlungen.**

    1. **Laufzeit.** Dieser Vertrag regelt die Nutzung der PureCloud Services ab dem Datum des Inkrafttretens und bleibt bis zum Laufzeitende in Kraft. Vor Beginn der Laufzeit wird Ihnen eine Frist von neunzig (90) Tagen eingeräumt, um Ihnen die Implementierung der PureCloud Services zu ermöglichen („**Anlaufphase**“). Die Laufzeit dieses Vertrags beginnt mit dem Ende dieser Anlaufphase. Am Ende der Laufzeit verlängert sich der Vertrag monatlich (mit einer monatlichen Zahlungsstruktur, wie in Punkt 6.2.1 beschrieben), es sei denn: (a) eine der Parteien teilt mindestens dreißig (30) Tage im Voraus schriftlich mit, dass sie keine Verlängerung wünscht; oder (b) die Parteien vereinbaren schriftlich eine Verlängerung der Laufzeit für einen anderen Zeitraum. Die Preise für alle folgenden Verlängerungsperioden bestimmen sich anhand unserer zum betreffenden Zeitpunkt geltenden Listenpreise, sofern nicht in einem Bestellformular eine andere Regelung getroffen wird.

    2. **Zahlungsstruktur.** Sie haben die auf dem entsprechenden Bestellformular angeführten Gebühren zu bezahlen. Die Abonnementzahlungen sind je nach der von Ihnen gewählten Laufzeit unterschiedlich strukturiert. Die Zahlungsstruktur wird im Bestellformular angegeben.

1. **Monatliche Laufzeit**. Die jeweils anfallenden monatlichen Gebühren werden nach Nutzung berechnet und Ihnen monatlich im Nachhinein in Rechnung gestellt. Die Zahlung hat innerhalb von 30 (dreißig) Tagen nach dem Rechnungsdatum zu erfolgen. Die Abonnementpreise für die monatliche Laufzeit können sich in Abhängigkeit mit unserer zum betreffenden Zeitpunkt geltenden Preisgestaltung ändern. Beachten Sie bitte, dass der Abonnementpreis für eine monatliche Laufzeit höher als für eine jährliche Laufzeit ist. Während der Anlaufphase kommt kein monatliches Mindestlimit zur Anwendung. Nach der Anlaufphase gilt ein monatliches Mindestlimit, das im Bestellformular angegeben ist.
2. **Jährliche Laufzeit**.
    1. **Jährliche Zahlung.** Sofern das betreffende Bestellformular keine anderen Zahlungsbedingungen enthält, werden Ihnen die Abonnementgebühren für zwölf Monate im Voraus in Rechnung gestellt. Diese Zahlung ist innerhalb von dreißig (30) Tagen ab dem Datum des Inkrafttretens zu leisten, unabhängig davon, ob eine Anlaufphase zur Anwendung kommt. Diese Zahlung deckt die Laufzeit des Vertrags, beginnend mit dem Ende der Anlaufphase, ab. **Für die Dauer der Anlaufphase wird Ihnen die tatsächliche Nutzung zu den im Bestellformular angegebenen anteiligen Jahresgebühren in Rechnung gestellt.** Wenn nach der Anlaufphase in einem Monat die tatsächliche Nutzung über dem im Bestellformular angegebenen Betrag für das Jahresabonnement liegt (anteilig für den Zeitraum von einem Monat berechnet), wird Ihnen die Überschreitung des Abonnementlimits zu der im Bestellformular angegebenen Gebühr bei Überschreitung von Abonnementlimits in Rechnung gestellt. Alle Rechnungen sind innerhalb von 30 (dreißig) Tagen ab Rechnungsdatum zur Zahlung fällig. Ein ggf. vorausbezahlter Betrag kann nicht erstattet werden.
    2. **Monatliche Zahlung.** Für die Dauer der Anlaufphase wird Ihnen die tatsächliche Nutzung zu den im Bestellformular angegebenen monatlichen Abonnementgebühren in Rechnung gestellt. Ihre monatlichen Abonnementgebühren sind im Bestellformular angeführt. Nach der Anlaufphase kommt als Mindestrechnungsbetrag der Betrag des monatlichen Abonnements zur Anwendung. Jede über das monatliche Abonnement hinausgehende Nutzung wird zu der im Bestellformular angegebenen Gebühr bei Überschreitung von Abonnementlimits in Rechnung gestellt.
3. **Zahlungsverzug.** Für alle überfälligen Zahlungen werden Verzugszinsen in Höhe von 1,5% pro Monat bzw. dem ggf. gesetzlich vorgeschriebenen niedrigeren Zinssatz erhoben. Wenn ein in Rechnung gestellter Betrag mehr als dreißig (30) Tage überfällig ist, können wir Ihre Nutzung des PureCloud Service mit sofortiger Wirkung suspendieren, sofern wir Sie unter Androhung der Diensteunterbrechung oder –abschaltung sowie unter Setzung einer Nachfrist von mindestens 14 Tagen schriftlich gemahnt haben.

4. **Steuern.** Sofern im Bestellformular nicht anders angegeben, enthalten die Gebühren keine Steuern, Abgaben, Zölle oder ähnliche behördliche Abgaben, einschließlich Mehrwert-, Umsatz-, Verbrauchs- oder Quellensteuer (zusammen als „**Steuern**“ bezeichnet). Sie sind dafür verantwortlich, alle im Zusammenhang mit dem Bestellformular stehenden Steuern zu bezahlen und uns alle von uns für die im Rahmen des Bestellformulars fälligen Beträge bezahlten Steuern – mit Ausnahme von auf Ihr Einkommen erhobenen Steuern – zu erstatten.

7. Kündigung.

1. **Kündigung aus wichtigem Grund.** Jede Partei kann diesen Vertrag mittels schriftlicher Kündigungsmitteilung an die jeweils andere Partei mit sofortiger Wirkung kündigen, ohne dass hieraus eine Haftung gegenüber der anderen Partei resultiert, wenn: (a) die andere Partei wesentlich gegen diesen Vertrag verstößt (im Fall des Kunden ist dies auch bei einem Verstoß gegen die Richtlinien zur angemessenen Nutzung von AWS gegeben) und (sofern der betreffende Verstoß behoben werden kann) diesen Verstoß nicht innerhalb von dreißig (30) Tagen nach Erhalt einer schriftlichen Benachrichtigung mit der Aufforderung zur Behebung des Verstoßes behebt; und wenn (b) die andere Partei Gegenstand eines Konkursverfahrens ist oder insolvent wird oder mit ihren Gläubigern eine einvernehmliche Regelung oder einen Vergleich schließt oder eine Abtretung zu ihren Gunsten vornimmt oder wenn ihr Vermögen ganz oder teilweise Sicherungsmaßnahmen jeder Art unterliegt, oder die andere Partei freiwillig oder unfreiwillig in Liquidation geht (mit Ausnahme einer freiwilligen Liquidation zum Zweck einer Umstrukturierung oder eines Unternehmenszusammenschlusses) oder wenn ein Sach- oder Vermögensverwalter für das Vermögen der anderen Partei bestellt wird (oder ein nach der Rechtsordnung der betreffenden anderen Partei gleichwertiger Fall eintritt). Wenn Sie diesen Vertrag aus wichtigem Grund kündigen, erstatten wir Ihnen als einzigen und ausschließlichen Rechtsbehelf alle bereits bezahlten, noch nicht konsumierten Gebühren für das PureCloud Service.

2. **Auswirkungen der Kündigung.** Wenn dieser Vertrag gekündigt wird oder ausläuft, gilt Folgendes: (a) Ihr Recht auf Zugriff auf die PureCloud Services endet mit sofortiger Wirkung; und (b) wir bewahren Daten für einen Zeitraum von dreißig (30) Tagen (bzw. den nach geltendem Recht vorgeschriebenen Zeitraum) auf. In diesem Zeitraum können Sie eine Kopie Ihrer Daten anfordern. Die folgenden Abschnitte bleiben auch nach Beendigung dieses Vertrags durch Zeitablauf oder vorzeitiger Kündigung aus jeglichem Grund weiterhin aufrecht und wirksam: Auswirkung der Kündigung, Vertraulichkeit, Nutzungsbedingungen, Kundendaten, Zahlungen, Gewährleistungsausschluss, Entschädigungspflichten, Haftungsbeschränkung und Sonstige Bestimmungen.

8. Geheimhaltung. Zusätzlich zu den in Abschnitt 3 (Kundendaten) festgelegten Schutzmechanismen werden wir angemessene Maßnahmen ergreifen, um zu verhindern, dass Dritte Ihre Kundendaten erhalten können. Unsere vertraulichen Informationen können wertvolles geistiges Eigentum enthalten. Sie nehmen daher zur Kenntnis und stimmen zu, dass im Zusammenhang mit Ihrer Nutzung des PureCloud Service an Sie weitergegebene oder Ihnen zur Verfügung gestellte Informationen vertraulich sind und Sie angemessene Sorgfalt darauf zu verwenden haben, zu verhindern, dass andere Personen diese Informationen erhalten können.

