Allgemeine technisch organisatorische Maßnahmen

erstellt am

02.10.2025

gültig für folgende Organisation

OMM Solutions GmbH
Vor dem Lauch 19
70567 Stuttgart
Deutschland

1.1.1 Vertraulichkeit: Zutrittskontrolle

Bezeichnung	Letztes Audit
1.1.1.03 Zugängliche Fenster und Außentüren der Unternehmensräumlichkeiten sind einbruchssicher ausgeführt	15.07.2024
1.1.1.04 Eingangstüren zu Unternehmensgebäuden oder Räumen sind durch eine genormte Schließanlage gesichert (Sicherheitsschlösser, Chipkarten, Transponder, Codeschloss)	15.07.2024
1.1.1.05 Eingangstüren zu Unternehmensräumlichkeiten weisen neben Schließanlagen, zusätzliche Zutrittssicherungen auf (zb. Türknauf außen)	15.07.2024
1.1.1.06 Die Vergabe, Verlust und Rückgabe von Schlüsseln, Transpondern, Chipkarten oder Codes an Personen wird dokumentiert	15.07.2024
1.1.1.07 Der Einsatz von Chipkarten, Transpondern oder die Verwendung von Zugangscodes wird protokolliert (zb. Zeitpunkt, Ort der Verwendung, Key)	15.07.2024
1.1.1.09 Ein ständig besetzter Empfang verhindert den unbemerkten Zutritt von nicht berechtigten Personen	15.07.2024
1.1.1.10 Besucher:innen oder Personal von Fremdfirmen müssen sich beim Zutritt in eine Besucherliste eintragen oder werden vom Empfang in eine solche eingetragen	15.07.2024
1.1.1.11 Besucher:innen oder Personal von Fremdfirmen werden beim Verlassen des Unternehmens aus Besucherlisten ausgetragen (Zeitpunkt)	15.07.2024
1.1.1.14 Besucher:innen oder Personal von Fremdfirmen werden von Mitarbeiter:innen begleitet	15.07.2024
1.1.1.15 Die Unternehmensräumlichkeiten werden durch Wachpersonal oder einen Wachdienst gesichert	15.07.2024
1.1.1.16 Personal von Fremdfirmen das ständig Zugang zu den Unternehmensräumlichkeiten hat (Reinigungskräfte, Sicherheitskräfte, Wartungspersonal), wurde auf die Geheimhaltung verpflichtet	15.07.2024
1.1.1.19 Lichtschranken oder Bewegungsmelder lösen die Außenbeleuchtung von Unternehmensgebäuden aus	15.07.2024

1.1.2 Vertraulichkeit: Zutrittskontrolle (sensible Räume)

Bezeichnung	Letztes Audit
1.1..2.02 Der Zutritt zu Räumen in denen Personaldaten verarbeitet (zB. gelagert) werden, ist nur mit einem gesonderten Schlüssel, Key, Transponder, Chipkarte möglich	15.07.2024
1.1..2.04 Personalakten werden in verschließbaren Aktenschränken aufbewahrt	15.07.2024
1.1.2.01 Personaldaten werden in gesonderten Räumlichkeiten verarbeitet (zb. Personalbüro)	15.07.2024
1.1.2.03 Die Eingangstüren zu Räumen, in denen Personaldaten verarbeitet werden, verfügen über einen automatischen Schließ- und Sperrmechanismus oder werden beim Verlassen versperrt	15.07.2024
1.1.2.05 Bildschirme auf denen Personaldaten verarbeitet werden sind von außen (Fenster) oder innen (Glastüre oder Glasfront) nicht einsehbar	15.07.2024
1.1.2.15 In sensiblen Räumlichkeiten (Personal, Kundenverwaltung, IT) befinden sich keine Geräte, zu denen ein Benutzerkreis außerhalb der eigentlich Berechtigten Zugang benötigt (zB. Drucker)	15.07.2024

