TOM - Technische und organisatorische Massnahmen

Anhang zum Auftragsverarbeitungsvertrag

1 Präambel

cyon gewährleistet im Interesse der Integrität, Nachvollziehbarkeit, Verfügbarkeit und Vertraulichkeit der verarbeiteten Personendaten mit geeigneten technischen und organisatorischen Massnahmen eine dem Risiko angemessene Datensicherheit.

cyon berücksichtigt bei der Auswahl der Massnahmen insbesondere die Art der verarbeiteten Personendaten, Art, Umfang, Umstände und Zweck der Auftragsverarbeitung, die hauptsächlichen Gefahren sowie die Wahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit trotz der ergriffenen Massnahmen.

2 Vertraulichkeit

«Vertraulichkeit» bedeutet, dass nur berechtigte Personen Zugang zu personenbezogenen Daten haben.

Massnahme	**Datacenter**	**cyon**
Individuelle Zutrittsberechtigungsvergabe	✓	✓
Elektronische Zutrittskontrollsysteme	✓	✓
Dokumentation von Zutrittsberechtigungen	✓	✓
Autorisiertes Wachpersonal	✓	
Besucher-Regulierungen	✓	✓
Kontrollgänge des Sicherheitspersonals	✓	
Schliessung aller Gebäudeeingänge wie Fenster und Türen	✓	✓
Transponder- oder schlüsselkartenbasierte Schliessanlage	✓	✓
Eingezäuntes Gelände inkl. Videoüberwachung	✓	
Zusätzliche Zugangsbeschränkung zu den Serverräumen	✓	
Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten	✓	✓
Protokollierung benutzerrelevanter Aktivitäten (z.B. Anmeldung, Abmeldung, Zugangsverweigerung etc.)	✓	✓

Zugangsbeschränkungen für bestimmte IP-Adressbereiche	✓	✓
VPN-Beschränkungen	✓	✓
Sperrung von nicht erforderlichen Ports	✓	✓
Externer Zugang über sichere Verbindungen (VPN etc.)	✓	✓
WLAN-Verschlüsselung	✓	✓
Regelmässige Software-Updates	✓	✓
Benutzerauthentifizierung für System- und Anwendungszugriff	✓	✓
Verschlüsselte Speicherung von Nutzer-Passwörtern	✓	✓
Nutzung Aktenvernichter		✓
Bildschirm-/Computersperre bei Verlassen des Arbeitsplatzes	✓	✓

3 Verfügbarkeit

«Verfügbarkeit» bedeutet, dass personenbezogene Daten verfügbar sind, wenn sie benötigt werden.

Massnahme	**Datacenter**	**cyon**
Schutz durch Firewalls	✓	✓
Überwachung/Protokollierung von administrativen Systemzugang und von Konfigurationsänderungen	✓	✓
Trennung von Anwendungs- und Administrationszugängen	✓	✓
Protokollierung von externen Support-Prozessen	✓	✓
Protokollierung von administrativen Änderungen	✓	✓
Zugriffsregelungen und Zugriffsverwaltung	✓	✓
Redundante Stromversorgung mit Notstrom sowie einer redundanten Diesel-Netzersatzanlage	✓	
Feuer-/Rauchmelder mit direkter Aufschaltung Feuerwehr	✓	✓
Kühlsystem im Rechenzentrum	✓	

Datensicherungspläne	✓	✓
Notfallplan	✓	

4 Integrität

«Integrität» bedeutet, dass personenbezogene Daten nicht unberechtigt oder unbeabsichtigt verändert werden.

Massnahme
• Verschlüsselte Verbindungen (https/sftp, o.ä.)
• E-Mail-Verschlüsselung (SSL/TLS)
• Rollenbasiertes Berechtigungskonzept
• Protokollierung von internen und externen (Support)-Prozessen
• Protokollierung von Dateneingaben (Nachvollziehbarkeit)
• Separate Instanzen für Entwicklungs- und Produktivsysteme

5 Regelmässige Überprüfung, Bewertung und Evaluierung

«Regelmässige Überprüfung, Bewertung und Evaluierung» bedeutet, dass die technischen und organisatorischen Massnahmen regelmässig überprüft, bewertet und evaluiert werden.

Massnahme
• Datenschutzmanagement
• Regelmässige Überprüfung und Optimierung der getroffenen Massnahmen
• Sorgfältige Wahl von geeigneten Unterauftragnehmenden

6 Schutz vor unrechtmässigem Zugang zu personenbezogenen Daten

«Schutz vor unrechtmässigem Zugang zu personenbezogenen Daten» bedeutet, dass Massnahmen ergriffen werden, aufgrund derer die Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können.

Massnahme
• Passwort-Richtlinie
• VPN-Beschränkungen
• Rollenabhängige Zugriffsbeschränkungen

7 Verarbeitung personenbezogener Daten nur nach Anweisung

«Verarbeitung personenbezogener Daten nur nach Anweisung» bedeutet, dass personenbezogene Daten nur gemäss vertraglichen Vereinbarungen mit dem Verantwortlichen oder gemäss Weisungen des Verantwortlichen bearbeitet werden.

Massnahme
• Vertraulichkeitsklausel in Arbeitsverträgen
• Datenschutz-Unterweisung der Mitarbeitenden
• Geregeltes Entsorgen von Datenträgern

8 Anonymisierung / Pseudonymisierung / Verschlüsselung

Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten des Auftraggebers sind grundsätzlich nicht Gegenstand der von cyon zu erbringenden Leistungen.

9 Belastbarkeit der Systeme

cyon unternimmt die unter Ziffer 3 dargestellten Massnahmen, um die Belastbarkeit der IT-Systeme sicherzustellen.