VERTRAG ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 9 DSG UND ART. 28 DSGVO FÜR PASCOM ONE (NACHFOLGEND VERTRAG ODER AVV)

VEREINBARUNG

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt –

und der

pascom Switzerland GmbH, Landis+Gyr-Strasse 1, 6300 Zug
(hiernach „pascom“)

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -
Der Auftragnehmer und der Auftraggeber zusammen auch die „Parteien“ genannt.

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Die Beauftragung des Auftragnehmers umfasst die Bereitstellung und den Betrieb von pascom ONE als Software as a Service (SaaS) („Hauptvertrag“). pascom ONE ist eine Voice-over-IP Telefonanlage aus der Cloud. Diese enthält einen Telekommunikationsdienst in das öffentliche Telefonnetz. Die Bereitstellung der Lösung erfolgt als Software as a Service über das Internet auf Basis von Nutzer-Abonnementen (User-Subscription). Es werden u. a. folgende Dienste zur Verfügung gestellt:

Unified Communication, Funktionen wie Desktop-, Mobile- und Web-Clients für Telefonie, Videokonferenzen, Screensharing, Gruppenchat, Fax- & Dateitransfer, Einzelplatz- und Multiline-TAPI, Contact Center, IVR & Analytics, Schnittstellen/Konnektoren und KI gestützte Transkriptionsdienste.

Neben der Bereitstellung des SaaS umfasst die Beauftragung auch die Administration und den Support des pascom ONE Dienstes.

Für die Anbindung an das Telefonnetz kommt der Dienst „Nummer-Hosting“ der Firma Colt Technology Services AG, Bahnhofplatz 1, 8001 Zürich („Colt“) zum Einsatz. Colt agiert als verantwortliche Stelle bei der zur Verfügungstellung des Telefonie-Dienstes im Sinne des Fernmeldegesetzes (FMG, SR 784.10) und weiterer anwendbarer fernmelderechtlicher Vorschriften, inkl. der Abrechnung von Verbindungsgebühren, die von einem mit Colt verbundenen Unternehmen mit Sitz in Indien vorgenommen werden. Als Rechtsgrundlage für die Verarbeitung durch die indische Colt-Gesellschaft dienen hier Binding Corporate Rules (BCR) und die Standardvertragsklauseln für die Weitergabe von Personendaten in Drittländer gemäss der Entscheidung 2004/915/EG der Europäischen Kommission vom 27. Dezember 2004, wie durch die Entscheidung 2021/679/EG der Kommission vom 4. Juni 2021 geändert, in ihrer jeweils gültigen Fassung, sowie den Anerkennungsbeschluss des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vom 27. August 2021 über die

revidierten EU-Standardvertragsklauseln für eine Datenübermittlung in Länder ohne ein angemessenes Datenschutzniveau („EU-Standardvertragsklauseln“). Datenschutzrechtlich ist Colt Unterauftragsnehmer der pascom.

Auf die datenschutzrechtlichen Bestimmungen des vorliegenden Auftrags-verarbeitungsvertrages finden Schweizer Datenschutzrecht (insbesondere das Bundesgesetz über den Datenschutz (DSG, SR 235.1) sowie die dazugehörige Verordnung) sowie, wenn ein Verbindungspartner oder der Nutzer sich in der EU befindet, die Regelungen der europäischen Datenschutzgrundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) (DSGVO) Anwendung. Aus sprachlichen Vereinfachungsgründen wird in diesem Vertrag die Terminologie der DSGVO verwendet.

Der vorliegende Vertrag und die dazugehörige(n) Anlage(n) geben die Daten-schutzverpflichtungen der Parteien und ihrer Tochtergesellschaften im Zusammenhang mit der Verarbeitung von Personendaten im Rahmen des Hauptvertrages (inkl. sämtlicher Bestandteile) vor. Der Auftragnehmer erhält unter Umständen Zugang zu Personendaten des Auftraggebers oder verarbeiten unter Umständen Personendaten des Auftraggebers oder erlangen oder erfassen unter Umständen Personendaten von oder für den Auftraggeber („Personendaten des Auftraggebers“ oder „personenbezogene Daten des Auftraggebers“), wobei Personendaten des Auftraggebers unter anderem Personendaten der Vertreter, Nutzer, Verbindungspartner, Kunden und/oder Auftragsverarbeiter des Auftraggebers einschliessen.

Der Auftragnehmer und/oder seine Tochtergesellschaften werden lediglich solche Personendaten des Auftraggebers nutzen, verarbeiten oder Zugang haben, die durch den Auftraggeber übertragen wurden oder Gegenstand einer durch den Auftraggeber ausdrücklich erteilten Nutzungs- oder Zugangsgenehmigung sind. Der Auftragnehmer und/oder seine Tochtergesellschaften werden keine Personendaten des Auftraggebers zu irgendwelchen anderen Zwecken als zur Erfüllung ihrer in diesem Vertrag festgehaltenen oder gesetzlichen Verpflichtungen nutzen.