1.2 Vertraulichkeit: Zugangskontrolle

Bezeichnung	Letztes Audit
1.2.01 Das Gehäuse von Desktop Rechnern ist versperrt und kann nur von Personen geöffnet werden die den Schlüssel dazu verwahren	15.07.2024
1.2.02 Laptops oder Smart Devices (Ipad etc.) werden nach Dienstende versperrt aufbewahrt oder werden mit nach Hause genommen	15.07.2024
1.2.04 Das BIOS oder UEFI von Clients ist mit einem gesonderten Passwort gesichert	15.07.2024
1.2.05 Die Anmeldung an einem Client erfolgt durch personenbezogene Benutzeraccounts (Benutzername und Passwort oder ähnliche Verfahren (Gesichtserkennung, Fingerprint etc.))	15.07.2024
1.2.06 Die Benutzer:innen am Client Rechner hat keine Administrator Rechte bzw. für die tägliche Arbeit wird mit einem Benutzer:in ohne Administratorrechten gearbeitet	15.07.2024
1.2.07 Sammelaccounts oder unpersonalisierte Benutzerzugänge auf Clients (mehrere Benutzer teilen sich einen Zugang) existieren nicht	15.07.2024
1.2.08 Auf jedem verwendeten Client (Rechner) ist eine Firewall aktiv	15.07.2024
1.2.09 Auf jedem Client Rechner ist eine Antiviren Software installiert, diese wird täglich bzw. bei einer Neuanmeldung aktualisiert	15.07.2024
1.2.10 Eingehende Mails werden online am E-Mail Server (beim Hoster) auf Viren geprüft	15.07.2024
1.2.11 Eingehende Mails werden online am Mail Server (Hoster) auf Spam geprüft	15.07.2024
1.2.12 Auf jedem Client Rechner ist eine (Antiviren) Software installiert die beim Surfen im Internet entsprechenden Schutz (Webfilter) bietet	15.07.2024
1.2.13 Bei Routern ins Internet (WLAN Router) sind nur die absolut erforderlichen Ports freigeschaltet	15.07.2024
1.2.14 Der Zugang zum internen Netzwerk (WLAN) ist mit einem eigenen Passwort gesichert	15.07.2024
1.2.15 Der Zugang zu Systemen (Server, Software) von außerhalb des Unternehmens erfolgt über verschlüsselte Verbindungen (VPN, Zugriff via Citrix)	15.07.2024

Bezeichnung	Letztes Audit
1.2.16 Der Zugang zur Konfigurationsoberfläche des (WLAN) Routers wurde mit einem eigenen Benutzernamen und einem eigenen Passwort (ungleich Standard Benutzeraccount) gesichert	15.07.2024
1.2.17 Gäste erhalten über einen gesondertes WLAN Zugriff auf das Internet	15.07.2024
1.2.19 Eine Firewall ist auf jedem Übergang zum Internet aktiviert (Router)	15.07.2024
1.2.20 Wir setzen Systeme ein, die Zugriffsversuche oder Angriffe von betriebsfremden Personen identifizieren und/ oder verhindern können (Intrusion Detection System)	15.07.2024
1.2.21 Auf jedem Server und sonstigen Systemen bei denen ein Datenaustausch über das Internet erfolgt ist eine Antiviren Software installiert die täglich aktualisiert wird	15.07.2024
1.2.22 Mobile Endgeräte werden durch den Einsatz einer Antiviren Software geschützt	15.07.2024
1.2.23 Wir setzen eine zentrale Smartphone-Administrations-Software zum Deaktivieren von Smartphones bzw. zum Löschen von Daten auf Smartphones ein	15.07.2024
1.2.24 Bei Bildschirmen die in Räumlichkeiten eingesetzt werden, zu denen Kund:innen (Patienten:innen...) Zugang haben und personenbezogene Daten verarbeitet werden, wird darauf geachtet, dass der Bildschirm nicht eingesehen werden kann. Allenfalls existiert ein entsprechender Sichtschutz.	15.07.2024
1.2.25 Bildschirme werden automatisch bei Inaktivität gesperrt und können nur durch Eingabe des Benutzerpasswortes oder ähnliche Verfahren (Fingerprint, Gesichtserkennung, etc.) wieder entsperrt werden	15.07.2024