Vertraulichkeitsverpflichtungen gelten jedoch nicht für Informationen, die (i) jetzt oder in Zukunft allgemein bekannt oder verfügbar sind oder werden; oder (ii) aufgrund gesetzlicher Bestimmungen bekannt gegeben werden müssen.

9. **Gewährleistungsausschluss.** SOFERN NICHT IN DIESEM VERTRAG AUSDRÜCKLICH EINE ANDERE REGELUNG FESTGELEGT IST, WERDEN DAS PURECLOUD SERVICE, DIE AUSSTATTUNG UND ANDERE DIENSTE, LIEFERGEGENSTÄNDE, PRODUKTE UND MATERIALIEN IN IHREM VORLIEGENDEN ZUSTAND („AS IS“) BEREITGESTELLT. WIR SCHLIESSEN IM GRÖSSTMÖGLICHEN RECHTLICH ZULÄSSIGEN UMFANG ALLE ANDEREN AUSDRÜCKLICHEN, STILLSCHWEIGENDEN UND GESETZLICHEN GEWÄHRLEISTUNGEN AUS, EINSCHLIESSLICH ALLER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN IM HINBLICK AUF VERMARKTBARKEIT, QUALITÄT, EIGENTUMSRECHT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, NICHTVERLETZUNG VON RECHTEN DRITTER, KOMPATIBILITÄT, UNGESTÖRTE NUTZUNG, AKTUALITÄT, VOLLSTÄNDIGKEIT ODER RICHTIGKEIT. OHNE DIE GÜLTIGKEIT DES VORSTEHENDEN EINZUSCHRÄNKEN GEWÄHRLEISTEN WIR NICHT, DASS DER ZUGANG ZU ODER DIE NUTZUNG DES PURECLOUD SERVICE ODER ANDERER DIENSTE ODER VON UNS BEREITGESTELLTER MATERIALIEN OHNE UNTERBRECHUNG ODER FEHLERFREI ERFOLGT. SIE SELBST SIND DAFÜR VERANTWORTLICH, DEN FÜR DIE ERZIELUNG DER VON IHNEN GEWÜNSCHTEN ERGEBNISSE ERFORDERLICHEN DIENST ZU WÄHLEN.

10. **Schad- und Klagloshaltung durch Genesys.** Unter dem Vorbehalt, dass Sie die Bestimmungen von Abschnitt 13 (Verfahren zur Schad- und Klagloshaltung) einhalten, werden wir Sie für alle Verluste, Schäden, Kosten, Aufwendungen und sonstigen Verbindlichkeiten (einschließlich angemessener Rechtskosten) schad- und klaglos halten, die Ihnen entstanden sind, zur Zahlung aufgetragen wurden oder deren Übernahme Sie zugestimmt haben und die sich aufgrund von Ansprüchen Dritter ergeben, die mit der Begründung vorgebracht werden, der PureCloud Service würde Patent- oder Urheberrechte oder Geschäftsgeheimnisse des betreffenden Dritten verletzen, solange diese Ansprüche nicht unter Abschnitt 12 (Haftungsausschluss) fallen. Wenn Ihre Nutzung des PureCloud Service Rechte an geistigem Eigentum Dritter verletzt, können wir nach unserem Ermessen: (i) eine Lizenz von dem betreffenden Dritten mit Ihnen als Begünstigtem einholen; (ii) den PureCloud Service so modifizieren, dass der Tatbestand der Verletzung nicht mehr besteht; oder (iii), wenn keine dieser Optionen kommerziell durchführbar ist, von Ihnen verlangen, die Nutzung des PureCloud Service einzustellen, diesen Vertrag kündigen und Ihnen alle bereits bezahlten, noch nicht konsumierten Gebühren erstatten.

11. **Schad- und Klagloshaltung durch den Kunden.** Für alle Verluste, Schäden, Kosten, Aufwendungen und sonstige Verbindlichkeiten (einschließlich angemessener Rechtskosten) die uns im Zusammenhang mit Haftungsausschlüssen im Sinne von Abschnitt 12. entstanden sind, zur Zahlung aufgetragen wurden oder deren Übernahme wir zugestimmt haben, werden Sie uns schad- und klaglos halten.

12. **Haftungsausschluss**. Als ausgeschlossen von unseren Gewährleistungs- und/oder Rechtsverteidigungs- oder Schad- und Klagloshaltungsverpflichtungen im Rahmen dieses Vertrags gelten Ansprüche aus: (i) Nichteinhaltung dieses Vertrags durch Sie; (ii) Ihrer Geschäftsmethode(n) oder -verfahren; oder (iii) Ihrer Inhalte, Kundendaten oder Produkte von Drittanbietern.

13. **Verfahren zur Schad- und Klagloshaltung.** Die Partei, die einen Anspruch auf Schadenersatz hat („**zu entschädigende Partei**“), wird die jeweils andere Partei („**entschädigungspflichtige Partei**“) unverzüglich von jeder zu entschädigenden Forderung („**Forderung**“) benachrichtigen und die entschädigungspflichtige Partei auf deren Kosten in angemessenem Rahmen unterstützen. Erfolgt keine rechtzeitige Benachrichtigung oder angemessene Unterstützung, wird die entschädigungspflichtige Partei von ihren Entschädigungspflichten entbunden, soweit die entschädigungspflichtige Partei durch dieses Säumnis einen wesentlichen Nachteil erlitten hat. Die entschädigungspflichtige Partei hat das alleinige Recht, Verteidigungsmaßnahmen gegen eine Forderung zu ergreifen oder einen Vergleich bezüglich einer Forderung einzugehen (dabei gilt jedoch die Ausnahme, dass die entschädigungspflichtige Partei einen Vergleich, durch den die zu entschädigende Partei nicht uneingeschränkt von allen Verpflichtungen entbunden wird, nicht ohne vorherige schriftliche Zustimmung der zu entschädigenden Partei eingehen darf).

14. **Ausschluss von Folge- und mittelbaren Schäden.** Vorbehaltlich der Bestimmungen von Abschnitt 16 haftet keine der Parteien für:

    1. INDIREKTE, BESONDERE, ZUFÄLLIG ENTSTANDENE FOLGESCHÄDEN, DECKUNGSSCHÄDEN ODER ANDERE VERGLEICHBARE SCHÄDEN JEDER ART UND BESTEHEN KEINE ANSPRÜCHE AUS STRAFSCHADENERSATZ;

    2. EINEN GEWINNENTGANG, GESCHÄFTS- ODER FIRMENWERTVERLUST (EINSCHLIESSLICH VERMÖGENSSCHÄDEN, DIE AUS EINEM FIRMENWERTVERLUST RESULTIEREN), EINEN UMSATZVERLUST SOWIE DEN VERLUST, BESCHÄDIGUNG ODER ZERSTÖRUNG VON DATEN, UND/ODER

    3. EINEN VERLUST, DER DIE FOLGE EINER ÜBERTRAGUNG VON VIREN IST.

15. **Haftungsbeschränkung.** VORBEHALTLICH DER ABSCHNITTE 14 UND 16 IST UNSERER HAFTUNG AUFGRUND VON VERTRAGLICHEN BESTIMMUNGEN, UNERLAUBTER HANDLUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER VERLETZUNG GESETZLICH VORGESCHRIEBENER VERPFLICHTUNGEN), PRODUKTHAFTUNG, VORSÄTZLICHER FEHLDARSTELLUNG, RESTITUTION ODER AUS SONSTIGEN GRÜNDEN, DIE SICH AUS DER ERFÜLLUNG ODER DER BEABSICHTIGTEN ERFÜLLUNG DIESES VERTRAGS ERGIBT, MIT DER SUMME DER IN DEN DER ENTSTEHUNG DES BETREFFENDEN ANSPRUCHS VORANGEGANGENEN ZWÖLF (12) MONATE AN UNS BEZAHLTEN ODER ZU BEZAHLENDEN GEBÜHREN BZW., FALLS DER ANSPRUCH WÄHREND EINES ZEITRAUMS VON WENIGER ALS ZWÖLF (12) MONATEN AB DEM ZEITPUNKT DES INKRAFTTRETENS ENTSTANDEN IST, DIE SUMME DER IN DIESEM KÜRZEREN ZEITRAUM AN UNS BEZAHLTEN ODER ZU BEZAHLENDEN GEBÜHREN, BETRAGLICH BESCHRÄNKT. DIESE HAFTUNGSBESCHRÄNKUNG STELLT EINE WESENTLICHE GRUNDLAGE FÜR DIE GETROFFENEN VEREINBARUNGEN DAR, DA ANDERENFALLS DIE JÄHRLICHE (ODER KÜRZERE) LAUFZEIT UND DIE JEWEILIGEN GEBÜHREN ANDERS ALS IN DIESEM VERTRAG FESTGELEGT SEIN WÜRDEN. DIESER ABSCHNITT GILT NICHT FÜR SCHÄDEN, DIE AUFGRUND GESETZLICHER BESTIMMUNGEN NICHT AUSGESCHLOSSEN

