Verantwortliche*r	Freigabe durch	Freigabe am	Versionsstand
ISB	ISB	01.02.2024	#1.1

MTO PSYCHOLOGISCHE FORSCHUNG UND BERATUNG

TOM Liste (technische und organisatorische Maßnahmen)

für die
MTO Psychologische Forschung und Beratung GmbH
Schleifmühleweg 68
72070 Tübingen

Nach Artikel 32 und 28 der DSGVO sind bei der Verarbeitung von personenbezogenen Daten sogenannte TOM (technische und organisatorische Maßnahmen) zu ergreifen. Um die Einhaltung dieser Verordnung nachweisen zu können, sind diese Maßnahmen dokumentiert. Sie folgen den Grundsätzen des Datenschutzes durch Technik (data protection by design) und des Datenschutzes durch datenschutzfreundliche Voreinstellungen (data protecion by default).

Beim Stand der Technik handelt es sich um bewährte und effektive Maßnahmen, die derzeit auf dem Markt verfügbar sind. Konkretisierung bieten anerkannte nationale oder internationale Standards (z.B. von BSI).

1. Vertraulichkeit der Systeme und Dienste

1.1 Physicher Schutz

Festlegung und Dokumentation zutrittsberechtigter Personen, einschließlich des Umfanges der Berechtigung
Gelebte Regelung für den Zutritt von Firmenfremden durch Begleitung des Verantwortlichen und Zutrittsverbote für nicht öffentliche Bereiche
Sichere Schließsysteme samt dokumentierter Schlüsselverwaltung
Protokollierung der eingehenden Mitarbeiter durch Schlüsselchip
Gesicherter Eingang durch Schlüsselchipleser
Gerätesicherung gegen Diebstahl, physische Manipulation und Beschädigung
Schaffung von verschiedenen Sicherheitszonen (öffentliche Bereiche, Arbeitsplätze, Serverräume)
Hochsicherheitsbereiche sind alarm- und videoüberwacht
Räume mit Servern sind alarm- und videoüberwacht
Maßnahmen gegen einfaches Mithören und Einsichtnahme (insb. bei Kundenempfang, Shared Spaces oder mobilem Arbeiten)
Akten- Festplattenvernichtung ausschließlich durch zertifizierten Dienstleister über breitgestellte Entsorgungstonnen
In Serverräumen ist Hardware durch verschlossene Racks, verschlossene Schränke gesichert
Unverzügliche Abarbeitung der Alarm- /Incidentmeldungen nach Incidentplan des ISMS

1.2 Schutz des Systemzugangs

Verpflichtende Verwendung starker Passwörter nach aktuellen Empfehlungen (BSI)
Passwörter werden nicht im Klartext gespeichert
Passwörter werden nach dem Stand der Technik gehashed gespeichert
Veröffentlichung von Passwortregeln für Mitarbeiter (Pflicht zur Nutzung des

Passwortmanagers, Verbot der Weitergabe, Verbot der Mehrfachverwendung)
Passwörter werden nach einem Sicherheitsvorfall, auch bei Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden
Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer
Automatische Sperrung des Zugangs bei zu vielen Fehlversuchen
Zeitverzögerungen zwischen mehrmaligen Login-Versuchen
Berechtigungskonzept und Geräteverwaltung für IT-Endgeräte
Berechtigungskonzept für IT-Applikationen/IT-Systeme
Weitere Interaktionen mit dem IT-System sind nur nach einer erfolgreichen Authentifizierung möglich
Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikobewertung getroffen und mögliche Angriffsszenarien wurden berücksichtigt
Einsatz von Zwei- oder Mehr-Faktor-Authentifizierung bei Systemzugängen zu kritischen Inhalten und Admin-Konten
Für die Admin-Konten der IT-Systeme werden ausschließlich starke Passwörter verwendet
Implementierung eines zentralen Systems zur Verwaltung von Benutzeridentitäten (Identity and Access Management System)
Eine Segmentierung der genutzten Netze ist definiert
Regeln und Verfahren zur Netzwerksegmentierung sind definiert und umgesetzt

1.3 Berechtigungsmanagement

Es werden nur eindeutige und personalisierte Benutzerkonten verwendet
Rollen- und Rechtekonzept für IT-Applikationen/IT-Systeme sind dokumentiert und umgesetzt
Zugriffsberechtigungen nur gemäß Erforderlichkeitsprinzip („Need-to-Know“) und mit den geringsten möglichen Rechten („Least Privilege“)
Regelmäßige Überprüfung der Berechtigungen der Systeme
Berechtigungsprüfung und Kontrolle der Zugangsbefugnisse aller Benutzer erfolgt auch innerhalb eines IT-Systems
Revisionssichere Dokumentation von Benutzerberechtigungen
Die Einrichtung von Benutzerkonten unterliegt einem Genehmigungsprozess nach dem 4-Augen-Prinzip
Die Nutzung von Gruppenkonten ist geregelt (und nur in Ausnahmefällen möglich wenn auf Nachvollziehbarkeit der Nutzeraktivität verzichtet werden kann)
Veränderungen der Zuständigkeiten/Arbeitsverhältnisse von Mitarbeitern führen zu umgehender Anpassung der Zugänge und Rechte
Protokollierung des schreibenden Zugriffs (inkl. Löschung/Überschreiben)
Protokollierung von unberechtigten Zugriffsversuchen
Regelmäßige Auswertung der Protokollierung
Anlassbezogene Auswertung der Protokollierung
Ein Management-Prozess (Genehmigung/Änderung/Löschung) für privilegierte Benutzerkennungen ist dokumentiert und etabliert
Benutzerkonten mit privilegierten Rechten sind dokumentiert und werden regelmäßig überprüft