Der Auftraggeber bleibt der ausschliessliche Verantwortliche für die betreffenden Personendaten des Auftraggebers.

1.2 Dauer

Die Dauer dieses AVV entspricht der Vertragslaufzeit des Hauptvertrages (seitens des Auftraggebers bestellten pascom ONE Abonnements).

2 Konkretisierung des Auftragsinhalts

2.1 Rechtmässige Verarbeitung

Der Auftraggeber erklärt und garantiert, dass die dem Auftragnehmer zur Verfügung gestellten Personendaten auf rechtmässige Weise bearbeitet wurden (z.B. rechtmässige Erhebung, Einhaltung der Auskunftspflicht) und durch ihn sowie den Auftragnehmer verarbeitet werden dürfen, mit - wo notwendig - entsprechendem Rechtfertigungsgrund. Der Auftragnehmer ist berechtigt, über die Dokumentation der rechtmässigen Datenverarbeitung einen Beleg zu verlangen.

Unbeschadet des Vorstehenden haftet der Auftragnehmer nicht für Verstösse seitens des Auftraggebers gegen die Gesetze und Vorschriften zum Datenschutz betreffend unrechtmässiger Verarbeitung.

Sofern dies nicht bereits im Hauptvertrag und/oder einer anderen Vereinbarung festgehalten ist, ist der Auftraggeber verpflichtet, den Auftragnehmer über die Kategorien der Personendaten und die Datenempfänger zu informieren, die über die Informationen in Ziffer 2.2 bis 2.4 hinausgehen. Der Auftraggeber nimmt zur Kenntnis, dass spezielle Kategorien von Personendaten (wie besonders schützenswerte Personendaten) und Profile, höhere Sicherheitsmassnahmen erfordern, was unter Umständen Kostenfolgen nach sich ziehen kann.

2.2 Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragnehmer erklärt und garantiert, dass die Verarbeitung ausschliesslich zu den im Hauptvertrag festgehaltenen Zwecken durchgeführt wird, es sei denn, der Auftragnehmer kann die Verarbeitung auf andere Rechtsfertigungsgründe abstützen. Zu keiner Zeit bearbeitet der Auftragnehmer irgendwelche Personendaten anderweitig und keine Personendaten werden länger aufbewahrt, als es für die Erfüllung des Hauptvertrags notwendig ist, oder zur Erfüllung eines gesetzlichen Zweckes oder anderweitigen Rechtfertigungsgrundes. Die Parteien halten im Hauptvertrag und/oder in diesem Vertrag den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Arten der Personendaten und die Kategorien der betroffenen Personen fest.

Die nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers ergeben sich aus den beauftragten Leistungen innerhalb des Hauptvertrages (pascom Lizenz). Das Hosting der personenbezogenen Daten findet ausschliesslich innerhalb der EU/EWR statt.

2.3 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Name, Vorname der Benutzer
- Vertragsstammdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Nutzungs- und Verhaltensdaten (Metadaten)
- Sprach- und Videoaufzeichnungen, gegebenenfalls Transkripte
- Dokumente

2.4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
Kunden, Interessenten, Beschäftigte, Lieferanten, Geschäftspartner und Bewerber des Auftraggebers.

2.5 Ort der Verarbeitung von Personendaten

Die Daten werden in der Schweiz und in Deutschland verarbeitet.

2.6 Relevante Weitergabe

Eine relevante Weitergabe der Daten an Dritte (ausgenommen Verrechnung durch Colt) erfolgt nicht.

3 Technisch-organisatorische Massnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Massnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Die aktuellen und dem Stand der Technik entsprechenden technischen und organisatorischen Massnahmen sind zu finden unter:

„Anlage 1“ auf Seite 14

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 8 DSG in Verbindung mit Art. 6 DSG bzw. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO sicherzustellen.

3.3 Der Auftragnehmer ist in jedem Fall verpflichtet, im Hinblick auf jedwede Verarbeitung und/oder relevante Weitergabe angemessene Sicherheitsvorkehrungen zu implementieren und umzusetzen und zu gewährleisten, dass seine verbundenen Unternehmen und/oder Subunternehmer die Verarbeitungen und/oder relevante Weitergaben für den Auftragnehmer vornehmen, ebenfalls derartige angemessene Sicherheitsvorkehrungen implementieren und umsetzen. Dazu gehören auch der Abschluss von EU-Standardvertragsklauseln im Namen und im Auftrag des Auftraggebers. Insgesamt handelt es sich bei den zu treffenden Massnahmen um Massnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 8 DSG bzw. Art. 32 Abs. 1 DSGVO zu berücksichtigen.