ODER BESCHRÄNKT WERDEN KÖNNEN (IN SOLCHEN FÄLLEN GILT ALS BESCHRÄNKUNG DAS JEWEILS GESETZLICH VORGESCHRIEBENEN MINDESTMASS). **DIESER ABSCHNITT UND UNSERE IHNEN GEGENÜBER GEMÄSS ABSCHNITT 10 GELTENDEN VERPFLICHTUNGEN ZUR SCHAD- UND KLAGLOSHALTUNG STELLEN IHREN EINZIGEN UND AUSSCHLIESSLICHEN RECHTSBEHELF FÜR ANSPRÜCHE AUFGRUND VON VERSTÖSSEN GEGEN BESTIMMUNGEN ODER RECHTE DAR, DIE SICH AUS ODER IN ZUSAMMENHANG MIT DIESEM VERTRAG ERGEBEN.**

16. **Nicht ausschließbare Haftungen**. DURCH KEINE BESTIMMUNG DIESES VERTRAGS WIRD DIE HAFTUNG DER PARTEIEN FÜR FOLGENDES AUSGESCHLOSSEN: (A) TOD ODER PERSONENSCHADEN; (B) BETRUG ODER BETRÜGERISCHE FEHLDARSTELLUNG; ODER (C) JEDE SONSTIGE HAFTUNG, DIE NACH ANWENDBAREM RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN.

17. **Sonstige Bestimmungen.**

    1. **Gesamte Vereinbarung und anwendbares Recht.** Dieser Vertrag, zusammen mit dem Bestellformular und den anderen hierin genannten Dokumenten, stellt die gesamte Übereinkunft der Parteien dar und tritt an die Stelle aller früheren oder aktuellen Vereinbarungen, gleich ob diese schriftlich oder mündlich getroffen wurden. Im Fall einer Diskrepanz zwischen diesem Vertrag und einem Bestellformular oder einer Leistungsbeschreibung (SOW) ist dieser Vertrag maßgeblich. Dieser Vertrag unterliegt dem Recht von England und Wales. Die Parteien vereinbaren unwiderruflich, dass die Gerichte von England und Wales die nicht ausschließliche Zuständigkeit zur Entscheidung über alle durch Recht oder Vertrag begründeten Ansprüche haben, die sich aus oder in Zusammenhang mit diesem Vertrag ergeben. Wir werden durch keine Bestimmung dieses Vertrags daran gehindert, bei jedem zuständigen Gericht für Sie einstweiligen Rechtsschutz zu erwirken.

    2. **Abtretung.** Eine Abtretung oder anderweitige Übertragung der Rechte und Pflichten des Kunden aus diesem Vertrag durch den Kunden ist nur mit unserer vorherigen schriftlichen Zustimmung möglich, die wir nicht unangemessen vorenthalten werden. Jeder Versuch, eine Abtretung unter Nichteinhaltung der Bestimmungen dieses Abschnitts durchzuführen, ist nichtig. Sie haben Kenntnis davon und stimmen zu, dass Dritte, unter anderem auch unsere verbundenen Unternehmen (z.B. Genesys Telecom US, Inc.), Ihnen Produkte und Dienste im Zusammenhang mit den PureCloud Services zur Verfügung stellen können und Ihnen dies in Rechnung gestellt werden kann.

    3. **Einhaltung von Gesetzen.** Wir werden alle angemessenen Anstrengungen unternehmen, um ethisch und gesetzestreu zu handeln und zwingende gesetzliche Bestimmungen einzuhalten, einschließlich der Gesetze zur Bekämpfung von Korruption und Bestechung. Es ist uns allerdings nicht möglich, zu überprüfen, ob sämtliche Vorhaben, die Sie mit unseren Produkten und Diensten umsetzen oder umsetzen wollen, im Einklang mit allen geltenden Gesetzen stehen. Sie sind dafür verantwortlich, sicherzustellen, dass Ihre Nutzung sämtlicher Produkte und Dienste den für Sie und Ihr Unternehmen oder Ihre Branche geltenden Gesetzen und Bestimmungen entspricht. Keine der Parteien übernimmt die Verantwortung für die Einhaltung der geltenden

Gesetze durch die jeweils andere Partei. Außerdem ist Ihnen die Ausfuhr oder Wiederausfuhr von Produkten oder unseren vertraulichen oder geschützten Informationen, gleich ob direkt oder indirekt, in Länder außerhalb der Vereinigten Staaten nicht gestattet, es sei denn, dies ist nach den *Export Administration Regulations* (Exportbestimmungen) des US-Handelsministeriums zulässig. Die Produkte enthalten kommerzielle Computersoftware im Sinne der Federal *Government Acquisition Regulations* (Beschaffungsverordnung der US-Bundesbehörden) und den sie ergänzenden Bestimmungen und werden ausschließlich unter Einhaltung der in den *Government Acquisition Regulations* festgelegten *Restricted Rights Provision* (Bestimmung zur Einschränkung von Rechten), die für kommerzielle Computersoftware gilt, deren Entwicklung privat finanziert wurde und die nicht öffentlich zugänglich ist, an die Bundesregierung und ihre Dienststellen bereitgestellt. Sie gewährleisten, dass weder Sie, ein verbundenes Unternehmen oder ein Benutzer auf einer von einer Regierung veröffentlichten Liste mit eingeschränkten Personen oder Organisationen aufscheinen. Dazu zählen unter anderem folgende Listen: „*Entity List*“, „*Denied Persons List*“ und „*Unverified List*“ des US-Handelsministeriums, „*Specially Designated Nationals and Blocked Persons List*“ des US-Finanzministeriums und „*Debarred Parties List*“ des US-Außenministeriums.

4. **Einhaltung von Gesetzen zur Bekämpfung von Korruption und Bestechung.** Bezüglich aller Handlungen oder Tätigkeiten in Verbindung mit diesem Vertrag oder im Zusammenhang mit der zwischen den Parteien bestehenden Beziehung wird keine der Parteien rechtswidrige Handels- oder sonstige Praktiken betreiben, die gegen den *U.S. Foreign Corrupt Practices Act* (US-Gesetz zur Bekämpfung internationaler Korruption), den *U.K. Bribery Act* (britisches Anti-Korruptionsgesetz) oder sonstige Gesetze verstoßen, die Bestechung oder ähnliche Aktivitäten unter Verbot stellen. Jede der Parteien hat sicherzustellen, dass weder sie noch ihre verbundenen Unternehmen, Subunternehmer und Vertreter direkt oder indirekt Geldbeträge, Schmiergelder oder andere geldwerte Zuwendungen verlangen, erhalten, annehmen, übergeben, anbieten, vereinbaren oder in Aussicht stellen (dies betrifft unter anderem, ohne darauf beschränkt zu sein, Vertreter oder Amtsträger von staatlichen Stellen oder Unternehmen), die als unzulässiger Anreiz oder Belohnung oder auf andere Weise als Motivation für die Vornahme oder Unterlassung von Handlungen oder die Ausübung von Einfluss dienen; oder es verabsäumen, angemessene Sicherheitsvorkehrungen zum Schutz vor solchen unzulässigen Handlungen zu treffen. Jede der Parteien wird auf Verlangen der jeweils anderen Partei Nachweise für die zur Vermeidung solcher unzulässiger Handlungen getroffenen Maßnahmen erbringen; unter anderem über die Einführung von Richtlinien, Praktiken und/oder unternehmerischen Kontrollmechanismen im Zusammenhang mit diesen Gesetzen. Soweit die zuständige Behörde dies gestattet, wird jede der Parteien die jeweils andere Partei unverzüglich von allen amtlichen Ermittlungen aufgrund mutmaßlicher Verstöße gegen die vorstehend genannten Gesetze informieren, die in irgendeinem Zusammenhang mit diesem Vertrag stehen.

5. **Mitteilungen.** Für Mitteilungen zwischen den Parteien ist die in der entsprechenden Richtlinie (verfügbar unter

https://help.mypurecloud.com/articles/notices/) festgelegte Vorgangsweise anzuwenden.

