Technisch-organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Unternehmen: **mint software GmbH** Stand (Datum): 15.01.2024
Bearbeiter (Name, Position, Kontakt): Maximilian Stein, Geschäftsführer, max.stein@mmmint.ai

Vertraulichkeit (Art. 32 Abs. 1 b DS-GVO)	**Vorhandene Maßnahmen**
Zutrittskontrolle *(Maßnahmen, die gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen im Unternehmen verwehrt wird)*	
Schließanlage zur Sicherung des Betriebsgeländes und -gebäudes (verschließbare Tore, Türe, Fenster usw.)	X
Besucherregelung, die den Zutritt zu Büroräumlichkeiten für Unbefugte verhindert (z.B. durch An-/Abmeldung am Empfang, Besucherbuch, Besucherausweis, Begleitung auf dem Betriebsgelände durch Mitarbeiter)	
Schutz vor Einbruch (z.B. durch Alarmanlage, Werkschutz, Videoüberwachung außerhalb/innerhalb des Gebäudes, Bewegungsmelder)	X
Festgelegte Sicherheitsbereiche (z.B. Bereiche, die für Unternehmensfremde nicht zugänglich sind; Bereiche, die nur einem eingeschränkten Mitarbeiterkreis zugänglich sind, wie z.B. Serverraum, Büro der Personalabteilung)	
Sonstiges (bitte beschreiben):	
Vertraulichkeit (Art. 32 Abs. 1 b DS-GVO)	**Vorhandene Maßnahmen**
Zugangskontrolle *(Maßnahmen, die gewährleisten, dass Unbefugten der Zugang und somit die Nutzung von Datenverarbeitungsanlagen verwehrt wird)*	
Zugangsdaten für Hardware (z.B. zur Nutzung der Hardware (PC, Laptop) sind individuelle Anmeldedaten (Benutzername und Passwort) erforderlich)	X
Zugangsdaten für Software (z.B. zur Nutzung der Systeme/Software sind individuelle Anmeldedaten (Benutzername und Passwort) erforderlich)	X
Sichere Passwörter (z.B. Richtlinie und Prozess zur Verwendung sicherer Passwörter und zur regelmäßigen Aktualisierung der Passwörter; Mindestanforderungen bzgl. der Passwortkomplexität (Mindestanzahl an Zeichen, Groß-/Klein, Sonderzeichen); Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passwortes; Automatische Passwortrücksetzung nach drei Anmeldefehlversuchen; systemseitige Erinnerung zum Passwortwechsel nach drei Monaten; Zwangs- oder Pflicht-Änderung der Kennwörter nach der ersten Anmeldung; Ablauf von Benutzerpasswörtern)	X
Sicherung des Serverraums (z.B. mittels gesondertem Schließsystem, Zugangsbeschränkung derart, dass der Zutritt nur einem beschränkten Mitarbeiterkreis möglich ist; externer technischer Support wird bei der Arbeit am Server stets von Mitarbeitern beaufsichtigt)	X
Warnsystem bei Hackerangriffen (z.B. Verwendung von Software, die Angriffe von außerhalb erkennt und den Nutzer oder Administrator warnt)	X
Verschlüsselung bei der Datenspeicherung (z.B. personenbezogene Daten gemäß dem neuesten Stand der Technik verschlüsseln und gegen Diebstahl, Manipulation oder Zerstörung schützen)	X
Nicht benötigte physikalische Schnittstellen an PCs und Laptops (USB, DVD, etc.) sind deaktiviert	
Portregeln/Sperrung von nicht erforderlichen Ports	

Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar) möglich	
W-LAN Verschlüsselung	X
Software-Firewall	X
Antivirus-Software auf allen Systemen	
Verschlüsselung von Netzwerken	X
Automatische Bildschirm- und Computer-Sperre bei Inaktivität	X
Regelmäßige Software-Updates	X
Verschlüsselte Speicherung von Passwörtern	X
