octonomy AI GmbH - TOMs

Technisch-organisatorische Maßnahmen	Technical and Organizational Measures
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)
• Zutrittskontrolle *Kein unbefugter Zutritt zu Datenverarbeitungsanlagen* • Biometrische Zugangskontrollen • Smartcards für Haupteingang und kritische Bereiche • 24/7 Sicherheitspersonal • Videoüberwachung der Eingänge • Manuelles Schließsystem • Besucherprotokolle • Empfang 24/7	• Physical Access Control *No unauthorized access to Data Processing Facilities* • Biometric Access Barriers • Smart Cards for Main door and critical areas • 24/7 Security Guard Personnel • Video surveillance of entrances and hallways • Manual Locking system • Visitors' Protocol • Managed Reception 24/7
• Zugangskontrolle *Keine unbefugte Systembenutzung* • Login • VPN-Zugang • Firewall zum Datenzentrum • Intrusion Detection System • Verschlüsselung • Desktop-Sperre • Zwei-Faktor-Authentifizierung	• Electronic Access Control *No unauthorized use of the Data Processing and Data Storage* • Login • VPN access • Firewall to data center • IDS • Encryption • Desktop lock • Two-factor authentication
• Zugriffskontrolle *Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems* • Rollen- und Berechtigungskonzept • Protokollierung von Zugriffen • Trennung von Entwicklung und Produktion • Regelmäßige Berechtigungsprüfungen • Richtlinien zur Nutzung mobiler Geräte • Informationssicherheitsrichtlinien	• Internal Access Control (permissions for user rights of access to and amendment of data) *No unauthorized Reading, Copying, Changes or Deletions of Data within the system* • Role and permission concept • Access logging • Separation of development and production • Regular permission audits • Mobile device policies • Information security policies
• Trennungskontrolle *Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden* • Physische und logische Trennung der Daten • Trennung von Produktiv- und Testumgebungen • Getrennte Datenhaltung für verschiedene Auftraggeber	• Separation Control *The separated processing of Data, which is collected for differing purposes* • Physical and logical separation of data • Separation of production and test environments • Separate data storage for different clients • Access permissions based on functional responsibility • Separation of databases

- Zugriffsberechtigungen nach Funktionszuordnung
- Trennung von Datenbanken

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)	2. Integrity (Article 32 Paragraph 1 Point b GDPR)
• Weitergabekontrolle	• Data Transfer Control
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport	*No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport*
• Verschlüsselung der Datenübertragung • VPN-Tunnel • Sichere Datenübertragungsprotokolle • Protokollierung von Datentransfers • Sorgfältige Auswahl von Transportdiensten • Sichere Löschung und Entsorgung	• Data transmission encryption • VPN tunnels • Secure data transfer protocols • Logging of data transfers • Careful selection of transport services • Secure deletion and disposal
• Eingabekontrolle	• Data Entry Control
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind	*Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted*
• Protokollierung von Eingaben und Änderungen • Dokumentiertes Berechtigungskonzept • Nachvollziehbarkeit von Benutzeraktionen • Schulung der Mitarbeiter • Regelmäßige Systemkontrollen	• Logging of inputs and changes • Documented authorization concept • Traceability of user actions • Employee training • Regular system checks
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)
• Verfügbarkeitskontrolle	• Availability Control
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust	*Prevention of accidental or willful destruction or loss*
• Backup-Systeme • Unterbrechungsfreie Stromversorgung (USV) • Klimaanlage in Serverräumen • Feuer- und Rauchmeldeanlagen • Notfallplan • Antivirenschutz • RAID-Systeme • Alarmsysteme	• Backup systems • Uninterruptible power supply (UPS) • Air conditioning in server rooms • Fire and smoke detection systems • Emergency plan • Anti-virus protection • RAID systems • Alarm systems
• Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);	• Rapid Recovery (Article 32 Paragraph 1 Point c GDPR);
Wiederherstellung der Verfügbarkeit	*Recovery of availability*
• Dokumentierte Wiederherstellungsprozesse • Regelmäßige Tests der Wiederherstellung	• Documented recovery procedures • Regular recovery testing

hat formatiert: Schriftart: 11 Pt.

• Definiertes Business Continuity Management • Notfallpläne und Eskalationswege • Redundante Systeme	• Defined Business Continuity Management • Emergency plans and escalation paths • Redundant systems

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)	4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)
• Datenschutz-Management; • Incident-Response-Management; • Auftragskontrolle; • Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO): Die Prinzipien von „Privacy by Design“ und „Privacy by Default“ werden im Softwareentwicklungszyklus berücksichtigt. Wir nutzen das OASIS Privacy Management Referenzmodell und die entsprechende Methodologie.	• Data Protection Management; • Incident Response Management; • Order or Contract Control; • Data Protection by Design and Default (Article 25 Paragraph 2 GDPR): The principles of Privacy by Design and Privacy by Default are taken into account in the software development lifecycle. We use the OASIS Privacy Management Reference Model and Methodology.
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers	*No third-party data processing as per Article 28 GDPR without corresponding instructions from the Client*
• Eindeutige Vertragsgestaltung • Kriterien zur Auswahl des Auftragnehmers • Kontrolle der Vertragsausführung	• Unambiguous wording of the contract • Criteria for selecting the Agent • Monitoring of contract performance