6. **Verzicht.** Sollte eine der Bestimmungen dieses Vertrags in irgendeiner Hinsicht ungültig, gesetzwidrig oder undurchsetzbar sein oder werden, so gilt diese aus diesem Vertrag gestrichen, und die Gültigkeit, Rechtmäßigkeit und Durchsetzbarkeit der übrigen Bestimmungen bleibt davon unberührt. Wenn wir bei einem von Ihnen begangenen Verstoß gegen diesen Vertrag nicht einschreiten, gilt dies keinesfalls als Verzicht auf unsere Rechte im Zusammenhang mit weiteren oder ähnlichen Verstößen.
7. **Rechtsbehelfe.** Alle uns zustehenden Rechtsbehelfe sind kumulativ, und die Inanspruchnahme eines Rechtsbehelfes schließt die Inanspruchnahme anderer Rechtsbehelfe, die im Gesetz oder anderweitig vorgesehen sind, nicht aus. Keine der Parteien haftet für eine Nichterfüllung im Rahmen dieses Vertrags, die auf Ursachen beruht, die außerhalb ihrer zumutbaren Kontrolle liegen und trotz angemessener Anstrengungen ohne ihr fehlerhaftes oder fahrlässiges Verhalten eintreten.
8. **Änderungen.** Für Änderungen gilt grundsätzlich Punkt 23 des Zusatzes zu diesem Vertrag. Sofern der Zusatz nicht anwendbar ist, gilt folgendes: Wir können Websites, auf die in diesem Vertrag verwiesen wird, jederzeit ändern, indem wir eine aktualisierte Version auf der PureCloud-Website veröffentlichen oder indem wir Sie in Übereinstimmung mit Abschnitt 17.5 benachrichtigen. Die geänderten Bedingungen werden mit Veröffentlichung bzw., wenn wir Sie per E-Mail benachrichtigen, so wie in der E-Mail-Nachricht angegeben wirksam. Durch die weitere Nutzung des PureCloud Service nach dem Wirksamkeitsdatum solcher Änderungen erklären Sie sich mit den geänderten Bestimmungen einverstanden. Wenn wir die uns obliegenden Verpflichtungen oder die Funktionalität des PureCloud Service wesentlich reduzieren, werden wir entweder Ihre Zustimmung einholen oder Sie können diesen Vertrag kündigen. Für jede Änderung der Bedingungen dieses Vertrags, bei der es sich nicht um eine Änderung der hierin genannten Web-Links handelt, ist die schriftliche Zustimmung beider Parteien erforderlich.
9. **Geschäftspartner.** Unsere Begünstigungen, Rechte und Pflichten im Zusammenhang mit den Nutzungsbedingungen, dem Haftungsausschluss, der Schad- und Klagloshaltung durch den Kunden, dem Haftunsgausschluss, der Haftungsbeschränkung, der Vertraulichkeit und der Einhaltung der gesetzlichen Bestimmungen erstrecken sich auch auf unsere verbundenen Unternehmen, nahestehenden Personen und Unternehmen, Geschäftspartner, Lizenzgeber und Dienstleister.
10. **Ihre Benutzer.** Sie sind vollumfänglich dafür verantwortlich, dass alle Ihre Mitarbeiter, Ihre externen Dienstleister und alle anderen Dritten, die auf die PureCloud Services zugreifen oder diese nutzen, diesen Vertrag einhalten, und Sie haften für deren Handlungen und Unterlassungen.

18. Definitionen.

1. „**Bestellformular**“ bezeichnet das zur Übermittlung der Bestellung verwendete Dokument, in dem die hier bestellten PureCloud-Produkte und -gebühren angeführt sind. Eine Kopie des Bestellformulars wird Ihnen per E-Mail übermittelt.

2. „**PureCloud Service**“ bezeichnet unseren Cloud-Kommunikationsdienst sowie die diesbezügliche Ausstattung und die damit verbundenen Leistungen, wie im Bestellformular beschrieben.
3. „**PureCloud Website**“ bezeichnet die Website, die für den Zugriff auf den PureCloud Service verwendet wird, sowie alle von uns spezifizierten Nachfolge-Websites oder verbundenen Websites.
4. „**Software**“ bezeichnet die im Eigentum von Genesys stehende Software, die zur Bereitstellung der PureCloud Services eingesetzt wird, einschließlich der im Bestellformular angeführten Software, jedoch ausgenommen jede Software, die von den Geschäftspartnern von Genesys bereitgestellt wird.
5. „**Laufzeit**“ bezeichnet die im Bestellformular angegebene Laufzeit der PureCloud Services, die Sie ausgewählt haben.

Datenverarbeitungsdokument

1. **DEFINITIONEN**
    a. ***Allgemein.*** In diesem DPS mit großem Anfangsbuchstaben geschriebene Begriffe, die nicht darin definiert sind, haben die ihnen im Rahmenvertrag oder in der Datenschutzgesetzgebung zugewiesene Bedeutung.
    b. Der Begriff ***verbundenes Unternehmen*** bedeutet in Bezug auf ein Unternehmen jedes andere Unternehmen, das dieses direkt oder indirekt beherrscht oder von ihm beherrscht wird oder zusammen mit ihm unter gemeinsamer Beherrschung steht.
    c. ***Kundendaten*** sind die personenbezogenen Daten (wie im Datenschutzgesetzgebung definiert), die zum Service hochgeladen werden.
    d. ***EWR*** ist der Europäische Wirtschaftsraum.
    e. ***Rahmenvertrag*** bezeichnet den zwischen Genesys und dem Kunden geschlossenen Vertrag über die Erbringung von Services.
    f. ***Datenschutzgesetzgebung*** bezeichnet die Verordnung (EU) 2016/679 (die „***Datenschutzgrundverordnung***"), die Richtlinie 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation) und alle weiteren anwendbaren nationalen und internationalen Gesetze und Verordnungen zum Datenschutz und Schutz der Privatsphäre in ihrer jeweils geltenden Fassung bzw. ihrer novellierten oder Nachfolgeversion.
    g. ***Service(s)*** bezeichnet die Software, professionellen Dienste und Kundenbetreuungsleistungen, die von Genesys erbracht werden und im Rahmenvertrag näher beschrieben sind.
    h. ***Standardvertragsklauseln*** bezeichnet die in DPS Anlage 1 zu diesem DPS enthaltenen Standardvertragsklauseln im Sinne des Beschlusses der Europäischen Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG.

2. **DATENVERARBEITUNG**
    a. ***Geltungsbereich.*** Dieses DPS regelt die Verarbeitung von Kundendaten durch Genesys. Der Zweck dieses DPS besteht darin, die Datenverarbeitung im Zusammenhang mit den Services in Übereinstimmung mit dem Rahmenvertrag zu regeln. Die Laufzeit dieses DPS ist dieselbe wie die des Rahmenvertrags.
    b. ***Einhaltung der Gesetze.*** Jede Partei hat alle für sie geltenden Gesetze, Vorschriften und Bestimmungen einzuhalten.
    c. ***Anweisungen zur Datenverarbeitung.*** Genesys wird die Kundendaten gemäß den Anweisungen des Kunden verarbeiten, wie dies in diesem DPS und im Rahmenvertrag festgelegt ist. Der Kunde wird als Erstes die Funktionen der von Genesys bereitgestellten Plattform nutzen, um die Einhaltung der ihm auf Basis der geltenden Datenschutzgesetzgebung obliegenden Datenschutzverpflichtungen sicherzustellen. Wenn der Kunde eine aufgrund der geltenden Datenschutzgesetzgebung erforderliche Handlung mit den von

Genesys zur Verfügung gestellten Tools oder Funktionen nicht bewerkstelligen kann, ist er berechtigt, Genesys detaillierte Anweisungen zu erteilen. Mündlich seitens des Kunden erfolgte Anweisungen in Bezug auf Datenschutzbelange sind vom Kunden unmittelbar danach über ein Support-Ticket oder eine E-Mail an DataPrivacy@Genesys.com zu bestätigen. Wenn der Kunde eine Anweisung im Rahmen dieses DPS erteilt, wird Genesys diese Anweisung für die Dauer des DPS dokumentieren, um die Einhaltung der Rechenschaftspflicht nach der geltenden Datenschutzgesetzgebung sicherzustellen.