1.4 Verschlüsselung und Pseudonymisierung

Die elektronische Übermittlung von personenbezogenen Daten erfolgt verschlüsselt
Die Speicherung von personenbezogenen Daten erfolgt verschlüsselt
Alle Daten auf mobilen Rechner und Speichermedien werden verschlüsselt
Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem Stand der Technik
Für die relevanten IT-Systeme ist die Verwaltung des Schlüsselmaterials definiert und dokumentiert
Transportverschlüsselung wird ausschließlich Ende-zu-Ende implementiert
Ein Regelwerk mit Anforderungen an Verschlüsselungsstärke, -algorithmus und Verwaltung der Schlüssel ist implementiert
Pseudonymisierung personenbezogener Daten wo möglich
Pseudonymisierung durch Zuordnungstabellen, diese sind von der übrigen Datenverarbeitung getrennt

2. Integrität der Systeme und Dienste

2.1 Schutz der Datenübertragung

Klassifikation von Daten und Definition von Schutzmaßnahmen
Einsatz von PGP als digitales Signaturverfahren zur Sicherung der Authentizität von Datenübertragungen
Beschränkung der Befugnisse der Mitarbeiter zur Datenübertragung
Anbindung von Homeoffice nur über VPN-Verbindungen
Regelmäßige Kontrolle der zulässigen Empfänger
Bei Massen-E-Mailversand wird die Offenlegung aller Empfänger technisch oder organisatorisch verhindert
Durchführung von Protokollierungen einer elektronischen Datenweitergabe oder Übermittlung
Durchführung von Plausibilitäts-, Vollständigkeits- und Richtigkeitsprüfungen

2.2 Eingabekontrolle

Protokollierung der Eingaben von und Änderungen an personenbezogenen Daten
Regelmäßige (anlasslose) Auswertung der Log-Dateien zur Erkennung von ungewöhnlichen Eingaben
Organisatorisch festgelegte Zuständigkeiten für die Eingabe

2.3 Weitere Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste

Härtungsmaßnahmen werden umgesetzt (z.B. Einschränkung/Deaktivierung nicht notwendiger Berechtigungen, Ports, Protokolle, Server)
Umsetzung der Mandantentrennung durch Trennung auf Datenebene
Beschreibung der Umsetzung der Mandantentrennung
Gemeinsam genutzte virtuelle Maschinen und/oder Applikationsinstanzen sind entsprechend gehärtet

Eine Separierung von Daten, Applikationen, Betriebssystem, Storage und Netzwerk ist umgesetzt
Es erfolgt eine automatische Überprüfung von empfangenen Dateien und Programmen vor deren Ausführung auf Schadsoftware (On-Access-Scan)
Es erfolgt eine regelmäßige Untersuchung des gesamten Datenbestandes aller Systeme auf Schadsoftware
Data Loss Prevention Lösungen werden eingesetzt

3. Verfügbarkeit der Systeme und Dienste

3.1 Sicherung der Verfügbarkeit personenbezogener Daten

Vorhandensein von redundanten IT-Systemen (Endgeräte, Server, Produktivsystem, Entwicklungssystem)
Unterbrechungsfreie Stromversorgung (USV)
Technische Schutzeinrichtungen für Brandschutz, Energieversorgung, Klimatisierung
Serverräume verfügen über Feuer- und Rauchmeldeanlagen
Serverräume verfügen über Feuerlöscher
Serverräume verfügen über Anlagen zur Überwachung von Temperatur und Feuchtigkeit
Regelmäßige Kontrollen des Systemzustandes (Monitoring)
Vorhandensein von divers ausgelegten IT-Systemen (gleiche Funktionalität von unterschiedlichen Herstellern)
Durchführung von regelmäßigen Bestandskontrollen für Ausdrucke und Datenträger

3.2 Löschung

Umsetzung von durch den Auftraggeber festgelegten Löschfristen für dessen Daten (Löschkonzept)
Definition und Dokumentation von Verfahren zur Entsorgung und Vernichtung von Datenträgern
Dokumentation eines Löschkonzeptes für die Auftragsverarbeitung
Umsetzung von Regelungen zur Entsorgung von Speichermedien
Integritätskontrolle bei Löschungen bzw. Löschroutinen
Umgesetzte Löschung auf Entwicklungs-, Test- und Produktivumgebungen
Aktenvernichter/-schredder (mind. Stufe 3, cross cutting) für Papierdokumente
Externer Aktenvernichter (DIN 32757)

