Nachweis der Umsetzung der TOM (Stand 01.02.2024)

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

Vorgabe	Erfüllt	Geplant	Bemerkung
Zutrittskontrolle			
Haupteingangstür mit Knauf auf der Außenseite	x		
Eingangsbereich & Fenster sind außerhalb der Geschäftszeit verschlossen	x		Dienstanweisung, letzte Person prüft und verschließt alles (Hinweis für letzte Person am Terminal der Zeiterfassung)
Sicherheitsschloss an der Eingangstür	x		Automatisches Verriegeln bei jedem Schließen und Öffnung über Zutrittssystem mit technischer Kontrolle der Türschließung
Besucher Begleitung durch P&S-Personal	x		
Außerhalb der Bürozeiten sind die Gebäude entsprechend gesichert	x		Automatisches Schließsystem am Gebäude
Sorgfalt bei der Auswahl des Reinigungsdienstes	x		
Zugangskontrolle			
Rechner- Login mit Benutzername und Passwort mit Protokoll	x		Durch Direktzuordnung der Geräte ist nur der jeweilige Mitarbeiter berechtigt
Verwendung von Anti-Virus Software auf Server und Clients	x		Clients mit Windows nutzen Microsoft Defender Server / Clients mit Linux nutzen ClamAV, Laptopfestplatten sind verschlüsselt
Firewall	x		Firewall PFsense
Intrusion Detection System	x		Firewall PFsense
Systeme werden auf den aktuellen Stand gehalten	x		Windows Updates auf Clients automatisch Server werden Updates manuell installiert (monatliche Wartung)
Einsatz von VPN bei Zugriffen von außen auf das P&S Netzwerk	x		Persönlicher Zugang für berechtigte Mitarbeiter

Organisatorische Maßnahmen			
Aktenvernichtung	x		Aktenvernichtung über zertifizierten Dienstleister
Nutzerrechte & Zugänge werden durch Administratoren verwaltet	x		Richtlinien und Nutzersperre über Windows AD
Berechtigung auf Netzwerkverzeichnisse nutzerbezogen rollenbasierend	x		
Einsatz entsprechender Passwortregelungen	x		Durch Dienstanweisung dazu angewiesen die hinterlegten Regeln einzuhalten
Zugänge werden nach einer entsprechenden Anzahl von Fehlversuchen gesperrt	x		Soweit wie möglich durch die genutzten Programme
Protokollierung von Zugriffen auf Anwendungen bei der Eingabe, Änderung und Löschung von Daten	x		Die genutzten Programme haben eine entsprechende Protokollierung der Datensätze
Regelmäßige Schulungen und Unterweisungen	x		Mindestens jährlich zu Verschwiegenheit, zum Datenschutz und zur Datensicherheit.
Nutzung von 2FA (Zwei-Faktor-Authentisierung)	x		Hetzner (Hoster)
Trennungskontrolle			
Trennung von Produktiv- und Testumgebung	x		
Physikalische Trennung von System und Datenbank	x		
Für untersch. Anwendungen werden getrennte Verzeichnisse / Datenbanken mit verschiedenen Rechten eingesetzt	x		

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

Vorgabe	Erfüllt	Geplant	Bemerkung
Weitergabekontrolle			
Einsatz von VPN zur Online-Datenübertragung	x		
Daten, die über Datenträger weitergegebenen werden, werden komprimiert und verschlüsselt	x		
Daten, die aufgrund von gesetzlichen Vorgaben an die entsprechenden Stellen zu übertragen sind, wie zum Beispiel Steuer- und Sozialversicherungsdaten werden auf den durch den Gesetzgeber vorgeschrieben Wegen und mit den dort vorgegeben Verschlüsselungen übertragen.	x		
Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind schriftlich zur Verschwiegenheit verpflichtet.	x		Arbeitnehmer sind durch Arbeitsvertag zur Verschwiegenheit verpflichtet. Es gibt Einweisung neuer Mitarbeiter und regelmäßige Belehrungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO

Vorgabe	Erfüllt	Geplant	Bemerkung
Cloud Kunden durch Rechenzentrum			
Die Sicherheit der Daten und deren Verfügbarkeit wird durch ein mehrstufiges Backup- und Recovery- Konzept gewährleistet, sowie die redundante Auslegung zentraler Systeme und ihrer Komponenten.	x		
Systeme und Datenbanken werden online gesichert, um eine größtmögliche Verfügbarkeit im Rahmen der vereinbarten Leistungserbringung zu gewährleisten.	x		
Im gesamten Gebäude existiert eine Brandmeldeanlage. Der Serverraum ist durch eine automatische Feuerlöschanlage gesichert. Im gesamten Gebäude besteht Rauchverbot.	x		
Das gesamte Gebäude ist durch eine Alarmanlage mit automatischer Benachrichtigung des Sicherheitsunternehmens geschützt. · Es erfolgen regelmäßige Datensicherungen sowie permanente Datenspiegelung.	x		
Der Zugang zu den Servern ist durch mehrstufige Sicherheitskomponenten abgesichert.	x		
Die Zugriffe auf die zentrale Anwendung im Rechenzentrumsbetrieb erfolgen über redundante Leitungen.	x		

Systeme und Datenbanken werden gesichert, um eine größtmögliche Verfügbarkeit zu gewährleisten	x		
Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen	x		
Cloud Kunden durch P&S			
Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen	x		
Für nicht Cloud Kunden obliegt die Verfügbarkeitskontrolle Auftraggeber.			
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)			Obliegt beim Auftraggeber

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

Vorgabe	Erfüllt	Geplant	Bemerkung
Datenschutzmanagement			
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf und Berechtigung durch Bereitstellung per Wiki im P&S Intranet.	x		
Interner Datenschutzbeauftragter	x		
Die Mitarbeiter sind geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet	x		
Auftragskontrolle			
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement.	x		