d. ***Dateneigentum.*** Alle Rechte, Eigentums- und Nutzungsansprüche an seinen Kundendaten verbleiben beim Kunden. Der Kunde gewährt Genesys ein nicht ausschließliches Recht zur Verarbeitung, Verwendung, Vervielfältigung, Speicherung, Übertragung, Abänderung, Darstellung und Ausführung der Kundendaten sowie zur Erstellung abgeleiteter Werke davon, und zwar ausschließlich in dem Umfang, der zur Erbringung des Service, wie dies im Rahmenvertrag definiert und nach den geltenden gesetzlichen Bestimmungen zulässig ist.
e. ***Zugriff oder Verwendung.*** Genesys wird nur soweit auf Kundendaten zugreifen oder diese verwenden, wie dies zur Erbringung des Service oder nach Anweisung des Kunden erforderlich ist.
f. ***Weitergabe.*** Genesys wird Kundendaten nicht an staatliche Stellen weitergeben, außer wenn dies erforderlich ist, um geltende Gesetze, oder eine gültige und verbindliche Anweisung einer Strafverfolgungsbehörde (z.B. eine Vorladung oder gerichtliche Anordnung) zu befolgen. Sollte eine Strafverfolgungsbehörde Kundendaten von Genesys verlangen, wird Genesys zu erwirken versuchen, dass die Strafverfolgungsbehörde diese Daten direkt vom Kunden verlangt. Im Rahmen eines solchen Versuchs kann Genesys der Strafverfolgungsbehörde ein Mindestmaß an Kontaktinformationen des Kunden zur Verfügung stellen. Sollte Genesys von einer Strafverfolgungsbehörde eine verbindliche Anordnung zur Weitergabe von Kundendaten erhalten, wird Genesys – sofern dies Genesys nicht gesetzlich untersagt ist – den Kunden über den Erhalt dieser Anweisung informieren, damit der Kunde eine Schutzanordnung beantragen oder ein anderes geeignetes Rechtsmittel einlegen kann.
g. ***Personal von Genesys.*** Das Personal von Genesys darf Kundendaten nur mit entsprechender interner Genehmigung verarbeiten. Alle Mitglieder des Personals von Genesys erhalten jährlich Schulungen zum Thema Datensicherheit und Datenschutz und sind entsprechende Geheimhaltungsverpflichtungen (sowohl während ihres Beschäftigungsverhältnisses als auch danach) eingegangen, soweit sie nicht ohnehin aufgrund der maßgeblichen Gesetze und Vorschriften dazu verpflichtet sind.
h. ***Datenkontrolle.*** Falls eine betroffene Person Genesys im Zusammenhang mit der Berichtigung, Löschung oder der Einschränkung der Verarbeitung von Daten direkt kontaktiert, wird Genesys das Ersuchen des Betroffenen so rasch

wie möglich an den Kunden weiterleiten. Soweit dies Teil des Leistungsumfangs ist, wird Genesys die Einforderung des Rechts auf Löschung, "Vergessenwerden" , Berichtigung, Datenübertragbarkeit und Auskunft ohne ungebührliche Verzug sicherstellen, oder wird Genesys dem Kunden Hilfsmittel zur Verfügung stellen, um solchen Anforderungen über das Service nachzukommen.

i. ***Übermittlung von Kundendaten.*** Dem Kunden ist bekannt, dass für die von Genesys bereitgestellten Services in manchen Fällen Kundendaten in ein Land oder Gebiet außerhalb des EWR übermittelt werden müssen. Der Kunde erteilt seine Zustimmung dazu, dass Genesys Kundendaten in ein solches Land übermittelt und die Kundendaten speichert und verarbeitet, um die Services bereitstellen zu können. Die Standardvertragsklauseln gelten für Kundendaten, die direkt oder per Weiterleitung außerhalb des EWR in ein Land übermittelt werden, das von der EU-Kommission nicht als Land mit einem angemessenen Schutzniveau für personenbezogene Daten (im Sinne der geltenden Datenschutzgesetzgebung) erachtet wird. Die Standardvertragsklauseln gelten nicht für Kundendaten, die direkt oder durch Weiterleitung nicht in Gebiete außerhalb des EWR übermittelt werden. Ungeachtet der vorstehenden Ausführungen gelten die Standardvertragsklauseln nicht, wenn Genesys in Bezug auf die Kundendaten als Subauftragsverarbeiter (wie in den Standardvertragsklauseln definiert) tätig ist, oder wenn Genesys verbindliche interne Datenschutzvorschriften oder einen anderen anerkannten Compliance-Standard für die rechtmäßige Übermittlung personenbezogener Daten (wie in der geltenden Datenschutzgesetzgebung definiert) in Gebieten außerhalb des EWR festgelegt hat.

j. ***Löschung und Rückgabe von Kundendaten.*** Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Kunden, spätestens jedoch mit Beendigung des Rahmenvertrags hat Genesys sämtliche in den Besitz von Genesys gelangten Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Kunden stehen, auszuhändigen. Andernfalls werden die Datenlöschungsrichtlinien von Genesys auf diese Daten zur Anwendung gebracht. Für Services, die nach Beendigung des Rahmenvertrags erbracht werden, sind zusätzliche Gebühren zu bezahlen.

3. **VERANTWORTLICHKEITEN VON GENESYS**

a. ***DATENSCHUTZBEAUFTRAGTER.*** In Übereinstimmung mit der geltenden Datenschutzgesetzgebung hat Genesys einen Datenschutzbeauftragten bestellt. Der Datenschutzbeauftragte von Genesys ist Herr Shahzad Muhammad Naveed AHMAD, VP Cloud Competence Center & Datenschutz EMEA, Firmenrufnummer: +44 (0) 1753418818, Tel.Nr. mobil: +447717861224, E-Mail-Adresse: Shahzad.Ahmad@Genesys.com. Ein Wechsel des Datenschutzbeauftragten wird dem Kunden unverzüglich mitgeteilt.

b. ***Sicherheit.***

i. *Sicherheitsverfahren.* Genesys wird Sicherheitsverfahren einführen, die der geltenden Datenschutzgesetzgebung entsprechen. Die zu treffenden Maßnahmen bieten ein dem Risiko in Bezug auf die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme angemessenes Schutzniveau. Dabei hat Genesys den Stand der Technik, die Implementierungskosten und die Art, den Umfang und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt. Weitere Informationen sind den Anhängen zu entnehmen.

ii. *Technische und organisatorische Maßnahmen.* Genesys hat Maßnahmen zum Erhalt der Sicherheit der Anlagen und Netzwerke von Genesys umgesetzt, wie dies in den Anhängen festgelegt ist. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es Genesys gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

iii. *Überprüfung der Sicherheit von Genesys.* Der Kunde allein ist dafür verantwortlich, die von Genesys bereitgestellten Informationen zur Datensicherheit zu überprüfen und eine unabhängige Entscheidung darüber zu treffen, ob die Services den Anforderungen des Kunden entsprechen sowie sicherzustellen, dass das Personal und die Berater des Kunden die ihnen vorgegebenen Leitlinien zur Datensicherheit einhalten.

4. **Prüfung**

Prüfung. Genesys setzt mindesten einmal pro Jahr externe Prüfer zur Überprüfung der Sicherheitsmaßnahmen von Genesys ein. Diese Überprüfung wird von einer unabhängigen Stelle durchgeführt, die einen Bericht über ihre Prüfung („**Bericht**“) erstellt. Dieser Bericht wird von Genesys vertraulich behandelt. Unter der Bedingung, dass eine zwischen den Parteien vereinbarte Geheimhaltungsvereinbarung (*Non Disclosure Agreement* „**NDA**“) vorliegt, kann der Kunde Zugang zu den Berichten erhalten. Wird dies vom Kunden schriftlich verlangt, wird Genesys dem Kunden einen Bericht zur Verfügung stellen, damit der Kunde die Einhaltung der Sicherheitsverpflichtungen, die Genesys gemäß diesem DPS obliegen, angemessen überprüfen kann. Falls die Standardvertragsklauseln zur Anwendung kommen, erklärt sich der Kunde damit einverstanden, sein Recht auf Überprüfung auszuüben, indem er Genesys anweist, die Prüfung wie in diesem Abschnitt beschrieben durchzuführen. Hat der Kunde nicht auf die Standardvertragsklauseln verzichtet und möchte diese Anweisung bezüglich der Ausübung des Rechts auf Überprüfung ändern, so

kann er sie wie in den Standardvertragsklauseln festgelegt ändern, wobei das diesbezügliche Verlangen schriftlich geäußert werden muss. Wenn die Standardvertragsklauseln zur Anwendung kommen, ergibt sich aus keiner der Bestimmungen in diesem Abschnitt des DPS eine Änderung oder Abwandlung der Standardvertragsklauseln, und die nach den Standardvertragsklauseln bestehenden Rechte einer Aufsichtsbehörde oder betroffenen Person werden davon nicht berührt.

5. **MELDUNG VON SICHERHEITSVERLETZUNGEN**

Meldung. Genesys wird den Kunden bei der Einhaltung der Meldepflichten im Fall von Datenschutzverletzungen unterstützen. Hierzu gehören u.a.:

i. die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten so rasch wie möglich an den Kunden zu melden. Die Parteien sind sich der Tatsache bewusst, dass aufgrund der datenschutzrechtlichen Anforderungen jedenfalls eine Informationspflicht im Fall des Verlusts oder der rechtswidrigen Offenlegung personenbezogener Daten oder des Zugriffs auf solche Daten besteht. Daher sind solche Vorfälle dem Kunden so rasch wie möglich mitzuteilen. Genesys wird geeignete Maßnahmen ergreifen, um die Daten zu schützen und potenzielle nachteilige Auswirkungen auf die betroffenen Personen zu begrenzen. Hat der Kunde nach geltendem Recht Meldung an eine staatliche Behörde zu erstatten, ist Genesys verpflichtet, den Kunden bei der Erstellung einer solchen Meldung zu unterstützen.

ii. die Verpflichtung, den Kunden im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen, sofern dies nach geltender Datenschutzgesetzgebung erforderlich ist, und ihm in diesem Zusammenhang sämtliche relevante Informationen so rasch wie möglich zur Verfügung zu stellen.