3.4 Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3.5 Die Parteien sind verpflichtet, einander bei einem Verdacht auf Verstösse gegen die Gesetze und Vorschriften zum Datenschutz und insbesondere bei Datenverlust bei der Verarbeitung von Personendaten umgehend zu informieren. Für die Meldung verwenden die Parteien Anlage 2.

4 Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers bzw. der Vertragsparteien

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten, insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich im Rahmen der getroffenen Vereinbarungen nur nach dokumentierten Weisungen des Auftraggebers, insbesondere in Zusammenhang mit einer relevanten Weitergabe von Personendaten, sofern er nicht zu einer anderen Verarbeitung gemäss geltenden Gesetzen oder Vorschriften, denen der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

b) Sofern gesetzlich vorgeschrieben, die schriftliche Benennung eines Datenschutzbeauftragten bzw. -beraters, der seine Tätigkeit gesetzeskonform ausübt.

c) Die Wahrung der Vertraulichkeit. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschliesslich entsprechend der Weisung des Auftraggebers verarbeiten, einschliesslich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) Die Umsetzung und Einhaltung für diesen Auftrag erforderlichen technischen und organisatorischen Massnahmen (Ziffer 3).

e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde und in gegenseitiger Rücksprache bei der Erfüllung ihrer Aufgaben zusammen.

f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Massnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Verwaltungs- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Verwaltungs- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen. Der Auftragnehmer kontrolliert regelmässig die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Massnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

i) Beide Parteien verpflichten sich, alle im Zusammenhang mit dem Hauptvertrag erlangten Informationen nicht-öffentlicher Art vertraulich und im Einklang mit den geltenden Vertraulichkeitspflichten zu behandeln. Diese Regel gilt insbesondere in Bezug auf (i) alle vertraulichen Informationen, die Personendaten sowie Personendaten des Auftraggebers betreffen und (ii) alle vertraulichen Informationen nicht-öffentlicher Art über das Geschäft des Auftraggebers, wie beispielsweise die Organisation, die betrieblichen und technischen Abläufe, die Infrastruktur und die Systeme, die Produkte und Dienstleistungen des Auftraggebers oder Informationen über vertragliche Beziehungen zu Drittparteien (Fertigungs- und Geschäftsgeheimnisse). Keine Partei darf Personendaten weitergeben oder offenlegen, ausser: (i) wenn dies im Hinblick auf die Erbringung der Dienstleistungen gemäss dem Hauptvertrag notwendig ist; oder (ii) mit schriftlicher Genehmigung der anderen Partei; oder (iii) bei der Hinzuziehung eines Subunternehmers im Einklang mit Ziffer 6 diesem Vertrag; oder (iv) wenn dies nach verbindlichen gesetzlichen Bestimmungen erforderlich oder zulässig ist, wobei die offenlegende Partei in diesem Fall verpflichtet ist, die andere Partei in Kenntnis zu setzen.

6 Unterauftragsverhältnisse (Subunternehmer)

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungs-anlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmassnahmen zu ergreifen.

6.2 Der Auftraggeber erteilt hiermit die generelle Genehmigung, dass der Auftragnehmer Subunternehmer mit der Verarbeitung beauftragen kann und stimmt mit Unterzeichnung dieses Vertrages der Beauftragung der unter https://www.pascom.net/ch/datenschutz/ ersichtlichen Subunternehmer zu.

6.3 Die Auslagerung auf weitere Subunternehmer oder der Wechsel des bestehenden Subunternehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Subunternehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht innerhalb von 14 Tagen gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Massgabe des Art. 9 DSG bzw. Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

6.4 Eine Beauftragung von Subunternehmern aus Drittstaaten ohne gleichwertiges Datenschutzniveau darf nur erfolgen, sofern die Personendaten bzw. sonstigen Daten des Auftraggebers nicht einem Berufs- oder Amtsgeheimnis unterstehen oder sonstige vertragliche Geheimhaltungspflichten dies explizit ausschliessen. In allen anderen Fällen ist beim Beizug eines Subunternehmers sicherzustellen, dass ein adäquates Datenschutzniveau im Sinne der Schweiz bzw. der EU besteht (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

6.5 Der Auftragsverarbeiter stellt sicher, dass kein Subunternehmer Personendaten in Verletzung der

Bestimmungen dieses Vertrages sowie der Gesetze und Vorschriften zum Datenschutz oder anderer geltender Gesetze verarbeitet und dass jeder Subunternehmer mindestens angemessene Sicherheitsvorkehrungen, wie die in Anlage 1 festgehaltenen technischen und organisatorische Massnahmen, implementiert.

6.6 Der Auftragnehmer hat weiter vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

7 Kontrollrechte des Auftraggebers, Unterstützungspflicht des Auftragnehmers

7.1 Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die notwendig sind, um die Einhaltung der in diesem Vertrag und/oder im Hauptvertrag festgehaltenen Verpflichtungen zu belegen. Der Auftraggeber hat überdies das Recht, Überprüfungen, einschliesslich Audits und Inspektionen, beim Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer nach vorheriger Terminabsprache durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer informiert den Auftraggeber, falls eine Anweisung nach seinem Dafürhalten, und wo erkennbar, gegen geltende Gesetze und Vorschriften zum Datenschutz verstösst.

