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.