6. **VERBUNDENE UNTERNEHMEN**

a. ***Verbundene Unternehmen.*** Genesys kann Daten an seine verbundenen Unternehmen übertragen und andere Unternehmen mit der Bereitstellung beschränkter Dienste im Namen von Genesys beauftragen, beispielsweise mit Erbringung von Hilfsdiensten für den Kundensupport. Solchen verbundenen Unternehmen und Subunternehmern ist es gestattet, Kundendaten ausschließlich für die Bereitstellung der Dienste zu beschaffen, mit deren Bereitstellung Genesys sie beauftragt hat, und es ist ihnen untersagt, Kundendaten für andere Zwecke zu nutzen. Genesys geht angemessene und rechtsverbindliche vertragliche Vereinbarungen ein und implementiert geeignete Kontrollmaßnahmen, um den Schutz und die Sicherheit der Daten des Kunden auch bei ausgelagerten Nebenleistungen zu gewährleisten.

b. ***Aktuelle Subunternhemer.*** PureCloud befindet sich in Rechenzentren von Drittanbietern, die von Amazon Web Services (AWS) bereitgestellt werden.

Außerdem werden bei unserem PureCloud-Angebot Drittanbieter zur Überwachung, Benachrichtigung und Protokollspeicherung eingesetzt. Alle Detailinformationen von Syslog, AppLog, CloudTrail und VPC Flow werden an SumoLogic gesendet. Für das Sicherheitsmonitoring werden Alert Logic und Threatstack eingesetzt, und New Relic für das Instanzen- und Applikationsmonitoring. OneLogin wird für die Bereiche Authentifizierung, Autorisierung und Abrechnung verwendet. Für Informationen zum Kundenkonto, Kontaktdetails der Kundenvertreter und Kundenservice-Tickets wird die Salesforce-Lösung (SFDC) eingesetzt. Für die Angebotserstellung und Fakturierung wird die Zuora-Lösung herangezogen. Außerdem werden folgende Anbieter für die Konnektivität von PureCloud Voice PSTN eingesetzt: Verizon, Bandwidth.com, iBasis, Voxbone, Intrado und Brightlink (nur relevant, wenn der Kunde Voice PSTN-Konnektivität bezieht).

Unterauftrags-verarbeiter	**Adresse/Land/Website**	**Leistung**
Amazon	AWS-Region Irland oder Deutschland (www.amazon.com)	PureCloud aufbauend auf AWS MicroServices
SumoLogic	https://www.sumologic.com	Protokollerfassungs-Tool
Alert Logic	https://www.alertlogic.com/	Sicherheit/Überwachung
Threatstack	https://www.threatstack.com	Sicherheit/Überwachung
New Relic	https://newrelic.com	Sicherheit/Überwachung
Onelogin	https://www.onelogin.com	Authentifizierung
Salesforce (SFDC)	https://www.salesforce.com	Kontoinformationen und Ticketing-System
Zuro	https://www.zuora.com	Angebote & Fakturierung

c. ***Änderungen bei Subunternehmern.*** Genesys wird den Kunden von allen beabsichtigten Änderungen informieren, die die Hinzuziehung weiterer Subunternehmer oder den Austausch von Subunternehmern betreffen und die Verarbeitung der Kundendaten wesentlich beeinflussen. Liegt seitens des Kunden eine angemessene Begründung vor, um solchen Änderungen zu widersprechen, so muss er seinen Einwand Genesys innerhalb von 10 Tagen nach Erhalt der Mitteilung von Genesys über die beabsichtigten Änderungen zur Kenntnis bringen. Nachdem der Kunde seinen Einwand vorgebracht hat, wird Genesys angemessene Anstrengungen unternehmen, um dem Kunden eine Änderung der betroffenen Services bereitzustellen oder dem Kunden empfehlen, wie er seine Konfiguration der Services wirtschaftlich sinnvoll ändern kann, um die vom Kunden vorgebrachten Bedenken auszuräumen. Wenn der Kunde auf seinem Einwand beharrt, kann er als einzigen und ausschließlichen Rechtsbehelf den Rahmenvertrag kündigen, jedoch unter der

Bedingung, dass er alle Gebühren und Kosten für die Restlaufzeit des Rahmenvertrags bezahlt.

7. **VERTRAULICHKEIT**

Vertrauliche Informationen. Der Kunde stimmt zu, dass es sich beim Inhalt dieses DPS um vertrauliche Informationen handelt.

8. **GESAMTE VEREINBARUNG; DISKREPANZEN**

Gesamte Vereinbarung; Diskrepanzen. Der Rahmenvertrag bleibt in vollem Umfang wirksam und gültig, sofern er nicht durch diesen DPS geändert wird. Im Fall von Unterschieden zwischen dem Rahmenvertrag und diesem DPS sind die Bestimmungen dieses DPS maßgeblich.

Anlagen:

- DPS Anlage 1: Standardvertragsklauseln (SVK)
- DPS Anhang 1: Beschreibung von Daten und Verarbeitung
- DPS Anhang 2: Sicherheitsmaßnahmen von Genesys

- DPS Anlage 1 – **Standardvertragsklauseln (SVK)**

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

Bezeichnung der Organisation (Datenexporteur): *[UNTERNEHMEN DES KUNDEN]*
Anschrift: *[ADRESSE DES KUNDEN]*
Tel.: _____; Fax: _____; E-Mail: _____
Weitere Angaben zur Identifizierung der Organisation:
……
(„**Datenexporteur**“)

und

Bezeichnung der Organisation (Datenimporteur): Genesys Telecommunications Laboratories B.V.
Anschrift: Gooimeer 6-02, 1411DD Naarden, Niederlande
Tel.: +31 35 625 7230, Fax: +31 35 678 2022; E-Mail: legal@genesys.com, DataPrivacy@genesys.com
……
(„**Datenimporteur**”)

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

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

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten“, „besondere Kategorien personenbezogener Daten“, „Verarbeitung“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“ und „Kontrollstelle“ entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1];

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

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

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

e) der Begriff „anwendbares Datenschutzrecht“ bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen“ sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

[1] Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

Klausel 2

Einzelheiten der Übermittlung

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

Klausel 3

Drittbegünstigtenklausel

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

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

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

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

Klausel 4

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den

zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

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

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

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

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

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

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

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

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

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs[2]

Der Datenimporteur erklärt sich bereit und garantiert, dass:

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

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

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

d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii) jeden zufälligen oder unberechtigten Zugang und

   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

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

---

[2] Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

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

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

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

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

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

Klausel 6

Haftung

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

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

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

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

Klausel 7

Schlichtungsverfahren und Gerichtsstand

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

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

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

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

Klausel 8

Zusammenarbeit mit Kontrollstellen

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

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

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In

diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: …

Klausel 10

Änderung des Vertrags

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

Klausel 11

Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss[3]. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

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

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

[3] Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

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

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

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

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

Für den Datenexporteur:
Name (ausgeschrieben):
Funktion:
Anschrift:
Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:
Unterschrift…….
(Stempel der Organisation)

Für den Datenimporteur:
Name (ausgeschrieben):
Funktion:
Anschrift:
Gegebenenfalls weitere Angaben, die den Vertrag verbindlich machen:
Unterschrift…….
(Stempel der Organisation)

DPS Anhang 1 zu den Standardvertragsklauseln
Beschreibung von Daten und Verarbeitung

1. **Datenexporteur:** Der Datenexporteur ist der Kunde.
2. **Datenimporteur:** Der Datenimporteur ist Genesys.
3. **Betroffene Personen**: Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen: Betroffene Personen sind die Vertreter und Endbenutzer des Datenexporteurs, darunter Mitarbeiter, Vertragspartner und Kunden des Datenexporteurs. Zu den betroffenen Personen können auch Personen gehören, die personenbezogene Daten an Nutzer der vom Datenimporteur bereitgestellten Dienste übermitteln oder Kontakt zu solchen Nutzern aufnehmen möchten.
4. **Kategorien von Daten**: Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien:Namen, Titel, E-Mails, Postadressen, Telefonnummern, Geo-Standorte, Daten zur Historie von Endkunden, Endkundenabrechnungs- und -fakturierungsdaten sowie andere Daten in elektronischer Form, die im Zusammenhang mit den Services erfasst werden.
5. **Verarbeitung**: Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:
    a. ***Dauer und Ziel der Datenverarbeitung.*** Die Dauer der Datenverarbeitung entspricht der vom Kunden spezifizierten Laufzeit. Das Ziel der Datenverarbeitung ist die Erbringung der Services.
    b. ***Umfang und Zweck der Datenverarbeitung***. Umfang und Zweck der Verarbeitung personenbezogener Daten sind im Rahmenvertrag beschrieben. Der Datenimporteur betreibt ein globales Netzwerk an Rechenzentren und Management-/Support-Einrichtungen, und die Datenverarbeitung kann unter der Rechtsordnung jedes Landes durchgeführt werden, in dem der Datenimporteur oder seine Unterauftragsverarbeiter solche Einrichtungen betreiben.
6. **Subunternehmer**: Der Datenimporteur ist berechtigt, andere Unternehmen mit der Bereitstellung beschränkter Dienste in seinem Namen zu beauftragen, beispielsweise mit der Bereitstellung von Kundensupport. Solchen Subunternehmern ist es gestattet, Kundendaten ausschließlich für die Bereitstellung der Dienste zu beschaffen, mit deren Bereitstellung der Datenimporteur sie beauftragt hat, und es ist ihnen untersagt, Kundendaten für andere Zwecke zu nutzen.