7.2 Der Auftragnehmer ist verpflichtet, bei allen derartigen Inspektionen und Prüfungen umfassend zu kooperieren und die wesentlichen daraus resultierenden Empfehlungen innerhalb eines angemessenen Zeitrahmens zu prüfen und, sofern angezeigt, auf Kosten des Auftraggebers innerhalb eines angemessenen Zeitrahmens umzusetzen. Der Auftragnehmer stellt zudem sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 9 DSG bzw. Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Massnahmen nachzuweisen.

7.3 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

7.4 Der Auftraggeber sieht von jeglicher Handlung ab, die den Auftragnehmer an der Erfüllung seiner vertraglichen oder gesetzlichen Pflichten hindern würde, einschliesslich im Zusammenhang mit Subunternehmern oder der Zusammenarbeit mit den zuständigen Aufsichtsbehörden.

7.5 Der Auftraggeber unterstützt den Auftragnehmer beim Nachweis und bei der Dokumentation der ihm gesetzlich obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemässer Datenverarbeitung einschliesslich der Umsetzung der notwendigen technischen und organisatorischen Massnahmen.

8 Mitteilung bei Verstössen des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 6, Art. 8, Art. 22 - 24 sowie Art. 25 – 29 DSG bzw. Art. 5 und Art. 6, Art. 12 – 23 und Art. 32 bis 36 der DSGVO genannten Pflichten zu Grundsätzen der Datenbearbeitung, Sicherheit personenbezogener Daten, Rechte der betroffenen Personen, Meldepflichten bei Verletzung der Datensicherheit, Datenschutz-Folgeabschätzungen und vorherige Konsultationen mit den Aufsichtsbehörden. Hierzu gehören u.a.:

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Massnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen der Datensicherheit unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber den Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

9 Weisungsbefugnis des Auftraggebers

9.1 Der Auftraggeber kann dem Auftragnehmer Weisungen in Bezug auf die Datenverarbeitung erteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich (mind. Textform). Die Weisungen des Auftraggebers dürfen nicht gegen die einschlägigen Datenschutzvorschriften verstossen.

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich unter Einhaltung seiner Sorgfaltspflichten zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften oder gesetzliche Vorgaben. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9.3 Verstossen Weisungen des Auftraggebers gegen gesetzliche oder vertragliche Vorschriften, insbesondere gegen Gesetze und Vorschriften zum Datenschutz, so ist der Auftragnehmer berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Wird die gesetzes- oder vertragsverletzende Anweisung nicht innert angemessener Frist geändert, so hat der Auftragnehmer das Recht, den Hauptvertrag vollständig oder teilweise zu kündigen.

10 Löschung und Rückgabe von Personendaten

10.1 Kopien oder Duplikate von Personendaten dürfen ohne Wissen des Auftraggebers nicht erstellt werden.

Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Vorbehalten bleiben gesetzliche Aufbewahrungspflichten gemäss nachfolgender Ziff. 10.3.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemässen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen gesetzlichen Aufbewahrungsfristen (in der Regel 10 Jahre) über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

10.4 Der Auftragnehmer ist verpflichtet, den Auftraggeber umgehend zu informieren, falls der Auftragnehmer vernünftigerweise davon ausgehen muss, dass in Bezug auf Personendaten des Auftraggebers, die sich in Besitz oder unter der Kontrolle des Auftragnehmers befinden, eine Beschlagnahme oder Einziehung droht (beispielsweise im Rahmen eines Insolvenz- oder Vergleichsverfahrens oder aufgrund von Schritten seitens einer Drittpartei). Der Auftragnehmer muss in einem solchen Fall alle geeigneten Massnahmen ergreifen, um die Rechte und die Rechtsposition des Auftraggebers zu schützen. Insbesondere muss er alle beteiligten Instanzen und Personen davon in Kenntnis setzen, dass die Verfügungsgewalt über die Personendaten beim Auftraggeber liegt.

11 Haftung

11.1 Die Haftung richtet sich nach dem Hauptvertrag. Im Übrigen gilt:

Jede Partei stellt die andere Partei auf erstes Anfordern von und gegen alle Ansprüche Dritter (einschliesslich der betroffenen Personen) bezüglich eines Verstosses gegen diesen Vertrag, die Gesetze und Vorschriften zum Datenschutz oder gegen datenschutzrelevante Bestimmungen des Hauptvertrages frei, unabhängig davon, ob dieser Verstoss von der haftbaren Partei oder einem ihrer Vertreter, Lieferanten oder Verkäufer begangen wurde, sofern der Verstoss von der haftbaren Partei rechtlich zu vertreten ist. Die Freistellungsverpflichtung der haftenden Partei umfasst uneingeschränkt alle Schadensersatzansprüche Dritter, einschliesslich der Kosten und Aufwendungen, die der empfangenden Partei im Zusammenhang mit der Verletzung oder der Abwehr von Ansprüchen Dritter entstehen.