1.3 Vertraulichkeit: Zugriffskontrolle

Bezeichnung	Letztes Audit
1.13.15 Passwortmanagementsystem	-
1.3.01 Die Anzahl der Administratoren für Server und zentrale Software ist auf das „Notwendigste“ reduziert	15.07.2024
1.3.02 Jeder Administrator verfügt über einen eigenen Benutzeraccount und das Passwort weist eine ausreichende Komplexität auf (beinhalten Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern und sind dem Schutzbedarf angemessen).	15.07.2024
1.3.04 Passwörter müssen so gewählt werden, dass sie sich von den letzten Passwörtern (zb. letzten 6 verwendeten) unterscheiden müssen	15.07.2024
1.3.05 Passwörter von Benutzer:innen weisen eine ausreichende Komplexität auf (beinhalten Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern und sind dem Schutzbedarf angemessen).	15.07.2024
1.3.06 Die Verwaltung von Benutzerrechten für genutzte Software erfolgt zentral über festgelegte Systemadministratoren	15.07.2024
1.3.07 Jeder User erhält für jedes System und jede Software die er für seine Tätigkeit benötigt einen eigenen Benutzeraccount (keine Sammelaccounts)	15.07.2024
1.3.08 Jeder User erhält auf Basis des "need to know" Prinzip, nur die Zugriffsrechte (auf Daten, Systeme, Software, Dateiablagesysteme) die er für seine Tätigkeit auch zwingend benötigt	15.07.2024
1.3.09 Beim Ausscheiden von Mitarbeiter:innen aus dem Unternehmen ist sichergestellt, dass Zugriffsberechtigungen umgehend entfernt und User in Systemen nach Ablauf einer gewissen Frist auch gelöscht werden.	15.07.2024
1.3.10 Die Vergabe von Zugriffsberechtigungen erfolgt auf Basis von definierten Benutzerprofilen	15.07.2024
1.3.11 Fällt die Notwendigkeit eines oder mehrerer Zugriffsrechte bei einem Benutzer weg, dann werden ihm die Rechte auch zeitnah entzogen	15.07.2024
1.3.12 Zugriffe auf sensible Anwendungen oder Daten werden protokolliert (wer hat wann auf Daten zugegriffen, sie verändert oder gelöscht)	15.07.2024
1.3.13 Papierakten mit personenbezogenen Daten werden durch den Einsatz von Aktenshredder (mind. Stufe 3, Cross-cut) geshreddert	15.07.2024

Bezeichnung	Letztes Audit
1.3.14 Elektronische Datenträger werden datenschutzkonform gemäß der Sicherheitsstufe F-4, O-4, T-4, H-4, E-4 vernichtet	15.07.2024

1.4 Vertraulichkeit: Trennungsgebot

Bezeichnung	Letztes Audit
1.4.02 Bei Softwareapplikationen die personenbezogene Daten verarbeiten existiert eine Trennung in Test- und Produktivsystem	15.07.2024
1.4.03 Der Zugriff auf Daten in Datenbanken ist geregelt	15.07.2024
1.4.04 Die Sicherung der Daten (Backup) erfolgt auf physisch und örtlich getrennte Medien	15.07.2024
1.4.05 Softwareapplikationen und Dateiablagen auf die mehrere Benutzer:innen Zugriff haben, sind mit einem Berechtigungssystem ausgestattet.	15.07.2024
1.4.06 Die Verarbeitung von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken	15.07.2024
1.4.07 Die Weitergabe von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken	15.07.2024