DATENEXPORTEUR
Name:
Unterschrift des/der Bevollmächtigten:

DATENIMPORTEUR
Name:
Unterschrift des/der Bevollmächtigten:

DPS Anhang 2 zu den Standardvertragsklauseln
Sicherheitsmaßnahmen von Genesys

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat (oder Dokument/Rechtsvorschrift beigefügt):

Dieser Anhang beschreibt die Mindestsicherheitsanforderungen für die Leistungserbringung an den Kunden durch den Auftragsverarbeiter. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragsverarbeiter in seiner Rolle als für den Kunden tätiger Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Auftragsverarbeiter wird daher jene angemessenen technischen und organisatorischen Maßnahmen sowie Sicherheitsmaßnahmen ergreifen, die erforderlich sind, um die personenbezogenen Daten des Kunden, die sich im Besitz des Auftragsverarbeiters befinden oder anderweitig vom Auftragsverarbeiter verarbeitet werden, vor unrechtmäßigem Zugang, unrechtmäßiger Änderung, Weitergabe oder Vernichtung zu schützen, wie in diesem Anhang näher beschrieben ist.

1. **Sicherheitsprogramm**
   Um die Kundendaten so zu schützen, wie es der Art und dem Umfang der bereitgestellten Services entspricht, haben wir ein Informationssicherheitsprogramm implementiert und setzen dieses ein. Dieses Programm folgt den allgemein anerkannten Systemsicherheitsprinzipien, die in der Norm ISO 27001 verankert sind. Das Informationssicherheitsprogramm wird vom PureCloud-Team Security & Compliance gepflegt und gewartet. Die Mitglieder des Teams sind erfahrene Fachleute, die eine breite Palette von Zertifizierungen in den Bereichen Sicherheit und Datenschutz vorweisen können. Das Informationssicherheitsprogramm beinhaltet zumindest folgende Elemente:

   a. **Sicherheitsbewusstsein und Schulung**
      Wir haben ein Informationssicherheits- und Sensibilisierungsprogramm implementiert und setzen dieses ein. Das Programm ist von Mitarbeitern bzw. Auftragnehmern (wo erforderlich) zum Zeitpunkt ihrer Einstellung/des Beginns ihres Vertragsverhältnisses und danach jährlich zu absolvieren. Das Programm zur Schulung des Sicherheitsbewusstseins wird elektronisch bereitgestellt und beinhaltet eine Testkomponente mit Mindestanforderungen, die erfüllt werden müssen, um das Programm erfolgreich zu absolvieren. Außerdem erhalten Mitarbeiter im Entwicklungsbereich Schulungen zur Entwicklung von sicheren Codes.

   b. **Richtlinien und Verfahren**
      Wir setzen Richtlinien und Verfahren ein, um das Informationssicherheitsprogramm zu unterstützen. Die Richtlinien und Verfahren werden jährlich überprüft und bei Bedarf aktualisiert.

c. **Änderungsmanagement**
Wir setzen einen auf Branchenstandards basierenden Änderungsmanagementprozess ein, um sicherzustellen, dass alle Änderungen in der PureCloud-Produktionsumgebung angemessen überprüft, getestet und genehmigt werden.

d. ***Patching***
PureCloud patcht nicht. Die Strategie besteht darin, alle Serverinstanzen mindestens alle 30 Tage zu vernichten und auf neuen „Gold Images" mit aktuellen *Patch*-Levels neu aufzusetzen. Die „Gold Images" werden mindestens alle zwei Wochen mit aktuellen Sicherheits*patches* aktualisiert.

e. **Datenspeicherung und Backup**
Wir erstellen auf der Grundlage dokumentierter Sicherungsverfahren Backups von kritischen Kundendaten. Es werden keine Backup-Daten auf portablen Medien gespeichert. Auf Backup-Medien gespeicherte Kundendaten werden mit serverseitiger Verschlüsselung, in der von Amazon Web Services („**AWS**") bereitgestellten Form, verschlüsselt.

f. **Überprüfung auf Schwachstellen und Penetrations-Tests**
Wir führen regelmäßig interne Überprüfungen auf etwaige Schwachstellen mit automatisierten Scans und Benachrichtigungen durch. Die Prüfergebnisse werden analysiert, um etwaige identifizierte Schwachstellen zu bestätigen. Die Behebung festgestellter Schwachstellen findet in einem Zeitrahmen statt, der dem mit der Schwachstelle verbundenen Risiko entspricht.

Mindestens einmal jährlich engagieren wir einen unabhängigen qualifizierten Anbieter, der eine Schwachstellenbewertung und Penetrations-Tests durchführt. Im Zuge der Tätigkeit dieses unabhängigen Anbieters identifizierte Problembereiche werden innerhalb eines angemessenen Zeitrahmens einer sachgerechten Lösung zugeführt, die dem mit dem Problem verbundenen Risikograd entspricht. Eine Kurzfassung der Resultate oder die vollständigen Testergebnisse können dem Kunden auf entsprechende schriftliche Anfrage übermittelt werden, wobei diesbezüglich Vertraulichkeits- und Geheimhaltungsvereinbarungen zur Anwendung kommen.

g. **Malware-Prävention**
Die in PureCloud ausgeführten Anwendungen wurden unter Einsatz branchenüblicher sicherer Codierungsverfahren entwickelt und werden unter Verwendung dieser Verfahren ausgeführt. Dazu zählen unter anderem Verfahren wie *Peer-Coding-Review*, Sicherheits- und Komponententests sowie Einhaltung sicherer Codierungstechniken. Wir setzen branchenübliche Praktiken ein, um zu verhindern, dass Programme, Routinen, Unterroutinen oder Daten (darunter auch Schadsoftware bzw. „Malware", Viren, Würmer und Trojaner) in Anwendungen, die innerhalb von PureCloud zum Einsatz kommen, eindringen können.

2. **Netzwerksicherheit**
   Von AWS wird in den Bereichen Sicherheit und Compliance eine solide Grundlage bereitgestellt, die wir durch branchenübliche Netzwerksicherheitskontrollen zum Schutz von Kundendaten ergänzen. Dazu zählen unter anderem:

   a. **Angriffserkennungssysteme**: Wir haben ein hostbasiertes Angriffserkennungssystem und ein netzwerkbasiertes Angriffserkennungssystem implementiert und setzen diese Systeme ein. Ihre Aufgabe besteht darin, uns bei verdächtigen Aktivitäten zu warnen.

   b. **Datenverbindungen:** Wir verwenden HTTPS/TLS mit AES-256-Verschlüsselung, um Verbindungen zwischen Browsern, mobilen Apps und anderen Komponenten zu PureCloud zu sichern.

   c. **Datenverbindungen zwischen PureCloud und Dritten**: Die Übermittlung von Kundendaten an Sie bzw. an Dritte, die Sie zum Erhalt von Kundendaten autorisiert haben, sowie der Austausch von Kundendaten mit Ihnen bzw. mit solchen Dritten, erfolgt unter Einsatz sicherer Methoden (z.B. TLS, HTTPS, SFTP).

   d. **Verschlüsselte Aufzeichnungen**: Wir verschlüsseln standardmäßig alle Aufzeichnungen. PureCloud generiert kundenspezifische Verschlüsselungscodes, die zur Sicherung von Anrufaufzeichnungen verwendet werden. Chat-Sitzungen werden im Zuge der Übertragung verschlüsselt.

   e. **Verschlüsselungsschutz**: Zur Unterstützung der Verschlüsselung setzen wir branchenübliche Methoden ein. Wir verwenden ein Mindestlevel von RSA 2048 bit für die Verschlüsselung mit asymmetrischen Schlüsseln. Für die Verschlüsselung mit symmetrischen Schlüsseln verwenden wir AES 128 bit. Beim Hashing setzen wir SHA1 und SHA2 ein.

