Technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO

mitteldeutsche IT GmbH | Stand: 14.03.2026

Inhaltsverzeichnis

1. Einleitung und Geltungsbereich

Die mitteldeutsche IT GmbH (nachfolgend „mIT") trifft gemäß Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten sicherzustellen. Die nachfolgenden Maßnahmen gelten für alle Cloud-, Managed-Service- und KI-Infrastrukturleistungen der mIT und werden mindestens jährlich auf Wirksamkeit überprüft.

Diese Maßnahmenübersicht dient als Anhang 2 zum Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DS-GVO und dokumentiert den Stand der Technik 2026 (DS-GVO, NIS-2, ISO 27001, BSI C5, EU AI Act).

2. Übersicht der TOM-Kategorien

Kategorie	Anzahl Maßnahmen
1. Grundsätzliche Maßnahmen	8
2. Zutrittskontrolle	13
3. Zugangskontrolle / Zugriffskontrolle	21
4. Weitergabekontrolle	7
5. Eingabekontrolle	5
6. Auftragskontrolle	5
7. Verfügbarkeitskontrolle / Integrität	8
8. Zweckbindungs-/Trennungsgebot	4
9. Informationssicherheitsmanagement	3
10. NIS-2 und Incident Management	8
11. Verschlüsselung und Kryptographie	6
12. Backup, Recovery und BCM	6
13. Protokollierung und Log-Management	7
14. Schwachstellenmanagement	8
15. KI-Infrastruktur (spezifisch)	10
16. RZ Leipzig (spezifisch)	4
GESAMT	123

3. Technische und Organisatorische Maßnahmen

1. Grundsätzliche Maßnahmen

Datenschutz-Management
Wir betreiben ein strukturiertes Datenschutz-Managementsystem, das regelmäßig (mindestens halbjährlich) auf Wirksamkeit überprüft wird. Dadurch stellen wir sicher, dass alle Datenschutzprozesse aktuell und wirksam sind.

Aktuelle Software-Versionen
Alle eingesetzte Software (Betriebssysteme, Anwendungen, Virenscanner, Firewalls) wird stets auf dem aktuell verfügbaren Sicherheitsstand gehalten. Sicherheitsupdates werden zeitnah eingespielt.

Rückgabe von Zugangsberechtigungen
Wenn Mitarbeiter das Unternehmen verlassen oder ihre Aufgaben wechseln, werden alle Zugangsberechtigungen (Schlüssel, Chipkarten, Systemzugänge) sofort entzogen. Dadurch wird unbefugter Zugriff verhindert.

Betroffenenrechte-Management
Wir haben Prozesse etabliert, um Anfragen betroffener Personen (Auskunft, Löschung, Berichtigung etc.) innerhalb der gesetzlichen Fristen zu bearbeiten. Formulare und Verantwortlichkeiten sind klar definiert.

Mitarbeiterschulungen Datenschutz
Alle Mitarbeiter werden mindestens jährlich zum Datenschutz geschult und auf Verschwiegenheit verpflichtet. Die Teilnahme wird dokumentiert. Spezielle Regelungen gelten für mobiles Arbeiten und Privatgeräte.

Privacy by Design
Datenschutz wird bereits bei der Planung und Auswahl von IT-Systemen berücksichtigt (Art. 25 DS-GVO). Wir prüfen Datenschutzrisiken, bevor neue Systeme eingeführt werden, und konfigurieren sie datenschutzfreundlich.

Data-Breach-Management
Für den Fall einer Datenschutzverletzung haben wir einen dokumentierten Prozess zur schnellen Reaktion (Prüfung, Dokumentation, Meldung an Behörden/Betroffene). Verantwortlichkeiten und Fristen sind klar geregelt.

Datenschutzbeauftragter
Wir haben einen externen Datenschutzbeauftragten bestellt, der uns berät und die Einhaltung der DS-GVO überwacht. Kontaktdaten werden auf Anfrage mitgeteilt.

2. Zutrittskontrolle

Sicherheitsschlösser
Alle Türen zu Bereichen mit IT-Systemen sind mit hochwertigen Sicherheitsschlössern ausgestattet, um unbefugten physischen Zutritt zu verhindern.

Schlüsselzugang für Berechtigte
Der Zutritt zum Unternehmen erfolgt über personalisierte Schlüssel. Jeder Zugang wird dokumentiert (wer erhält wann welchen Schlüssel).

Dokumentation der Zutrittsmöglichkeiten
Alle Personen mit Zutrittsberechtigung werden namentlich in einem System erfasst. Dadurch ist nachvollziehbar, wer zu welchen Bereichen Zugang hat.

Private-Suiten im Rechenzentrum
Für Kunden mit hohem Schutzbedarf bieten wir eigene, abgetrennte Colocation-Bereiche (Private-Suites), die von gemeinschaftlichen Flächen separiert sind.

Besucherausweise
Alle Besucher des Rechenzentrums müssen sichtbar einen Besucherausweis tragen. Dadurch sind Unbefugte sofort erkennbar.

Zutrittsregelungen für Betriebsfremde
Externe Personen (z. B. Wartungstechniker, Lieferanten) dürfen das Gebäude nur nach Anmeldung und in Begleitung eines Mitarbeiters betreten.

Überwachungseinrichtungen
Das Rechenzentrum ist mit Alarmanlage, Videoüberwachung und Einbruchmeldeanlage ausgestattet. Unbefugtes Eindringen wird sofort erkannt.

Chipkarten-/Transponder-Schließsystem
Der Zugang zu sensiblen Bereichen erfolgt über elektronische Chipkarten oder Transponder. Jeder Zutritt wird elektronisch protokolliert.

Elektronisches Besucherbuch
Alle Rechenzentrums-Besucher tragen sich in ein elektronisches Besucherbuch ein (Name, Firma, Zeitpunkt, Besuchsgrund). Dies ermöglicht lückenlose Nachvollziehbarkeit.

Beaufsichtigung von Hilfskräften
Zeitarbeitskräfte oder externe Dienstleister werden bei Tätigkeiten in sensiblen Bereichen stets beaufsichtigt.

Persönlicher Empfang von Betriebsfremden
Externe Personen werden persönlich empfangen und während ihres gesamten Aufenthalts begleitet. Unbeaufsichtigter Aufenthalt ist nicht möglich.

24/7/365 Wachdienst-Verbindung
Das Rechenzentrum ist rund um die Uhr mit einem professionellen Wachdienst verbunden. Bei Alarmen erfolgt sofortige Reaktion.

Sicherheitszonenkonzept
Das Rechenzentrum ist in Sicherheitszonen mit abgestuften Zugangsberechtigungen unterteilt. Je sensibler der Bereich, desto strenger die Zugangskontrollen.

3. Zugangskontrolle / Zugriffskontrolle

Hardware-Firewall
Alle Netzwerkverbindungen werden durch leistungsstarke Hardware-Firewalls geschützt, die unberechtigte Zugriffe von außen blockieren.

Software-Firewall
Zusätzlich zu Hardware-Firewalls sind alle Server und Arbeitsplätze mit Software-Firewalls ausgestattet, die lokalen Schutz bieten.

Protokollierung von Datenänderungen
Alle Änderungen und Löschungen von Daten werden automatisch protokolliert (wer, wann, was). Dies ermöglicht lückenlose Nachvollziehbarkeit.

Berechtigungskonzept
Jeder Mitarbeiter erhält nur die Zugriffsrechte, die er für seine Aufgaben benötigt (Least-Privilege-Prinzip). Berechtigungen werden regelmäßig überprüft.

Zugriff auf Kundensysteme nur mit AVV
Wir greifen auf Ihre Systeme nur zu, wenn dies vertraglich vereinbart ist (z. B. im Rahmen eines Auftragsverarbeitungsvertrags) und Sie uns dazu beauftragt haben.

Aufgabenbezogene Berechtigungen
Zugriffsrechte werden strikt nach Aufgabe vergeben. Ein Mitarbeiter aus der Buchhaltung hat z. B. keinen Zugriff auf technische Systeme.

Automatische Benutzersperrung
Nach mehrfacher falscher Passworteingabe oder nach einer Inaktivitätsphase wird der Benutzer automatisch gesperrt. Dadurch werden Brute-Force-Angriffe verhindert.

Protokollierung von Zugriffen
Alle Zugriffe auf personenbezogene Daten werden protokolliert. Wir können nachvollziehen, wer wann auf welche Daten zugegriffen hat.

Datenträgervernichtung nach DIN 66399
Ausgemusterte Datenträger (Festplatten, USB-Sticks) werden nach DIN 66399 sicher vernichtet (Sicherheitsstufe P-4 oder höher), sodass Daten nicht wiederherstellbar sind.

USB-Stick-Richtlinie
Die Nutzung von USB-Sticks ist reglementiert. Private USB-Sticks dürfen nicht verwendet werden; Firmen-USB-Sticks sind verschlüsselt und personalisiert.

Zwei-Faktor-Authentifizierung (2FA)
Für den Zugriff auf kritische Systeme ist neben dem Passwort ein zweiter Faktor erforderlich (z. B. Hardware-Token, Smartphone-App). Dies erhöht die Sicherheit erheblich.

Passwortrichtlinie
Passwörter müssen mindestens 12 Zeichen lang sein und Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Passwörter werden regelmäßig gewechselt.

Aktueller Virenschutz
Auf allen Systemen läuft stets aktueller Virenschutz mit tagesaktuellen Signaturen. Verdächtige Dateien werden automatisch blockiert und gemeldet.

Aktuelle Softwareversionen
Alle eingesetzte Software wird zeitnah aktualisiert. Sicherheitspatches werden priorisiert eingespielt (kritische Lücken innerhalb 72 Stunden).

Least-Privilege-Prinzip
Benutzer und Systeme erhalten nur die minimal notwendigen Zugriffsrechte. Administrative Rechte werden nur bei konkretem Bedarf und zeitlich begrenzt vergeben.

Passwortmanager
Mitarbeiter nutzen Passwortmanager zur sicheren Speicherung und Verwaltung komplexer Passwörter. Passwörter müssen nicht aufgeschrieben oder wiederverwendet werden.

VPN-Technologie
Alle Verbindungen von außen (z. B. Homeoffice) erfolgen über verschlüsselte VPN-Tunnel. Dadurch sind Datenübertragungen vor Abhören geschützt.

Multifaktor-Authentisierung (MFA)
Bei Systemen mit erhöhtem Schutzbedarf (z. B. Zugriff auf Kundendaten) ist zusätzlich zum Passwort eine Multifaktor-Authentisierung (z. B. per Smartphone-App) erforderlich.

Intrusion-Detection-System (IDS)
Wir setzen Intrusion-Detection-Systeme ein, die verdächtige Aktivitäten im Netzwerk erkennen und Alarm auslösen. Dadurch werden Angriffe frühzeitig erkannt.

Festplattenverschlüsselung
Alle Festplatten (Server, Laptops, Desktops) sind mit AES-256-Verschlüsselung geschützt (FileVault auf Mac, BitLocker auf Windows). Bei Verlust/Diebstahl sind Daten nicht lesbar.

Verschlüsselung mobiler Datenträger
Mobile Datenträger (USB-Sticks, externe Festplatten) sind verschlüsselt. Nur autorisierte Personen können darauf zugreifen.

4. Weitergabekontrolle

Festlegung und Dokumentation der Empfänger
Wenn personenbezogene Daten weitergegeben werden (z. B. an Dienstleister), wird dokumentiert, wer Empfänger ist, welche Daten weitergegeben werden und auf welcher Rechtsgrundlage.

Pseudonymisierung
Wo möglich, werden personenbezogene Daten pseudonymisiert (z. B. durch Kennungen statt Namen), um das Risiko bei einer Datenweitergabe zu reduzieren.

Protokollierung/Auswertung
Datenweitergaben werden protokolliert und regelmäßig ausgewertet, um unberechtigte Weitergaben zu erkennen.

VPN-Tunnelverbindung
Bei der Übertragung von Daten über das Internet werden verschlüsselte VPN-Tunnel genutzt, sodass Daten vor Abhören geschützt sind.

Transportverschlüsselung TLS 1.3
Alle Datenübertragungen im Internet erfolgen verschlüsselt mit TLS 1.2 oder höher (bevorzugt TLS 1.3), dem aktuellen Sicherheitsstandard.

Informationsklassifizierung
Daten werden nach Schutzbedarf klassifiziert (z. B. öffentlich, intern, vertraulich, streng vertraulich). Je nach Klassifizierung gelten unterschiedliche Schutzmaßnahmen.

Verschlüsselung von Datenträgern und Verbindungen
Sowohl gespeicherte Daten (Datenträger) als auch übertragene Daten (Netzwerkverbindungen) werden verschlüsselt, um Schutz vor unbefugtem Zugriff zu gewährleisten.

5. Eingabekontrolle

Berechtigungskonzept für Dateneingabe
Nur autorisierte Personen dürfen Daten eingeben, ändern oder löschen. Die Berechtigungen werden nach Rolle und Aufgabe vergeben.

Datenbankprotokolle mit Zeitstempel
Alle Änderungen in Datenbanken werden automatisch protokolliert (wer, wann, was). Zeitstempel ermöglichen genaue Nachvollziehbarkeit.

Aufbewahrung von Formularen
Formulare, von denen Daten in IT-Systeme übernommen wurden (z. B. Anträge, Verträge), werden archiviert, um die Herkunft der Daten nachweisen zu können.

Protokollierung von Dateneingaben
Alle Dateneingaben, -änderungen und -löschungen werden protokolliert. Dies ermöglicht Nachvollziehbarkeit und Aufdeckung unbefugter Änderungen.

Zentrale Logserver
Alle Protokolldaten werden auf zentralen, besonders geschützten Logservern gesammelt. Dadurch sind Manipulationen von Protokollen praktisch ausgeschlossen.

6. Auftragskontrolle

Due-Diligence-Prüfung von Auftragnehmern
Bevor wir Unterauftragnehmer beauftragen, prüfen wir deren Eignung und Zuverlässigkeit (z. B. