Technische und organisatorische Maßnahmen des Mensch und Maschine Konzerns

gem. Art. 25 Abs. 1 und Art. 32
Datenschutz-Grundverordnung (DSGVO)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten, die sich den IT-Systemen, Datenverarbeitungsanlagen sowie den vertraulichen Akten und Datenträgern physisch nähern.

Die Zutrittskontrollen an den Standorten sind nicht einheitlich. Die individuellen Maßnahmen der einzelnen Standorte finden sich unter „5. Übersicht der Zutrittskontrollen an den einzelnen Standorte“.

Allgemein gültige Regelungen zur Zutrittskontrolle:

elektronische Zutrittskontrollsysteme: Zutrittsprotokollierung: Die Speicherung von Öffnungs- und Schließereignissen erfolgt für den Zeitraum von 6 Monaten. (i.d.R. nur bei elektronischer Zutrittskontrolle)

Schlüsselvergabe: Die Ausgabe von jeglichen Schlüsseln wird dokumentiert und quittiert. Schlüssel werden ausschließlich an festangestellte Mitarbeiter ausgegeben, die regelmäßig am Standort tätig sind.

Besucherregelung: Besucher dürfen sich nur in ständiger Begleitung eines Mitarbeiters in den Geschäftsräumen aufhalten.

IT-Räume und technische Versorgungsräume: sind entsprechend einer verbindlichen Schließregelung stets verschlossen zu halten.

Lokal vorhandene Serverräume mit Netzwerkhauptverteilsystemen (insbesondere Switches), sind sowohl in verschlossenen Räumen als auch in abgesperrten Server-Racks platziert. Zutritt haben ausschließlich das IT-Personal und im Notfall Wachdienst und Feuerwehr.

Der Zutritt zum Rechenzentrum (ISO/IEC 27001 zertifiziertes ISMS) erfolgt mit einem separaten Zylinder-Schlüsselsystem. Zutritt haben ausschließlich IT-Mitarbeiter.

1.2 Zugangskontrolle

Das Eindringen Unbefugter in die Datenverarbeitungssysteme ist zu verhindern. Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Regelung der Benutzerberechtigung. (differenziertes Berechtigungskonzept für Systeme, Anwendungen und Daten, für normale und privilegierte Nutzer)
- Alle Benutzerkonten werden zentral im Active Directory angelegt und verwaltet.
- Single-Sign-On-Verfahren mit MFA
- Ausschließlich personalisierte Benutzerkennungen, keine Gruppen-Accounts.
- Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität.
    - Verwendung von individuellen Passwörtern.
    - Sichere Passwörter werden vom System technisch erzwungen, die letzten 5 Passwörter können nicht mehr verwendet werden.
    - Initial-Passwörter und zurückgesetzte Passwörter müssen in gleicher Weise geschützt werden und sind zusätzlich vom Nutzer unverzüglich zu ändern.

    - Speicherung von Passwörtern ausschließlich in verschlüsselter Form. Verpflichtender Einsatz einer freigegebenen Passwort-Manager Software. (z.B. Bitwarden)
    - Automatische Sperrung von Nutzer-Accounts nach mehrfacher Fehleingabe von Passwörtern.
- 2-Faktor-Authentifizierung mittels Authenticator-App für den Zugriff auf sämtliche M365 Anwendung. (unabhängig ob per lokaler App oder Webapp)
- Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität.
- Beschränkung der Zahl der Administratoren auf ein Minimum. Mitarbeiter verfügen nicht über lokale Admin-Konten.
- Netzwerksegmentierung mittels VLANs
- Schutz der IT-Anlagen mit Perimeter-Firewall
- Nutzung eines Intrusion Detection and Prevention Systems
- WLAN-Authentication mittels RADIUS (Protokollierung der Anmeldungen)
- Prozess zur Rechtevergabe und -entzug bei Neueintritt oder Austritt von Mitarbeitern
- Verpflichtung auf das Datengeheimnis
- Regelungen zum mobilen Arbeiten (VPN, MFA, Gerätesicherheit)
- Betriebsordnung „Mobiles Arbeiten“
- Clean-Desk-Policy
- Kontrollierte Vernichtung von Datenträgern

1.3 Zugriffskontrolle

Unerlaubte Tätigkeiten in Datenverarbeitungssysteme außerhalb eingeräumter Berechtigungen sind zu verhindern. Bedarfsorientierte Ausgestaltung des Berechtigungs-konzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Berechtigungskonzept. Vergabe, Entzug und Änderungen von Berechtigungen (On-, und Offboarding- und Wechselprozesse) nach dokumentierten Antrags- und Genehmigungsverfahren.
- Differenzierte Berechtigungen (Rollenkonzept nach Need-to-Know-, bzw. Least-Privilege-Prinzip)
- Protokollierung des Zugriffs auf personenbezogene Daten, sofern technisch möglich.
- Schadsoftware-Scanner (Malware-Schutz) auf allen Mitarbeitergeräten (Sophos Virenscanner) Zentrales Reporting aller Angriffe von innen und außen.
- Sophos Virenscanner auf allen Servern.
- Schadsoftware-/Spam-Filterung für E-Mails
- Firewall-Konfiguration nach Default-Deny-Prinzip. Freischaltung nur von, zur Aufgabenerfüllung notwendiger, Ports.

1.4 Trennbarkeit

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Logische Mandantentrennung (z.B. auf Basis von Kundennummern)
- Trennung von Entwicklungs-, Test- und Produktivsystem

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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:

- Datenmaskierung gemäß interner „Richtlinie zur Datensicherheit“

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Fernzugriff via IPSEC-VPN
- Sichere Übertragung vertraulicher und personenbezogener Daten via SSL, TLS (Version 1.2 oder höher) oder IPSEC-VPN.
- Verschlüsselter E-Mail-Versand zwischen den Servern (TLS-Verschlüsselung)
- Aufbewahrungskonzept für personenbezogene Daten
- Kontrollierte Vernichtung von Daten Papier, Datenträger durch zertifizierte Entsorger.
    - Akten, CDs und DVDs - physische Zerstörung
    - Festplatten - mechanische Zerstörung
- interne Aktenvernichter der Stufe P-4, gemäß DIN 66399-2
- Umfangreiche Protokollierung (Drucker, Firewall-Logs)

2.2 Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt worden sind:

- Nutzung ausschließlich personalisierter Benutzerkennungen.
- Alle Benutzerkonten werden zentral im Active Directory angelegt und verwaltet.
- Verwaltung der Zugriffe für das CRM-System (Salesforce)
- Protokollierung jeder Veränderung (inkl. Administrator-Tätigkeiten) von personenbezogenen Daten, sofern technisch möglich.
- Verpflichtung auf das Datengeheimnis

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

3.1 Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung. Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- ISMS des Rechenzentrumsbetreibers nach ISO/IEC 27001 zertifiziert.
- Ausschließliche Nutzung und Installation von freigegebener Software und Softwareversionen. (Freigabe durch die IT)
- Separate Backup-Konzepte für unterschiedliche Bereiche:
    - **Komplettsystem:** Nächtliche Voll-Backups auf separates Speichersystem. 12 Wochen Vorhaltezeit
    - **M365 Umgebung:** Nächtliche Voll-Backups zu separaten Backupanbietern in der Cloud.
    - **SQL-Datenbanken:** Stündliche Inkrementell-Backups und nächtliche Voll-Backups auf Festplatten
- Automatische Updates
- Redundante Datenhaltung im Rechenzentrum
- Klimatisierte Serverräume. Klimaanlagen sind redundant ausgelegt.
- Unterbrechungsfreie Stromversorgung (USV) in Serverräumen
- Brandschutz:
    - Einsatz wasserloser Brandlöschmittel (z.B. C02-Löscher)

    - Brandmeldeanlage mit Brandfrüherkennungssystem und Aufschaltung auf eine Brandmeldezentrale
    - brandhemmende Wände und Türen (T90) im Serverbereich
    - keine Brandlasten im Serverbereich
- Notfallpläne
- Regelmäßige Schulung und Sensibilisierung der Mitarbeiter.

3.2 Verschlüsselung

- Verschlüsselung bei Übertragung über Funk-Netzwerke (WLAN)
- Verschlüsselung bei Übertragung via internetbasierter Kommunikation (E-Mail)
- Verschlüsselung von Online-Diensten (HTTPS)

3.3 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Nutzung einfacher Sicherungsverfahren
- Einsatz redundanter Hardwarekomponenten
- Einsatz virtueller Server
- Regelmäßiges Testen der Wiederherstellbarkeit der Daten
- Notfallpläne

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

- Datenschutzmanagement
- Informationssicherheitsmanagement
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auswertung von Protokollen auf sicherheitsrelevante Ereignisse und Alarmierung bei potenziellen Hackerangriffen oder Verstößen gegen die Richtlinien.
- Regelmäßige Penetrationstests
- Regelmäßige Durchführung von netzwerkbasierten Sicherheits-Scans

4.1 Auftragskontrolle

Technische und organisatorische Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer. Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers:

- Abschluss von Verträgen zur Auftragsdatenverarbeitung (AV-Verträge) gemäß gesetzlicher Vorgaben. (Art. 28 DSGVO)
- Vereinbarung aller vorgeschriebenen Kontrollrechte.
- Vertragliche Verpflichtung von Unterauftragnehmern (sofern vorhanden) im gleichen Umfang, wie der Auftragnehmer selbst.
- Zentrale Erfassung vorhandener Auftragsverarbeitungsverhältnisse.
- Technische und organisatorische Maßnahmen des Auftragnehmers unterliegen einer regelmäßigen Prüfung durch den Auftraggeber.

5. Übersicht der Zutrittskontrollen an den einzelnen Standorte

Maßnahme	Gesellschaft und Standorte																										
	Mensch und Maschine Deutschland GmbH																OPEN MIND Technologies AG				Mensch und Maschine acadGraph GmbH				MuM Mechatronik GmbH	MuM Infrastruktur GmbH	MuM At Work GmbH
	Wessling	Bad Krozingen	Bissendorf	Dortmund	Düren	Friedrichshafen	Hamburg	Hannover	Kirchheim unter Teck	Limburg	Nürnberg	Saarbrücken	Schotten	Wiehl	Wiesbaden	Velbert	Wessling	Füssen	Hannover	Ludwigsburg	Borken	Dortmund	Leipzig	München	Donzdorf	Ditzingen	Bissendorf
Perimeterschutz (Zäune, Mauern, Schranken, Tor)	x		x		x		x	x				x				x	x		x						x		x
Einbruchsmeldeanlage mit aufgeschaltetem Wachdienst	x		x		x												x		x						x		x
GSM-Alarmanlage																x											
Zugang zu den Geschäftsräumen über mechanische Schlüssel	x	x			x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Verantwortliche Person für die Schlüsselvergabe + Schlüsselliste	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
elektronisches Zutrittskontrollsystem	x		x	x	x			x							x	x	x		x		x					x	x
Besetzter Empfang (während der Geschäftszeiten)	x		x		x	x		x		x			x				x										x
Protokollierung von Besuchern	x																x										
Besucherausweise	x																x										
Eingangsbereiche im Blickfeld von Mitarbeitern		x								x		x	x		x	x						x					x
Büros bei Abwesenheit verschlossen		x	x	x			x	x		x			x	x		x		x	x			x	x	x			