11.2 Sofern die DSGVO zur Anwendung gelangt, haften die Parteien gesamtschuldnerisch gegenüber den betroffenen Personen im Sinne von Art. 82 Abs. 4 DSGVO. Die Haftungsbestimmungen gemäss der DSGVO (Art. 82 Abs. 4 DSGVO) sind nicht anwendbar. Etwaige Haftungsbeschränkungen zwischen dem Auftraggeber und den betroffenen Personen gelten auch zugunsten des Auftragnehmers.

12 Sonstiges

12.1 Vereinbarungen zu den technischen und organisatorischen Massnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschliessend noch für drei volle Kalenderjahre aufzubewahren. Vorbehalten bleiben gesetzliche Aufbewahrungsplichten.

12.2 Änderungen und Ergänzungen in Bezug auf diesen Vertrag und all seine Bestandteile, einschliesslich jeglicher Zusicherungen durch den Auftragnehmer, erfordern Schriftlichkeit und eine ausdrückliche Erklärung dahingehend, dass es sich dabei um eine Änderung oder Ergänzung in Bezug auf die vorliegenden Bedingungen handelt. Dasselbe gilt auch im Hinblick auf einen Verzicht auf diese formelle Anforderung. Mündliche Nebenabreden bestehen nicht. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

12.3 Sollten einzelne Teile dieses Vertrages ganz oder teilweise unwirksam sein oder werden oder sollte sich eine Lücke herausstellen, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht. Anstelle einer unwirksamen Bestimmung oder zur Ausfüllung einer Regelungslücke soll eine angemessene Regelung gelten, die, soweit möglich, dem am nächsten kommt, was die Parteien gewollt haben würden, sofern sie diesen Punkt bedacht hätten.

12.4 Dieser Vertrag ist auf der Grundlage des materiellen schweizerischen Rechts auszulegen, unter Ausschluss der Regeln des Internationalen Privatrechts und anderer multi- oder bilateraler internationaler Kollisionsnormen. Ausschliesslicher Gerichtsstand ist Zug.

13 Definitionen

Für diesen Vertrag gelten folgende Definitionen:

“**Angemessene Sicherheitsvorkehrungen**” umfasst geeignete Massnahmen für die Bearbeitung von Personendaten gemäss den Gesetzen und Vorschriften zum Datenschutz, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; sie werden in Anlage 1 konkretisiert.

“**Auftragsverarbeiter**“ bedeutet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Personendaten im Auftrag des Verantwortlichen verarbeitet.

“**AVV**” bedeutet dieser Auftragsverarbeitungsvertrag.

“**Bearbeitung / Bearbeiten**“ (bzw. «**Verarbeitung / verarbeiten**») bedeutet jegliche Aktivitäten oder Gruppen von Aktivitäten, die in Bezug auf Personendaten oder Sätze von Personendaten ausgeführt werden, unabhängig davon, ob unter Verwendung automatisierter Mittel oder nicht, wie beispielsweise die Erfassung, Aufzeichnung, Organisation, Gliederung, Speicherung, Anpassung oder anderweitige Veränderung, Abfrage, Einsichtnahme, Nutzung, Offenlegung durch Weitergabe, Verbreitung oder anderweitige Bereitstellung, Abgleichung oder Kombination, Beschränkung, Löschung oder Vernichtung von Daten oder der Zugang zu ihnen.

"**Betroffene Person(en)**" bedeutet eine identifizierte oder identifizierbare natürliche Person, die auf direkte oder indirekte Weise identifiziert werden kann, insbesondere unter Bezugnahme auf einen Identifikator, wie beispielsweise einen Namen, eine Identifikationsnummer, eine IP-Adresse, Ortsdaten, einen Online-Identifikator oder einen oder mehrere Faktoren, die sich konkret auf die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität der betreffenden natürlichen Person beziehen, vorbehaltlich dessen, dass betroffene Personen (i) auch andere Personen als lebende Einzelpersonen sowie (ii) juristische Personen, soweit die Bearbeitung von Personendaten einer juristischen Person durch die Gesetze oder Vorschriften zum Datenschutz reguliert wird, einschliesst.

