CONTRACT REGARDING PURCHASE ORDER PROCESSING PURSUANT TO ARTICLE 28 OF THE GDPR

AGREEMENT

Between

- controller - hereinafter referred to as Client -
and

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

- processor - hereinafter referred to as Agent

1 Subject matter and Term of the Order

1.1 Subject matter

The subject matter of the order results from requesting a pascom licence (purchase, partner or subscription). This may contain various services depending on the specific assignment. In particular, this includes the Agent hosting the software and making it available to the Client in the form of a SaaS solution and/or the Agent handling remote support for the Client.

1.2 Term

The term of this order amounts to the duration of the pascom licence contract ordered by the Client.

2 Substantiation of the Order Content

2.1 Nature and purpose of the proposed data processing

A more detailed description of the subject matter of the order with regard to the nature and purpose of the Agent's tasks will emerge from the services assigned within the pascom licence.

The purchase order processing shall take place exclusively within a European Union member state or in another participating state of the Agreement on the European Economic Area. Relocation into a third country may only occur with the consent of the Client and in accordance with the conditions stipulated in chapter V of the GDPR and in compliance with the terms of this agreement.

2.2 Nature of the data

The following types/categories of data constitute the subject matter of personal data processing (list/description

of data categories)

- Personal master data
- Contact details (e.g. telephone numbers, e-mail)
- Contract master data
- Contractual billing and payment data
- Usage and behavioural data

2.3 Categories of data subjects

The categories of the data subjects affected by this processing include:

- Customers
- Interested parties
- Employees
- Suppliers
- Business partners
- Applicants

3 Technical and Organisational Measures

3.1 The Agent must document the implementation of the technical and organisational measures necessary that are stated in the preliminary stages of order placement before commencing with processing, particularly with regards to the concrete order execution, and must present this to the Client for inspection. The measures described in Appendix 1 are set as binding between the parties.

3.2 The Agent must establish security in accordance with Articles 28, para 3 c, and 32 of the GDPR, particularly in combination with Article 5, para 1, para 2 of the GDPR. These measures concern measures for data security and aim towards safeguarding against any risk to the appropriate level of security regarding the confidentiality, integrity, availability and capacity of the systems. This requires consideration of the state of the art, of implementation costs and the nature, scope and purposes of the processing as well as the differing probability of occurrence and severity of the risk to rights and freedoms of natural persons in the sense of Article 32, para 1 of the GDPR.

3.3 The technical and organisational measures are subject to technical progress and further development. In this respect, the Agent is permitted to implement alternative adequate measures. In doing so, the level of security shall not fall short of the measures specified. Significant alterations shall be documented.

4 Adjusting, Constraining and Erasing Data

4.1 The Agent may not adjust, erase or constrain the data processed in the order without authorisation. Rather, this can only occur with documented instructions from the Client. If a data subject approaches the Agent directly concerning this matter, the Agent shall pass the request on to the Client immediately.

4.2 If they are included within the scope of services, the erasure procedure, the right to be forgotten, any adjustment, data portability and information are to be secured by the Agent promptly following the documented instructions given by the Client.

5 Quality Assurance and Other Agent Duties

The Agent has certain legal responsibilities in addition to complying with the regulations of this order, pursuant to Articles 28 to 33 of the GDPR; to this effect, the Agent shall ensure compliance with the following stipulations:

a) Designating a data protection officer in writing who shall perform their duties in accordance with Articles 38 and 39 of the GDPR:

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

b) Ensuring confidentiality in accordance with Articles 28, para 3, clause 2 b, 29 and 32, para 4 of the GDPR. The Agent shall only appoint employees who are committed to confidentiality and who are made familiar with the data protection regulations relevant to them beforehand when conducting the work. The Agent and any person under the Agent's control who has access to the personal data may process these data only with respect to the instructions given by the Client, including the authorities granted in this contract, unless these persons are legally obliged to process.

c) The implementation of and compliance with all of the technical and organisational measures required for this order pursuant to Articles 28, para 3, clause 2 c and 32 of the GDPR in accordance with Appendix 1

d) The Client and the Agent shall cooperate with the supervisory authority on request while completing their tasks.

e) The Client will promptly inform the supervisory authority about assessment activities and measures if these are relevant to the order. This also applies if a competent supervisory authority makes investigations into the Agent's order processing with regards to processing personal data in the context of a non-compliance or criminal procedure.

f) If the Client is put through an inspection by the supervisory authority, a non-compliance or criminal procedure, a liability claim from a data subject or a third party or another claim in connection with the order processing for the Agent then the Agent shall support the Client to the best of their power.

g) The Agent shall monitor internal processes regularly as well as checking technical and organisational measures in order to ensure that processing in the Agent's area of authority remains in line with the demands of the applicable data protection law and that the protection of the data subject's rights are ensured.

h) Ensuring the technical and organisational measures implemented can be verified for the Client within the scope of their supervisory capacity according to item 7 in this contract.