1.5 Vertraulichkeit: Pseudoanonymisierung und Anonymisierung

Bezeichnung	Letztes Audit
1.5.01 Personenbezogene Daten werden so abgelegt oder gespeichert, dass die Zuordnung einer identifizierbaren Person nur auf Basis von entsprechenden Zugriffsrechten möglich ist	15.07.2024
1.5.03 Personenbezogenen Identifikationsdaten werden maskiert und mit fixen "Dummy" Werten überschrieben	15.07.2024
1.5.04 Pseudonyme werden ausschließlich vom Betroffenen selbst vergeben. Ein Beispiel hierfür ist der „Nickname“ des Nutzers im Chat.	15.07.2024
1.5.05 Pseudonyme werden natürlich auch vom ursprünglichen Verarbeiter vergeben, wie dies beispielsweise bei der IP-Adress-Vergabe durch einen Internet-Provider erfolgt..	15.07.2024
1.5.07 Das Pseudonym wird durch eine schlüsselabhängige Einweg- oder Hashfunktion aus invarianten Daten (Bsp. Identitätsdaten) erzeugt.	15.07.2024
1.5.09 Das Pseudonym wird (zufällig) frei gewählt oder nach einem Zufallsverfahren erzeugt.	15.07.2024
1.5.10 Personenbezogenen Identifikationsdaten werden maskiert und mit fixen "Dummy" Werten überschrieben oder gelöscht, sobald der Zweck der Verarbeitung verloren gegangen ist.	15.07.2024
1.5.12 Personenbezogenen Identifikationsdaten werden mit modernen kryptografischen Methoden verschlüsselt und verschlüsselt gespeichert	15.07.2024

1.6 Vertraulichkeit: Verschlüsselung

Bezeichnung	Letztes Audit
1.6.01 Festplatten in Servern werden verschlüsselt	15.07.2024
1.6.02 Festplatten in Laptops / Notebooks werden verschlüsselt	15.07.2024
1.6.04 Zur Datenweitergabe werden verschlüsselte Verbindungen wie https (Webseite) oder sftp (FTP Server) genutzt	15.07.2024
1.6.05 Der Zugriff auf Systeme des Unternehmens von außen, erfolgt über verschlüsselte Verbindungen (zB. VPN Tunnel)	15.07.2024
1.6.06 Es wird die aktuellste Version des TLS Verschlüsselungsprotokolls verwendet	15.07.2024
1.6.07 Die Versendung von Mails mit sensiblem Inhalt oder sensiblen Daten im Mail oder in Anhängen erfolgt verschlüsselt	15.07.2024
1.6.08 Datenbanken in den personenbezogene Daten verarbeitet werden sind verschlüsselt	15.07.2024
1.6.09 Datenfelder mit personenbezogenen Daten werden verschlüsselt in der Datenbank abgelegt	15.07.2024
1.6.10 Verschlüsselte Datenfelder werden in Benutzeroberflächen nur berechtigten Personen entschlüsselt angezeigt. Eine Bearbeitung von verschlüsselten Feldern ist für nicht berechtigte Personen nicht möglich.	15.07.2024

2.1 Integrität: 1. Eingabekontrolle

Bezeichnung	Letztes Audit
2.1.02 Es existiert eine Übersicht/ Dokumentation, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.	15.07.2024
2.1.03 Die Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer (nicht Benutzergruppen) kann nachvollzogen werden	15.07.2024
2.1.04 Es erfolgt eine technische Protokollierung der Eingabe, Änderung und Löschung von Daten inkl. Zeitpunkt der Änderung sowie wer die Daten geändert hat	15.07.2024
2.1.05 Die An- und Abmeldung an Softwareapplikationen auf die mehrere Benutzer Zugriff haben wird protokolliert	15.07.2024
2.1.06 Die An- und Abmeldung auf Servern wird protokolliert	15.07.2024

2.2. Integrität: 2. Weitergabekontrolle

Bezeichnung	Letztes Audit
2.2.01 Die Übermittlung von personenbezogenen Daten zu Lieferanten (Auftragsverarbeiter) erfolgt verschlüsselt (Mailverschlüsselung, VPN Tunnel etc.)	15.07.2024
2.2.03 Auf Rechner wird mittels Fernwartung nur nach Zustimmung des Benutzers zugegriffen. Ausgenommen davon sind Update- und Konfigurationsvorgänge am Rechner mit Hilfe automatischer Installationstools.	15.07.2024
2.2.04 05 Die Daten auf Datenträgern von Laptops oder Desktop-Computern werden vor deren internen oder externen Weitergabe gelöscht oder formatiert.	15.07.2024
2.2.05 Daten auf sonstigen Datenträgern (USB Sticks, mobile Festplatten, ausgebaute Festplatten) werden vor deren internen oder externen Weitergabe gelöscht oder formatiert.	15.07.2024
2.2.06 Bei Druckern oder Faxgeräten werden deren interne Datenträger vor der externen Weitergabe formatiert oder die Daten nach Vorgaben des Herstellers gelöscht	15.07.2024
2.2.07 Die Weitergabe von personenbezogenen Daten an Dritte erfolgt in anonymisierter oder pseudonymisierter Form	15.07.2024
Datenträger werden vor der Entsorgung physisch zerstört	15.07.2024

3.1 Verfügbarkeit und Belastbarkeit: Verfügbarkeitskontrolle

Bezeichnung	Letztes Audit
3.1.01 Auf Clients und Servern werden Updates und Sicherheitspatches regelmäßig eingespielt	15.07.2024
3.1.02 Von relevanten Systemen (zB. Buchhaltung, CRM, HR Software) oder sonstigen Systemen die personenbezogene Daten verarbeitet werden, werden regelmäßige Datensicherungen erstellt	15.07.2024
3.1.03 Datensicherungen werden räumlich getrennt von den Produktivdaten aufbewahrt	15.07.2024
3.1.04 Es wird regelmäßig geprüft ob Datensicherungen vollständig rückgesichert werden können und Daten damit wieder hergestellt werden können	15.07.2024
3.1.05 Datensicherungen werden nach einem definierten Zeitraum gelöscht	15.07.2024
3.1.06 Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, sind mit einer Feuer- und Rauchmeldeanlage ausgestattet	15.07.2024
3.1.07 Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, verfügen leicht erreichbar, über geeignete Löschmittel zur Brandbekämpfung (zB. Feuerlöscher)	15.07.2024

4.1 Verfahren zur Überprüfung: Datenschutz-Management

Bezeichnung	Letztes Audit
4.1.02 Es wird ein Verzeichnis der Verarbeitungstätigkeiten geführt und laufend aktualisiert	15.07.2024
4.1.03 Eine Überprüfung der Wirksamkeit der technisch organisatorischen Maßnahmen findet jährlich statt	15.07.2024
4.1.04 Es existieren Abläufe zur Erfüllung der Rechte von betroffenen Personen	15.07.2024
4.1.05 Eine Datenschutz Management Software ist im Einsatz	15.07.2024
4.1.06 Die Informationspflichten (Datenschutzerklärung) werden regelmäßig geprüft	15.07.2024
4.1.07 Es existiert ein Löschkonzept in dem festgelegt ist, wann, welche Daten zu löschen sind. Die Löschung von Daten wird stichprobenartig oder regelmäßig überprüft.	15.07.2024
4.1.08 Die Vernichtung von Akten oder elektronischen Datenträgern wird protokolliert	15.07.2024
4.1.09 Zum Schutz vor unberechtigtem Zutritt zu unseren Unternehmensräumlichkeiten wurde ein Zutrittsberechtigungskonzept erstellt	15.07.2024
4.1.10 Alle Mitarbeiter:innen sind auf Vertraulichkeit und Datengeheimnis verpflichtet	15.07.2024
4.1.11 Mitarbeiter:innen werden jährlich im Bereich Datenschutz geschult bzw. nachweislich sensibilisiert	15.07.2024
4.1.12 Alle Mitarbeiter:innen sind nachweislich geschult, wie sie bei Anfragen von Betroffenen zu Auskunft oder Löschung der Daten vorgehen sollen	15.07.2024
4.1.13 Für die Vergabe von Zugriffsberechtigungen existiert ein Konzept, dass regelmäßig einem Audit unterzogen wird	15.07.2024
4.1.14 Eine Richtlinie zur richtigen Verwendung und Aktualisierung von Passwörtern wurde erstellt und die Mitarbeiter werden dahingehend geschult	15.07.2024
4.1.15 in Bereichen in denen sensible personenbezogene Daten verarbeitet werden existiert eine Clean/ Clear Desk Richtlinie. Die betroffenen Mitarbeiter werden regelmäßig dahingehend sensibilisiert.	15.07.2024