3. **Benutzerzugriffskontrolle**
   Angemessene Zugriffskontrollen und das Prinzip der geringsten Rechte wurden von uns implementiert und werden eingesetzt, um sicherzustellen, dass innerhalb von PureCloud ausschließlich autorisierte Benutzer Zugriff auf Kundendaten haben. Der Benutzerzugriff wird zu Prüfungszwecken protokolliert.

   a. **Zugriff durch Benutzer des Kunden**
      Die Verwaltung der Benutzerzugriffskontrollen innerhalb der Anwendung liegt in der Verantwortung der Kunden. Der Kunde definiert die Benutzernamen, Rollen und Kennwortmerkmale (Länge, Komplexität und Geltungsdauer) für seine Benutzer. Wird es vom Kunden, von Vertretern, Auftragnehmern oder Mitarbeitern (einschließlich, ohne Einschränkung, sämtlichen Benutzern des Kunden) verabsäumt, die Sicherheit aller Benutzernamen, Passwörter und sonstigen Kontoinformationen, die unter der Kontrolle des Kunden stehen, zu gewährleisten, dann trägt der Kunde dafür die alleinige Verantwortung. Mit Ausnahme einer Sicherheitslücke, die durch grobe Fahrlässigkeit oder

vorsätzliche Handlung bzw. Unterlassung unsererseits verursacht wurde, trägt der Kunde die alleinige Verantwortung – gleich ob er von Ihnen autorisiert wurde oder nicht – für jede Nutzung von PureCloud über Benutzernamen und Passwörter des Kunden, und für alle aus einer solchen Nutzung resultierenden Kosten. Sie haben uns unverzüglich zu benachrichtigen, wenn Sie Kenntnis von einer unautorisierten Verwendung der PureCloud-Produktionsumgebung erhalten.

b. **Zugriff durch unsere Benutzer**
Wir werden individuelle Benutzerkonten für jeden unserer Mitarbeiter oder Auftragnehmer erstellen, die aufgrund geschäftlicher Notwendigkeiten auf die PureCloud-Produktionsumgebung zugreifen müssen. Bei unserer Benutzerkontenverwaltung halten wir folgende Richtlinien ein:
   i. Benutzerkonten werden von unserer Geschäftsleitung angefordert und autorisiert.
   ii. Bei Benutzerkonten gilt das Prinzip der geringsten Rechte.
   iii. Für den Zugriff zur PureCloud-Produktionsumgebung ist eine Multifaktor-Authentifizierung erforderlich.
   iv. Innerhalb von PureCloud werden SSH-Schlüssel anstatt von Passwörtern verwendet.
   v. Inaktive oder nicht genutzte Konten werden nach 90 Tagen Nichtbenutzung deaktiviert.
   vi. *Session-Timeouts* werden systematisch durchgesetzt.
   vii. Benutzerkonten werden bei Kündigung oder Wechsel in eine andere Funktion von Mitarbeitern umgehend deaktiviert, so dass ein Zugriffsbedarf aufgrund geschäftlicher Notwendigkeiten ausgeschlossen wird.

4. **Geschäftskontinuität und *Disaster Recovery***
PureCloud wird in einer redundanten Infrastruktur über AWS bereitgestellt und konfiguriert. Die von PureCloud bereitgestellten Services folgen einer zustandslosen Architektur. Datenspeicher in PureCloud setzen Redundanz- und Replikationsverfahren ein, um die Datenverfügbarkeit zu gewährleisten und bei Ausfall eines Datenknotens Datenverluste zu vermeiden. Die PureCloud-Umgebung ist physisch von der Netzwerkumgebung unseres Unternehmens getrennt, sodass ein die Unternehmensumgebung betreffender Störvorfall die Verfügbarkeit der PureCloud Services nicht beeinträchtigt.

a. **Geschäftskontinuität**
Wir werden einen Geschäftskontinuitätsplan auf Unternehmensebene umsetzen, der sicherstellen soll, dass die laufenden Überwachungs- und Supportdienste im Fall einer Störung, die den Unternehmensbereich betrifft, weiterhin erfolgen.

b. **Hohe Verfügbarkeit**
PureCloud setzt die Dienste von AWS ein, um hochverfügbare Umgebungen realisieren zu können. Dazu zählen unter anderem:

i. Verfügbarkeitszonen (*Availability Zones, AZs*), die aus einem oder mehreren isolierten Rechenzentren mit jeweils redundanter Stromversorgung, Vernetzung und Konnektivität bestehen und in unterschiedlichen Standorten untergebracht sind;
ii. Automatische Skalierungsgruppen (*Auto Scaling Groups, ASGs*), um Cluster je nach Bedarf dynamisch zu skalieren und bei einem Ausfall automatisch Ersatzinstanzen zu starten;
iii. AWS Elastische Lastenausgleichsmodule (*Elastic Load Balancers, ELBs*), um den internen und externen Datenverkehr auf eine fehlerfreie Infrastruktur zu verteilen und den Datenverkehr automatisch von der fehlerhaften Infrastruktur wegzuleiten;
iv. Stabile Message-Queuing-Systeme, die Anforderungswarteschlangen und Punkt-zu-Multipunkt-Benachrichtigungen unterstützen. Nachrichtenwarteschlangen ermöglichen es uns, einen Lastenausgleich für Anfragen/Vorfälle durchzuführen und Lastenspitzen ohne Datenverlust zu bewältigen.
v. Amazon Simple Storage Service ("**Amazon S3**"). Amazon S3 speichert Objekte redundant auf mehreren Geräten an mehreren Standorten in einer Amazon S3 Region. Amazon S3 ist auf eine 99,999999999-prozentige Haltbarkeit (11/9) ausgelegt.

5. **<u>Reaktion auf sicherheitsrelevante Vorfälle</u>**
Wir setzen ein auf Branchenstandards basierendes *Security-Incident-Response* Programm ein, um vermutete und tatsächliche sicherheitsrelevante Vorfälle, die Kundendaten betreffen, zu identifizieren und darauf zu reagieren. Das Programm wird mindestens einmal jährlich überprüft, getestet und ggf. aktualisiert. Ein „**sicherheitsrelevanter Vorfall**“ (*Security Incident*) ist ein bestätigtes Ereignis, das einen unautorisierten Zugriff auf oder eine unautorisierte Verwendung, Löschung, Änderung, Weitergabe von Kundendaten zur Folge hat.

a. **Meldungen**
Im Fall eines bestätigten sicherheitsrelevanten Vorfalls, der die unautorisierte Freigabe oder Bekanntmachung von Kundendaten oder einen anderen Sicherheitsvorfall betrifft, für den nach geltendem Recht eine Meldung erfolgen muss, erfolgt innerhalb von sechsunddreißig (36) Stunden eine Kundenverständigung durch uns, und wir werden in angemessenem Umfang kooperieren, damit der Kunde die erforderlichen Meldungen im Zusammenhang mit einem solchen Vorfall vornehmen kann, es sei denn, uns wird von Exekutivorganen oder durch gerichtliche Anordnung ausdrücklich aufgetragen, dies nicht zu tun.

b. **Einzelheiten einer Meldung**
Wir werden dem Kunden im Zusammenhang mit einem bestätigten sicherheitsrelevanten Vorfall folgende Einzelheiten zur Verfügung stellen: (i) Datum, an dem der sicherheitsrelevante Vorfall identifiziert und bestätigt wurde; (ii) Art und Auswirkungen des sicherheitsrelevanten Vorfalls; (iii) bereits von uns ergriffene Maßnahmen; (iv) zu ergreifende Abhilfemaßnahmen; und (v) Bewertung von Alternativen und weiteren Schritten.

c. **Laufende Kommunikation**
Wir werden den Kunden weiterhin sachdienliche Statusberichte zur Behebung des sicherheitsrelevanten Vorfalls zur Verfügung stellen und in gutem Glauben laufend daran arbeiten, den sicherheitsrelevanten Vorfall zu bereinigen und künftige sicherheitsrelevante Vorfälle zu verhindern. Wir werden, soweit Sie dies in angemessenem Rahmen verlangen, mit Ihnen kooperieren, um den sicherheitsrelevanten Vorfall weiter zu untersuchen und einer Lösung zuzuführen.

6. **Datenschutz**

Wir haben ein zur Absicherung und zum Schutz der unter unserer Kontrolle befindlichen Kundendaten dienendes Datenschutzprogramm entwickelt, das von uns eingesetzt wird. Dieses Programm ist unter https://help.mypurecloud.com/articles/purecloud-privacy-policy/ abrufbar. In keinem Fall werden wir Kundendaten vermieten, verkaufen oder in sonstiger Weise außenstehenden Parteien überlassen. Die Verwendung von und der Zugriff auf Kundendaten erfolgt ausschließlich zum Zweck der Bereitstellung von PureCloud Services.