6 Sub-contractual Relations

6.1 Sub-contractual relations within the meaning of this regulation should be understood as those services

which relate directly to the performance of the main service. This does not include supplementary services which the Agent evokes for other purposes, e.g. telecommunication services, postage/transportation services, maintenance and user services or disposing of data media or other measures for ensuring the confidentiality, availability, integrity and capacity of the hardware and software used in data processing systems. However, the Agent is obliged to establish appropriate and lawful contractual agreements and monitoring measures in order to ensure data protection and data security for the Client's data, even in the case of outsourced supplementary services.

6.2 The Agent may only commission sub-contractors (other order processors) with prior express permission from the Client, obtained in written/documented form.

A list of all commissioned sub-contractors can be found on the website https://www.pascom.net/en/data-protection/. The Client agrees to the commission of the sub-contractors listed there, abiding by the conditions of a contractual agreement subject to Article 28, para 2-4 of the GDPR.

6.3 Outsourcing further sub-contractors or changing the existing sub-contractor is permitted, provided that:

- the Agent informs the Client of this sub-contractor outsourcing in advance with reasonable time to spare, in written or text form and
- the Client does not raise an objection to the planned outsourcing with the Agent within 14 days in written or text form and
- a contractual agreement is established subject to Article 28, para 2-4 of the GDPR.

6.4 The transferral of the Client's personal data to sub-contractors and their initial commencement are only permitted once all requirements for sub-contracting are met.

7 Supervisory rights of the Client

7.1 The Client has the right to conduct inspections in consultation with the Agent or to have such inspections conducted by an inspector designated on a case by case basis. The Client has the right to ensure the Agent's compliance with this agreement during business operations by way of random inspections which shall generally be declared with sufficient time.

7.2 The Agent shall ensure that the Client can be assured of compliance with the Agent's duties in accordance with Article 28 of the GDPR. The Agent is obliged to present the Client with the necessary information on request and in particular to demonstrate the implementation of technical and organisational measures.

7.3 Demonstration of any measures which do not only concern the present order shall occur through

- current attestation from the external data protection officer
- suitable certification by an audit of IT security or data protection (ISMS12).

7.4 The Agent can claim payment entitlements via the Client in order to allow inspections.

8 Reporting Infringements by the Agent

8.1 The Agent shall support the Client in complying with the responsibilities listed in Articles 32 to 36 of the GDPR

regarding the security of personal data, reporting duties of data breaches, data protection impact assessments and previous consultations. This includes but is not limited to

a) ensuring an appropriate level of protection using technical and organisational measures which take into account the context and purpose of the processing as well as the projected likelihood and severity of a possible violation of the law occurring as a result of security gaps, and which allow immediate identification of relevant violating acts

b) the obligation to report violations of personal data to the Client immediately

c) the obligation to assist the Client in the context of their information duty towards the data subject and to make all relevant information available to them immediately in connection with this

d) supporting the Client with their data protection impact assessment

e) supporting the Client within the scope of previous consultations with the supervisory authority

8.2 For those supporting services which are not included in the service description or which cannot be ascribed to misconduct on the Agent's part, the Agent can claim remuneration.

9 Client's Authority to Issue Directives

9.1 The Client shall confirm spoken directives immediately (at least in text form).

9.2 The Agent must inform the Client immediately if they believe that a directive violates data protection legislation. The Agent is entitled to suspend implementation of this particular directive until it is confirmed or altered by the Client.

10 Erasing and Returning Personal Data

10.1 Copies or duplicates of data will not be produced without the Client's knowledge. This excludes security copies, provided that these are necessary to ensure proper data processing, as well as data which are necessary in order to comply with legal obligation to retain records.

10.2 After concluding contractually arranged work or earlier on the Client's request - at the latest when the services agreement is terminated - the Agent must return all documents they have obtained, all processing and usage results as well as data bases which are associated with the order relation to the Client or to destroy these with prior agreement in a manner in keeping with data protection requirements. The same applies to test and commission materials. The method for erasing the data shall be submitted on request.

10.3 Documentation that serves as proof of the ordered and proper data processing are to be retained by the Agent in accordance with the respective retention period beyond the termination of the contract. The Agent can deliver these to the Client when the contract is terminated for mitigation.

11 Miscellaneous

Agreements regarding the technical and organisational measures as well as monitoring and inspection

documents (and regarding sub-contractors) shall be retained by both contractual partners for the duration of their validity and then for another three full calendar years after this.

Verbal side agreements do not exist. Written agreement or a documented electronic format is a strict requirement for side agreements.

If the Client's property or personal data to be processed is put at risk by the Agent because of actions committed by third persons (for instance through seizure or confiscation), by insolvency proceedings or a conciliation procedure or through some other occurrences, then the Agent must inform the Client of this immediately.