Überwachung und Protokollierung von administrativem Systemzugang und von Konfigurationsänderungen	X
Dokumentierter User-Login-Verlauf	X
Regelmäßige Überprüfung der Systemzugangsberechtigungen durch Administratoren	X
Sonstiges (bitte beschreiben):	
Vertraulichkeit (Art. 32 Abs. 1 a, b DS-GVO)	**Vorhandene Maßnahmen**
Zugriffskontrolle *(Maßnahmen, die den Zugriff auf Daten durch Unbefugte verhindern sowie Informationen vor unerlaubter Kenntnisnahm, Veränderung oder Löschung schützen)*	
Rollenbasierte Berechtigungskonzepte (z.B. Zugriffsberechtigungen der Mitarbeiter sind auf das erforderliche Minimum zu beschränken; Nur diejenigen Mitarbeiter, die die Daten zur Erfüllung ihrer Aufgaben unbedingt benötigen, erhalten gemäß des Need-to-Know-Prinzips Zugriffsberechtigung)	X
Dokumentation der Vergabe von Zugriffsrechten/Rollen/Profilen und Genehmigungsroutine / Prozess zur Vergabe von Berechtigungen	X
Protokollierung von Datenverarbeitungen (z.B. Verarbeitung, Veränderung, Löschung von Daten wird dokumentiert und somit nachvollziehbar gemacht, wann welcher Nutzer zu welchem Zweck Umgang mit den Daten hat)	X
Clean-Desk-Prinzip (z.B. Papierdokumente und mobile Datenspeicher werden in (abschließbaren) Möbeln aufbewahrt)	X
Schriftliche Verpflichtung aller Mitarbeiter auf das Datengeheimnis (z.B. bezugnehmend auf Art. 5, Abs. 2, DS-GVO, § 53 BDSG)	X
Geregeltes Löschen / Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks sowie papiergebundenen Daten/Akten (z.B. Löschung von Datenträgern durch IT-Abteilung; Vernichtung von Datenträgern durch Entsorgungsunternehmen gegen Ausstellung eines Vernichtungszertifikats; Vernichtung von physikalischen Medien nach DIN 66399/Sicherheitsstufe 3 Aktenvernichter)	
Pseudonymisierung von Daten (z.B. bestimmte Datenarten werden pseudonymisiert; innerhalb bestimmter Systeme werden eingegebene Daten pseudonymisiert)	X
Verbot von nicht autorisierten Software-Installationen (z.B. im Rahmen einer IT-Richtlinie; Anweisung, dass Software ausschließlich von Systemadministratoren installiert werden darf)	
Sonstiges (bitte beschreiben):	
Vertraulichkeit (Art. 32 Abs. 1 a, b DS-GVO	**Vorhandene Maßnahmen**
Trennungskontrolle *(Maßnahmen, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden)*	

Logische Datentrennung (z.B. separate Datenbanken oder strukturierte Dateiablage; Nutzung unterschiedlicher physischer und virtueller Systeme mit eigenständigen Betriebssystemen oder Datenbanken, für deren Nutzung Anwender unterschiedliche Rechte erhalten)	X
Für pseudonymisierte Daten: Speicherung der Zuordnungsdatei auf einem separaten IT-System	X
Die Daten der verschiedenen Kunden / Projekte werden so weit wie möglich von verschiedenen Mitarbeitern bearbeitet (Trennung nach Zugriffsregelungen/Zugriffsberechtigungen)	X
Sonstiges (bitte beschreiben):	
Integrität (Art. 32 Abs. 1 b DS-GVO)	**Vorhandene Maßnahmen**
Weitergabekontrolle *(Maßnahmen, die gewährleisten, dass bei der Weitergabe von Daten ein unberechtigter Zugriff, unbefugte Kenntnisnahme oder unbeabsichtigter Abfluss verhindert wird)*	
Verschlüsselung von Daten während der Übertragung (end-to-end-Verschlüsselung)	X
