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.