Bezeichnung	Letztes Audit
4.1.16 Eine Clear Screen Richtlinie ist definiert und die Mitarbeiter werden regelmäßig sensibilisiert	15.07.2024
4.1.17 Eine Closed door Richtlinie für kritische/ sensible Bereiche (zb. Personalbüro, IT) ist definiert und wird im Unternehmen aktiv gelebt	15.07.2024
4.1.18 Eine Mobil Device Richtlinie wurde definiert und deren Einhaltung wird regelmäßig überprüft	15.07.2024
4.1.19 Es existiert eine Richtlinie zum Transport und zur Verwahrung von Laptops und Smart Devices bei Dienstreisen und im Heimbüro	15.07.2024
4.1.20 Mitarbeiter:innen sind angewiesen, die gültigen Datenschutzmaßnahmen auch im Home Office zu gewährleisten	15.07.2024
4.1.21 Um bei Angriffen auf die IT oder Katastrophenfällen geordnet reagieren zu können, haben wir einen Notfallplan erstellt.	15.07.2024

4.2 Verfahren zur Überprüfung: Incident-Response-Management

Bezeichnung	Letztes Audit
4.2.01 Fehlerhafte Login Versuche führen zu einer automatischen Sperre des User Logins. Die Sperre bleibt für einen definierten Zeitraum (siehe Passwort Richtlinie) bestehen.	15.07.2024
4.2.02 Ein Ablauf zur Meldung von Sicherheitsverletzungen an die Datenschutz Behörde und betroffene Personen existiert	15.07.2024
4.2.03 Ein Ablaufplan zum Umgang mit Sicherheitsverletzungen liegt vor	15.07.2024
4.2.04 Jede Sicherheitsverletzung wird an zentraler Stelle dokumentiert und priorisiert	15.07.2024
4.2.05 Mitarbeiter:innen werden jährlich geschult wie sie mit Sicherheitsverletzungen umgehen sollen	15.07.2024
4.2.06 Zu jeder Sicherheitsverletzung werden Maßnahmen diskutiert und umgesetzt die zu einer Vermeidung oder Milderung weiterer Sicherheitsverletzungen führen (TOMs!)	15.07.2024
4.2.07 Verarbeitungen werden hinsichtlich einer Datenschutz Folgeabschätzung geprüft. Eine solche wird bei Bedarf auch durchgeführt und dokumentiert	15.07.2024
4.2.08 Ein IT Security Manager ist bestellt	15.07.2024

4.3 Verfahren zur Überprüfung: Datenschutzfreundliche Voreinstellungen

Bezeichnung	Letztes Audit
4.3.04 Beim Einsatz neuer Systeme oder Software wird darauf geachtet, dass DSGVO Anforderungen erfüllt sind	-

4.4 Verfahren zur Überprüfung: Auftragskontrolle

Bezeichnung	Letztes Audit
4.4.01 Es existiert eine Übersicht über alle Lieferanten (Empfänger), die in unserem Namen personenbezogene Daten als Auftragsverarbeiter verarbeiten	15.07.2024
4.4.02 Die Auswahl von Auftragnehmern erfolgt unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	15.07.2024
4.4.03 Wir beauftragen nur Unternehmen mit der Verarbeitung von personenbezogenen Daten, nur wenn sie einen Datenschutzbeauftragten bestellt haben	15.07.2024
4.4.04 Mit all unseren Auftragsverarbeitern haben wir einen Auftragsverarbeitervertrag abgeschlossen	15.07.2024
4.4.06 In den Auftragsverarbeiter-Verträgen ist sicher gestellt, dass Daten nach Beendigung des Auftrags auch vernichtet oder übergeben werden	15.07.2024
4.4.07 Wir überprüfen regelmäßig ob unsere Auftragsverarbeiter die festgelegten Datenschutzmaßnahmen einhalten	15.07.2024
4.4.08 Die Wirksamkeit von Datenschutzmaßnahmen oder die Gültigkeit entsprechender Zertifikate werden bei Auftragsverarbeitern regelmäßig geprüft	15.07.2024
4.4.10 Mitarbeiter von Auftragnehmern werden auf das Datengeheimnis verpflichtet bzw. der Auftragnehmer muss dies seinerseits sicher stellen	15.07.2024