Verschlüsselung von E-Mails (z.B. E-Mail-Verschlüsselungsverfahren nach dem aktuellen Stand der Technik; Passwortschutz einzelner Dokumente oder Dateien und separate Übermittlung des Passwortes)	
Anonymisierung/Pseudonymisierung (z.B. vor der Weitergabe personenbezogener Daten werden diese anonymisiert oder pseudonymisiert)	
Verschlüsselung von Hardware und Datenträgern (z.B. Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops, etwa per Betriebssystem, True Crypt, Safe Guard, WinZip, PGP)	X
Protokollierung aller digitalen Übertragungsvorgänge	
Protokollierung von externen Support-Prozessen und Fernwartung	
Getunnelte Datenverbindung (VPN = Virtual Private Network)	
SSL-Verschlüsselung bei Web-Access	X
Gesichertes W-LAN	X
Verbot der Nutzung von privaten Datenträgern zwecks Datentransport	X
Regelung zur Verwendung von FAX- und Multifunktionsgeräten (z.B. Leeren des Zwischenspeichers bei Multifunktionsgeräten bei Verwendung der Scan to Mail Funktion; Anweisung, dass Mitarbeiter sich beim Versenden von FAX-Nachrichten den korrekten Empfang bestätigen lassen)	
Sonstiges (bitte beschreiben):	
Integrität (Art. 32 Abs. 1 b DS-GVO)	**Vorhandene Maßnahmen**
Eingabekontrolle *(Maßnahmen, die eine nachträgliche Überprüfung ermöglichen, wann und von wem personenbezogene Daten in Systemen eingegeben, verändert oder gelöscht wurden)*	
Protokollierung der Datenverarbeitung (z.B. einzelne Datenverarbeitungssysteme protokollieren, wer, wann, welche Daten eingegeben, verändert oder gelöscht hat; Protokolle der Datenverarbeitung werden kontinuierlich auf Unregelmäßigkeiten überprüft; Protokolle der Datenverarbeitung werden für einen angemessenen Zeitraum aufbewahrt und im Anschluss datenschutzkonform gelöscht)	X
Rollenabhängige Zugriffsbeschränkungen (z.B. Zugriffsrechte, funktionelle Verantwortlichkeiten für einzelne Systeme)	X
Verwendung eines Schreibschutzes, der (unbeabsichtigtes) Überschreiben oder Löschen von Daten verhindert	X
Protokollierung von administrativen Änderungen (Protokollierungssoftware)	X

Sonstiges (bitte beschreiben):	
Auftragsverarbeitung (Art. 28 und Art. 32 Abs. 4 DS-GVO)	**Vorhandene Maßnahmen**
Auftragskontrolle *(Maßnahmen, die gewährleisten, dass Daten, die im Auftrag verarbeitet werden, ausschließlich gemäß den Vorgaben des Auftraggebers verarbeitet werden)*	
Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers (z.B. in Folge von Regelungen im Auftragsverarbeitungsvertrag zwischen Auftraggeber und Auftragnehmer)	Regelungen zur Schließung von Auftragsverarbeitungs-verträgen wurden von DSB eingeführt
Regelmäßige Kontrolle externer Dienstleister (z.B. bzgl. der Einhaltung und Optimierung technisch-organisatorischer Maßnahmen; Verpflichtung von Subdienstleistern)	Wird durch DSB angeregt
Regelmäßige Datenschutz-Unterweisung der Mitarbeiter (Schulungen)	Wird vom DSB durchgeführt
Verpflichtung der Mitarbeiter auf das Datengeheimnis (z.B. gem. Art. 5 Abs. 2 DS-GVO / § 53 BDSG)	Wird vom DSB initiiert
Auswahl externer Dienstleister anhand von Datenschutzgesichtspunkten (z.B. Dienstleister, die im Auftrag personenbezogene Daten verarbeiten, werden vor Beauftragung sorgfältig ausgewählt nach Kriterien des Datenschutzes und mittels Auftragsverarbeitungsvertrag oder Vertraulichkeitsvereinbarung zur Einhaltung des Datenschutzes verpflichtet)	Wird vom DSB initiiert
Übersicht externer Dienstleister, die im Auftrag personenbezogene Daten verarbeiten oder (potentiellen) Zugriff auf diese haben (z.B. regelmäßige Pflege der Übersicht externer Dienstleister und Prüfung, ob eine schriftliche Regelung zum Datenschutz notwendig ist, z.B. Auftragsverarbeitungsvertrag, Vertraulichkeitsvereinbarung)	Wird vom DSB initiiert
Sonstiges (bitte beschreiben):	
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b, c DS-GVO)	**Vorhandene Maßnahmen**
Verfügbarkeitskontrolle *(Maßnahmen, die gewährleisten, dass personenbezogene Daten vor (zufälliger) Zerstörung und Verlust geschützt sind)*	
Unterbrechungsfreie Stromversorgung (insbesondere für Server)	X
Feuer und/oder Rauchmelder, Feuerlöschanlage und/oder Rauchmelder (z.B. im Serverraum)	X
Kühlsystem im Rechenzentrum / Serverraum	X
Geografisch getrennte Rechenzentren	X
Redundante Infrastruktur mit Backup-Systemen	X
Disaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust	X
Back-Up-Konzept (z.B. Konzept zur regelmäßigen Datensicherung, das die Sicherungsmethode und die Häufigkeit der Sicherung definiert)	X
Spiegelung von Festplatten	X
Tägliche inkrementelle Datensicherung	X
Wöchentliche vollständige Datensicherung	X
Wöchentliche Back-Ups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen	X
Unterscheidung zwischen Archivierung und Backup	X
Geeignete Archivierungsräumlichkeiten	X

Notfallplan (z.B. schriftliches Konzept, das festlegt, wie im Falle von Zerstörung oder Beschädigung von Datenverarbeitungsanlagen der Geschäftsbetrieb aufrechterhalten werden kann)	X
Tests der IT-Systeme und IT-Infrastruktur (z.B. regelmäßige Notfalltests; Penetrationstests; regelmäßige Übungen, in denen Notfallsituationen, z.B. durch Wasser oder Feuer, simulieren und die Wiederherstellung der Daten getestet werden)	X
Externe Audits und Sicherheitstests	X
Sonstiges (bitte beschreiben):	
Überprüfung, Bewertung, Evaluierung von Maßnahme (Art. 32 Abs. 1 d DS-GVO)	**Vorhandene Maßnahmen**
Kontrollverfahren *(Maßnahmen, die eine regelmäßige Überprüfung, Kontrolle und – sofern notwendig – Anpassung von Sicherungsmaßnahmen gewährleisten)*	
Regelmäßige Aktualisierung der Verzeichnisse von Verarbeitungstätigkeiten (VVT)	X
Regelmäßige Überprüfung der technisch-organisatorischen Maßnahmen	X
Regelmäßige Überprüfung von Datenverarbeitungsprozessen inkl. Dokumentation	X
Prozess zur Wahrung von Betroffenenrechte	X
Prozess zum Umgang mit Datenschutzvorfällen	X
Regelung zur Einbeziehung des Datenschutzbeauftragten bei der Implementierung neuer oder Änderung bestehender Datenverarbeitungsverfahren	X
Sonstiges (bitte beschreiben):	
Zertifizierungen und internationale Standards: *(Bitte Belege beifügen)*	**Vorhandene Testate**
Zertifizierung nach ISO 27001	
Zertifizierung nach ISO 27002	
Zertifizierung nach IDW PS 330	
Zertifizierung nach IDW RS FAIT 1	
Zertifizierung nach BSI-Standard 100-3 (Notfallmanagement)	
Datenschutzzertifikat / Datenschutzprüfsiegel (gemäß Art. 42 EU-DSGVO)	
Genehmigte Verhaltensregeln (gemäß Art. 40 EU-DSGVO)	
Verifizierte verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) (Gemäß Art. 47 EU-DSGVO)	
Sonstiges (bitte beschreiben):	