VERTRAG ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 28 DS-GVO

VEREINBARUNG

zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -
und der

pascom GmbH & Co.KG
Berger Straße 42
D-94469 Deggendorf

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Bestellung einer pascom Lizenz (Kauf, Partner oder Subscription). Je nach Beauftragung kann diese verschiedene Leistungen enthalten. Hierzu zählt insbesondere, dass der Auftragnehmer die Software hostet und dem Auftraggeber in Form einer SaaS Lösung zur Verfügung stellt und/oder dass der Auftragnehmer beim Auftraggeber Fernwartungen (remote Support) durchführt.

1.2 Dauer

Die Dauer dieses Auftrags entspricht der Vertragslaufzeit der seitens des Auftraggebers bestellten pascom Lizenz.

2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers ergeben sich aus den Beauftragten Leistungen innerhalb der pascom Lizenz.
Die Auftragsverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und den in Kapitel V der DS-GVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieser Vereinbarung erfolgen.

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/ Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Nutzungs- und Verhaltensdaten

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Geschäftspartner
- Bewerber

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 in Anlage 1 beschriebenen Maßnahmen werden zwischen den Parteien als verbindlich festgelegt.

3.2 Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. 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. 32 Abs. 1 DS-GVO zu berücksichtigen.

3.3 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.

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

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt:

   Herr Michael Gruber
   BSP-SECURITY
   Franz-Mayer-Str. 1, D-93053 Regensburg
   T +49 (0) 941 462 909 29
   E-Mail: michael.gruber@bsp-security.de

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO gemäß der Anlage 1

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) 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 Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- 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.

g) 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.

6 Unterauftragsverhältnisse

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 Telekommunikationsleistungen, 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 Datenverarbeitungsanlagen 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 Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
Auf der Webseite https://www.pascom.net/de/datenschutz/ befindet sich eine Liste aller beauftragten Unterauftragnehmer. Der Auftraggeber stimmt der Beauftragung der dort aufgeführten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

6.3 Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht innerhalb 14 Tage gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

6.4 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7 Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer 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.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, erfolget durch

- aktuelles Testat des externen Datenschutzbeauftragten

- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (ISIS12).

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

8 Mitteilung bei Verstößen des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. 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 personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem 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 Vergütung beanspruchen.

9 Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

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

10 Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. 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.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11 Sonstiges

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.

Mündliche Nebenabreden bestehen nicht. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, insbesondere Geschäftsgeheimnisse und Kenntnisse über Datensicherheitsmaßnahmen, zeitlich unbegrenzt auch nach Beendigung des Vertrages vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

Sollten einzelne Teile dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden oder sollte sich eine Lücke herausstellen, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen 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.

	Auftraggeber
Deggendorf	pascom GmbH & Co KG • Berger Straße 42 94469 Deggendorf • www.pascom.net
	Auftragnehmer

Anlage 1

Technische und Organisatorische Maßnahmen (ToM) (Art. 32 DS-GVO)

ToM der pascom GmbH & Co. KG
Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle	
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen	Büro: • Zugang über Schlüssel / RFID Chip Rechenzentrum (TSI V3.2 Level 2 (erweitert)): • Alarmanlage • Wachdienst • Zugang mit RDIF und Fingerabruck (MFA) • Protokollierung des Zutritts
Zugangskontrolle	
Keine unbefugte Systembenutzung	• Authentifizierung mit Benutzer und Passwort • Multi Faktor Authentifizierung (MFA) • Firewall • Komplexe Kennwörter • Passwort-Datenbank (Team password Manager) • Technische Sperre des Arbeitsplatzes bei Nicht-Aktivität • Festplatten der Notebooks sind Verschlüsselt • VPN Einwahl für Mitarbeiter • Umfassender Schutz gegen Malware auf Arbeitsplatzrechnern und Servern
Zugriffskontrolle	
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems	• Berechtigungskonzepte erfolgt durch die Aktualisierung einmal pro Jahr. • Änderungen und Berechtigungen an IT-System werden im Ticket-System dokumentiert • VPN Einwahl für Mitarbeiter • Laufende Bereinigung der AD/Samba 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)	• Pseudonymisierung wird im Unternehmen standardmäßig nicht verwendet und kommt nur Ausnahmefällen wie z.B. Upgrade von Datenbanken durch externe Dienstleister zum Einsatz.

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

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 Laptops
Eingabekontrolle	
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind	• Protokollierung von Eingaben • Ticketsystem

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

Verfügbarkeitskontrolle	
	• Flächendeckender Virenschutz • Einsatz von Firewalls • Aktuelles Notfallhandbuch vorhanden • Backupkonzept • Datenhaltung in zwei zertifizierten Rechenzentren mit Spiegelung kritischer Daten • Unterbrechungsfreie Stromversorgung (USV) • Automatisiertes Patchmanagement • Monitoring-Systeme • Datensicherung an einem sicheren, ausgelagerten Ort
Rasche Wiederherstellbarkeit	
(Art. 32 Abs. 1 lit. c DS-GVO)	• Wiederherstellung mit einzelnen Dateien werden bei Bedarf durchgeführt und im Ticket-System dokumentiert. • Es finden Übungen und Tests zum Wiederanlauf von Systemen im Notfall statt.

Hinweis:
Das Unternehmen ist nach ISIS12 zertifiziert.

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

Organisationskontrolle	
Datenschutzmanagement	• 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 (Artt. 33, 34 DS-GVO)
Datenschutzfreundliche Voreinstellungen	

(Art. 25 Abs. 2 DS-GVO)	• SMTP Server (STARTTLS, PFS)
	• Webserver mit SSL (HTTPS)
	• Maßnahmen für die pascom Cloud (SaaS)
	  • ZZugriff auf die Webseiten nur über (HTTPS)
	  • Verschlüsseltes Signalling (SIP/TLS)
	  • Übertragung der Sprache nur verschlüsselt (SRTP)
	  • Sichere Provisionierung der Endgeräte (HTTPS/ AES256 token)
	  • Verschlüsselung der Client Kommunikation (TLS/XMPPS)
	• WLAN Kommunikation WPA2

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