4. Belastbarkeit der Systeme und Dienste

4.1 Absicherung gegen Störungen

Virenscanner mit aktuellen Suchmustern (mind. tagesaktuell) auf allen Endgeräten
Patch Management Prozess vorhanden (u.a. Update-Plan für die eingesetzte Software)
Redundant ausgelegte IT-Systeme
Einsatz von Firewall Systemen (z.B. am zentralen Übergang ins Internet, Absicherung von Datenbanken auf Webservern)

Geregelter Prozess zur ordnungsgemäßen Konfiguration von Firewall-Systemen, einschl. Freigaben/Ausnahmen
Datenspeicherung in einem RAID-System
Intrusion Detection Systeme
Intrusion Prevention Systeme
Maßnahmen zur Steigerung der Fehlertoleranz von Systemen und Diensten
Bei Websites und Webanwendungen: Content-Security-Policy (CSP) ist definiert und umgesetzt

4.2 Wiederanlauf und Wiederherstellung der Verfügbarkeit

Schriftlich fixiertes Backup-Konzept (regelmäßige Datensicherungen)
Geeignete physische Aufbewahrung von Backup-Medien (räumliche Trennung)
Geeigneter Schutz von Backups vor Verschlüsselung durch Ransomware
Wiederanlaufkonzept (Maßnahmen zur unverzüglichen Wiederherstellung der Verfügbarkeit bei Systemausfall)
Dokumentiertes und getestetes Notfall-Betriebskonzept (IT-Service Continuity)
Dokumentiertes und etabliertes Business Continuity Management

5. Organisatorische Schutzmaßnahmen

5.1 Organisatorische Sicherheitsmaßnahmen

Die Rollen und Verantwortlichkeiten im Bereich der Datensicherheit sind beschrieben, besetzt und intern bekannt
Implementierung eines Informationssicherheitsmanagement-Systems nach ISO 27001
Sicherheitsrichtlinien für den Umgang mit Informationen sind definiert, von der Geschäftsleitung verabschiedet und den Mitarbeitern kommuniziert
Existenz eines Incident Management (Meldung und Reaktion auf Sicherheitsverletzungen)
Es existiert eine Angriffserkennung und Meldungsmöglichkeiten (Incident-Responce)
Schriftlich dokumentierter Change Management Prozess für IT-Systeme die personenbezogene Daten im Kontext diese Vertrages verarbeiten
Informationen über technische Schwachstellen zu den genutzten Systemen und Software (Assets) werden gesammelt und hinsichtlich Auswirkungen bewertet
Angemessene Reaktion auf identifizierte technische Schwachstellen (z.B. Abschaltung/ Abtrennung von Services und Systemen, Monitoring, Anpassen von Firewalls)
Awarenessmaßnahmen für alle Anwender bezüglich Datenschutz und Datensicherheit
Schulungsmaßnahmen und eigene geeignete Fortbildung im Datenschutz und Informationssicherheit
Klassifizierung aller Informationen nach ihrem Schutzbedarf (hinsichtl. Vertraulichkeit, Verfügbarkeit, Integrität)
Trennung von Produktivsystemen und Entwicklungs-/Testsystemen
In der Test- und Entwicklungsumgebung werden nur synthetische Daten, also keine Echtdaten oder personenbezogene Daten verarbeitet
Verbot der Ablage personenbezogener Daten in Source Code (Repositories)
Regelung zur mobilen/privaten Nutzung von Endgeräten (z.B. Smartphones, Note-

books) durch Mitarbeiter sind getroffen
Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme (z.B. Audits durch IT-Sicherheit oder Datenschutzbeauftragten)
Prozess zur regelmäßigen Überprüfung der Wirksamkeit aller Schutzmaßnahmen und gegebenenfalls deren Anpassung zur Gewährleistung der Sicherheit der Verarbeitung (PDCA-Zyklus)

5.2 Auftragskontrolle

Dokumentation aller Unterauftragsverarbeiter, die für die Verarbeitung der in diesem Vertrag beschriebenen personenbezogenen Daten eingesetzt werden
Es existiert ein Qualitäts-Management System bei den relevanten Unterauftragsverarbeitern, das die Auftragsverarbeitung vollständig abdeckt
Es existiert ein Informationssicherheits-Management System (ISMS) bei den relevanten Unterauftragsverarbeitern, dass die Auftragsverarbeitung vollständig abdeckt
Regelmäßige Kontrolle der relevanten Unterauftragsverarbeiter durch Prüfung der Verträge mit Unterauftragsverarbeitern
Vorhandensein von Richtlinien und Arbeitsanweisungen für die Verarbeitung im Auftrag