"**Dienstleistungen**" umfasst (1) die im Hauptvertrag beschriebenen Dienste und Dienstleistungen, Aufgaben und Zuständigkeiten, darin eingeschlossen die Bereitstellung von Liefergegenständen, sofern zutreffend, gegebenenfalls einschliesslich jeglicher Gewährleistungsbehelfe, die dem Verantwortlichen und/oder ihre verbundenen Unternehmen durch den Auftragsverarbeiter unentgeltlich eingeräumt werden; (2) Dienstleistungen, Aufgaben und Zuständigkeiten, die vorvertraglich in Hinblick auf den Vertragsabschluss erbracht wurden; und (3) jegliche Dienstleistungen, Aufgaben und Zuständigkeiten, die zwar nicht ausdrücklich in irgendeinem der Verträge festgehalten sind, die jedoch im Hinblick auf die ordnungsgemässe Ausführung und Erbringung der unter (1) und (2) beschriebenen Dienstleistungen erforderlich sind.

"**EU-Standardvertragsklauseln**" bedeutet die Standardvertragsklauseln gemäss der Entscheidung 2004/915/EG der Europäischen Kommission vom 27. Dezember 2004 über Standardvertragsklauseln für die Weitergabe Personendaten in Drittländer, wie durch die Entscheidung 2021/679/EG der Kommission vom 4. Juni 2021 geändert, in ihrer jeweils gültigen Fassung sowie den Anerkennungsbeschluss des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vom 27. August 2021 über die revidierten EU-Standardvertragsklauseln für eine Datenübermittlung in Länder ohne ein angemessenes Datenschutzniveau. Bei Änderungen der EU-Standardklauseln durch eine zuständige Aufsichtsbehörde wird davon ausgegangen, dass sich Verweise und Bezugnahmen auf die EU-Standardklauseln auf die geänderten EU-Standardklauseln beziehen.

"**Fertigungs- und Geschäftsgeheimnis**" bedeutet die gesetzliche und vertragliche Verpflichtung, keine Informationen offenzulegen, die sich auf irgendeinen durch den Verantwortlichen geheim gehaltenen Geschäftsbereich beziehen.

"**Fernmeldegeheimnis**" bedeutet die gesetzliche Verpflichtung und Garantie zur Achtung des Brief-, Post- und Fernmeldeverkehrs nach den geltenden fernmelderechtlichen Vorschriften.

"**Gesetze und Vorschriften zum Datenschutz**" bedeutet Gesetze und Vorschriften zum Datenschutz und/oder zur Bearbeitung von Personendaten in Bezug auf den Verantwortlichen und Auftragsverarbeiter wie insbesondere aber nicht abschliessend das Schweizerische Bundesgesetzes über den Datenschutz vom 25. September 2020 (DSG, SR 235.1), und die Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Bearbeitung von Personendaten und zum freien Datenverkehr sowie zur Aufhebung der Richtlinie 95/46/EG (Allgemeine Datenschutzverordnung, DSGVO), wenn ein Verbindungspartner oder der Nutzer sich in der EU befindet, einschliesslich der für jeden Verantwortlichen und/oder jedes Konzernmitglied des Verantwortlichen geltenden nationalen Gesetze und Vorschriften zum Datenschutzes.

“**Hauptvertrag**“ bedeutet der zwischen den Parteien geschlossene Vertrag gemäss Ziffer 1.1 dieses AVV.

“**Partei(en)**” bedeutet die im Vertrag definierte(n) Partei(en), einschliesslich der genehmigten Empfänger und Nachfolger der betreffenden Partei(en).

“**Personendaten des Auftraggebers**” schliesst unter anderem Personendaten der Endkunden, deren Verbindungsteilnehmer, Mitarbeiter, und/oder Auftragsverarbeiter des Auftraggebers ein.

“**Personendaten**“ bedeutet alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, einschliesslich besonders schützenswerter Personendaten gemäss diesem Vertrag und Gesetze und Vorschriften zum Datenschutz.

“**Pseudonymisierung**” bedeutet die Bearbeitung von Personendaten in der Weise, dass Personendaten nicht länger einer betroffenen Person ohne Nutzung zusätzlicher Informationen zugeordnet werden können, unter der Bedingung, dass die betreffenden zusätzlichen Informationen gesondert verwahrt werden und Gegenstand technischer und organisatorischer Massnahmen sind, durch die sichergestellt wird, dass keine Re-Identifikation erfolgen kann.

“**Relevante Weitergabe**“ bedeutet eine Weitergabe von Personendaten an eine Drittpartei, die sich in einem Land befindet, das (für die Zwecke dieses AVV) keine angemessenen Sicherheitsvorkehrungen bietet.

“**Subunternehmer**” bedeutet jegliche durch den Auftragsverarbeiter beauftragten Erfüllungsgehilfen, Auftragnehmer oder sonstigen Drittparteien.

“**Verantwortlicher**“ bedeutet die natürliche oder juristische Person, Behörde, Agentur oder eine beliebige sonstige Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Bearbeitung von Personendaten entscheidet.

“**Verbundene Unternehmen**” bedeutet des Verantwortlichen oder Auftragsverarbeiters Tochtergesellschaften und/oder Konzerngesellschaften, an denen eine stimm- oder kapitalmässige Mehrheitsbeteiligung von mehr als 51% besteht.

“**Vertrauliche Informationen**” bedeutet alle Informationen nicht-öffentlicher Art in Bezug auf eine Partei oder eines ihrer verbundenen Unternehmen, die durch eine Partei oder eines ihrer verbundenen Unternehmen (hierin “Offenlegende Partei” genannt) gegenüber der anderen Partei oder einem ihrer verbundenen Unternehmen (hierin “Erhaltende Partei” genannt) in mündlicher, schriftlicher, elektronischer oder beliebiger sonstiger Form offengelegt werden oder der Erhaltenden Partei während der Erbringung von Dienstleistungen gemäss Vertrag anderweitig zur Kenntnis gelangen. vertrauliche Informationen umfassen unter anderem technologische oder organisatorische Prozesse, Kunden, Personal, geschäftliche Aktivitäten, Datenbanken, geistiges Eigentum, die Bestimmungen und Konditionen beliebiger Verträge und andere damit zusammenhängende Informationen sowie alle sonstigen Informationen und Werte, bei denen angemessener Weise oder üblicherweise von einem vertraulichen oder anderweitig sensiblen Charakter auszugehen ist, unabhängig davon, ob sie konkret als vertraulich gekennzeichnet sind oder nicht wie z.B. Fertigungs- und Geschäftsgeheimnisse. Vertrauliche Informationen beinhalten keine Informationen, die (i) der Erhaltenden Partei bereits vor der Offenlegung auf rechtmässige Weise ohne Vertraulichkeitsverpflichtung vorgelegen haben und durch die Erhaltende Partei weder direkt noch indirekt von der Offenlegenden Partei erlangt wurden, oder (ii) aufgrund einer durch den

Eigentümer der betreffenden Informationen genehmigten Offenlegung allgemein verfügbar sind oder werden, oder (iii) der Erhaltenden Partei auf rechtmässige Weise durch eine Drittpartei zur Verfügung gestellt wurden, die zur Weitergabe oder Offenlegung derselben auf nicht-vertraulicher Grundlage befugt ist, oder (iv) durch die Erhaltende Partei auf eigenständige Weise und ohne Bezugnahme auf vertrauliche Informationen der Offenlegenden Partei nachweislich selbst entwickelt werden.

"**Vertreter**" umfasst die Belegschaft, Direktoren, Führungskräfte, Mitarbeiter, Erfüllungsgehilfen, Berater, Auftragnehmer, Subunternehmer sowie jegliche sonstigen Arten von ermächtigten Vertretern und Beratern einer Partei, sofern zutreffend, bzw., je nach Fall, Personal.

"**Zugang bzw. Fernzugang**" bedeutet die Tätigkeit oder Fähigkeit des Erstellens, Abrufens, Änderns, Weitergebens, Speicherns oder Bearbeitens von Personendaten, Assets, Medien und Datenträgern des Verantwortlichen oder des Auftragsverarbeiters.

	PASCOM® www.pascom.net
Auftraggeber	Auftragnehmer

Stand: 13.08.2025

Anlage 1
Technische und Organisatorische Massnahmen (ToM) (Art. 8 DSG iVm. Art. 2 ff. Datenschutzverordnung (DSV) bzw. 32 DSGVO)

ToM der pascom Switzerland GmbH
Vertraulichkeit (Art. 8 DSG iVm Art. 2 lit. a Datenschutzverordnung (DSV) bzw. Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle	
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen	Büroräume: • Zugang über Schlüssel / RFID-Chip • Rechenzentrum AWS (Frankfurt) (https://aws.amazon.com/de/compliance/iso-27001-faqs/)
Zugangskontrolle	
Keine unbefugte Systembenutzung	• Authentifizierung mit Benutzer und Passwort • Multi-Faktor-Authentifizierung (MFA) • Firewall • Komplexe Kennwörter • Passwort-Datenbank • Technische Sperre des Arbeitsplatzes bei Nichtaktivität • Datenträger der Endgeräte sind verschlüsselt • VPN-Einwahl für Mitarbeiter • Umfassender Schutz gegen Malware auf Arbeitsplatzrechnern und Servern • Role-Based Access Control (RBAC) mit minimalen Berechtigungen
Zugriffskontrolle	
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems	• Berechtigungskonzepte erfolgt durch die Aktualisierung einmal pro Jahr. • Änderungen und Berechtigungen an IT-Systemen werden im Ticket-System dokumentiert • VPN-Einwahl für Mitarbeiter • Laufende Bereinigung der zentralen Benutzerdatenbank (Entra ID) und VPN-Berechtigungen
Trennungskontrolle	
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden	• Mandantenfähigkeit • Getrennte Speicherung von Kundendaten • Getrennte Entwicklungs-, Test- und Produktivsysteme

Pseudonymisierung	
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen; (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)	• Teil-Anonymisierung der Daten im Falle von Einzelverbindungnachweisen

Integrität (Art. 8 DSG iVm Art. 2 lit. c DSV bzw. Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle	
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport	• Remote Zugang via Virtual Private Networks (VPN) • Sicherer SMTP-Server (STARTTLS, PFS) • Verschlüsselung der Datenträger • Drahtlose Netze mit WPA3-Verschlüsselung • Sicherer Zugang für Kunden über my.pascom.net Portal
Eingabekontrolle	
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind	• Protokollierung von Eingaben (Änderungshistorie) • Protokollierung der Zugriffe auf Kundensystemen • Ticket-System

Verfügbarkeit und Belastbarkeit (Art. 8 DSG iVm Art. 2 lit. b DSV bzw. Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle	
	• Flächendeckender Virenschutz • Einsatz von Firewalls • Aktuelles Notfallhandbuch vorhanden • Backup- und Recovery-Konzept • Zeitnahes Einspielen von Sicherheitspatches und -Updates • Datenhaltung in zertifizierten Rechenzentren (AWS) mit Spiegelung kritischer Daten • Unterbrechungsfreie Stromversorgung (USV) • Automatisiertes Patchmanagement • Monitoring-Systeme mit Alarmierung • Datensicherung an einem sicheren, ausgelagerten Ort • Feuerlöscheinrichtung • Klimatisierung

Rasche Wiederherstellbarkeit	
(Art. 32 Abs. 1 lit. c DS-GVO)	• Wiederherstellung mit einzelnen Dateien wird bei Bedarf durchgeführt und im Ticket-System dokumentiert. • Es finden Übungen und Tests zum Wiederanlauf von Systemen im Notfall statt.

Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung (Art. 7 DSG, Art. 8 DSG iVm Art. 2 lit. d DSV bzw. Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Organisationskontrolle	
Datenschutzmanagement	• Informationssicherheitsleitlinie • Verpflichtung der Mitarbeiter auf Vertraulichkeit und Fernmeldegeheimnis • Benennung eines Datenschutzbeauftragten • Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) • Organisatorische und technische Maßnahmen (Art. 32 DS-GVO) • Risikoanalyse (Art. 32 DS-GVO) • Datensicherheitsrichtlinien • Schulung und Sensibilisierung der Mitarbeiter • Meldung von Sicherheitsvorfällen (Art. 33, 34 DS-GVO) • Bei Bedarf: Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) • Interne Audits Informationssicherheit • Datenschutzaudits intern • Externe Audits (Zertifizierungen)
Datenschutzfreundliche Voreinstellungen	

(Art. 25 Abs. 2 DS-GVO)	• SMTP Server (STARTTLS, PFS)
	• Webserver mit SSL (HTTPS)
	• Maßnahmen für die pascom ONE (SaaS)
	  • Zugriff auf die Webseiten nur über (HTTPS)
	  • Verschlüsseltes Signaling (SIP/TLS)
	  • Übertragung der Sprache nur verschlüsselt (SRTP)
	  • Sichere Provisionierung der Endgeräte (HTTPS/ AES256 Token)
	  • Verschlüsselung der Client-Kommunikation (TLS)
	• Drahtlose Netze mit WPA3-Verschlüsselung

Auftragskontrolle	
	• Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers • Eindeutige Vertragsgestaltung • formalisiertes Auftragsmanagement • strenge Auswahl des Dienstleisters • Vorabüberzeugungspflicht • Nachkontrollen

Hinweis:
Das Unternehmen ist nach ISO/IEC 27001 zertifiziert.

Anlage 2 zum AVV: Template zur Meldung von Datenschutzverletzungen

Meldung an: den Datenschutz- bzw. Informationsschutzverantwortlichen des «Verantwortlichen»

Auftragsverarbeiter	
Zeitspanne/-datum des Vorfalles	
Zeitpunkt der Feststellung	
Beschreibung des Vorfalles	
Betroffene Datenkategorien	
Anzahl der betroffenen Personen	
Betroffenes IT System Verantwortliche Abteilung beim Auftragsverarbeiter	
Name und Kontaktdetails des Datenschutzbeauftragten oder -beraters	
Autor + Datum der Meldung	
Wer wurde von wem informiert (Datenschutzbehörden, betroffene Personen, Aufsichtsbehörden) und falls ja, was wurde kommuniziert	
Quelle der Information über die Datenschutzverletzung	
Beschreibung der Konsequenzen des Vorfalles	
Beschreibung der allenfalls bereits getroffenen Massnahmen durch den Auftragsverarbeiter (unter Berücksichtigung, dass keine Beweise zerstört werden)	
Wurde eine Strafverfahren anhängig gemacht	
Beschreibung weitergehenden zukünftiger technischer und organisatorischer Massnahmen	
Massnahmen zur Mitigation des Schadens des Vorfalles	
Gesamtrisikobeurteilung	