A plea for the right of retention in the sense of section 273 of the German Civil Code (BGB) is precluded with respect to the data processed for the Client and the associated data media.

Both parties are obliged to treat as confidential all information that they receive in connection with the completion of this contract, especially trade secrets and knowledge about data security measures, indefinitely, even after the contract is terminated and only to use this information in order to complete the contract. Neither party is entitled to use part or all of this information for purposes other than those stipulated or to make this information accessible to third parties.

If individual parts of this agreement are or become wholly or partially ineffective or if a gap appears then this does not affect the validity of the rest of the agreement. In place of the ineffective clause or in order to fill a gap in the regulation, a suitable regulation shall apply which will be as close as possible to the one the parties would have intended if they had considered this point.

City / Town / Place Date	Client
Deggendorf	pascom GmbH & Co KG • Berger Straße 42 94469 Deggendorf • www.pascom.net Agent

Appendix 1

Technical Organisational Measures (ToM) (Art. 32 GDPR)

ToM of pascom GmbH & Co. KG
Confidentiality (Art. 32 §1 b GDPR)

Building Access	
No unauthorised entry to data processing areas.	Office: • External Key Control / RFID Chip Access DataCentre (TSI V3.2 Level 2 (Advanced)): • Alarm system • Security Service • RFID chip and fingerprint controlled access (MFA) • Access logging
System Access	
No unauthorised system usage.	• Authentication with user and password • Multi-Factor Authentication (MFA) • Firewall • Complex passwords • Password database (Team password Manager) • Technical workstation locking upon not active • Encrypted notebook hard disks • Employee VPN access • Comprehensive malware protection for workstations and servers
Data Access	
No unauthorised reading, copying, modifying or removal from within the system.	• Authorisation concepts annually reviewed and updated • Document all changes to authorisations and to IT systems • Employee VPN access • Annual clean of AD / Samba and VPN permissions
Data Separation	
Separate processing of data collected for different purposes	• Multi-tenancy • Separated storage of customer data • Separated Development, Test and Productive Systems

Pseudonymisation	
The processing of personal data in such as way that the data can no longer be assigned to a specific data subject without requiring additional information, provided that such additional information is kept separate and subject to appropriate technical and organisational measures; (Art. 32 §. 1a GDPR; Art. 25 §. 1 GDPR)	• Per default, Pseudonymisation is not used within the company and only occurs under exceptional circumstances e.g. when the upgrading of databases by external service providers.

Integrity (Art. 32 (1) lit. b GDPR)

Confidentiality - Data Transmission / Storage / Destruction	
No unauthorised reading, copying, modifying or destruction by electronic transmission or transportation.	• Remote access via Virtual Private Networks (VPN), • Secure SMTP-Server (STARTTLS, PFS) • Encrypted Laptops
Integrity - Data Entry Controls	
Determine if and by whom personal information within the data processing systems was entered, modified or deleted.	• Protocol logging of data entry • Ticket System

Availability and Resilience (Art. 32 (1) lit. b GDPR)

Availability	
	• Comprehensive virus protection • Use of Firewalls • Robust & maintained emergency / data recovery protocol available • Backup concept • Data stored in two certified data centres with critical data mirrored in both centres • Uninterrupted Power Supply (USP) • Automated patch management • Monitoring system • Data backup in a secure, outsourced location
Rapid Recovery & Restore	
(Art. 32 §. 1c GDPR)	• Restoration of individual files conducted according to requirements and documented within the ticket-system. • Regular emergency system restore training and certification.

Note:
The company is certified according to ISIS12.

Procedure for regular testing, assessing and evaluating (Art. 32 (1) lit. d GDPR; Art. 25 (1) GDPR)

Organisational Control	
Data Protection Management	• Appointing a Data Protection Officer • Records of processing activities (Art. 30 GDPR) • Security of Processing (Organisational and Technical Measures) (Art. 32 GDPR) • Risk Analysis (Art. 32 GDPR) • Data Security Policies • Training and sensitization of employees • Reporting / notification of security incidents (Art. 33, 34 GDPR)
Data Protection by Design and Default	

(Art. 25 §. 2 GDPR)	• SMTP Server (Start TLS, PFS)
	• SSL Web Server (HTTPS)
	• Measures for pascom Cloud (SaaS)
	  • Website access only over (HTTPS)
	  • Encrypted Signalling (SIP/TLS)
	  • Voice transmission encryption (SRTP)
	  • Secure provision of endpoints (HTTPS/AES256 token)
	  • Encryption of desktop UC / CTI application communication (TLS/XMPPS)
	• WiFi Communication WPA2

Order Controls / Tracking / Auditing	
	No order data processing in the sense and meaning of Art. 28 GDPR is conducted without the corresponding instruction of the Client, for example. clear contract design, formalised order management, strict selection of service providers / subcontractors, compulsory pre-compilation and follow up controls etc.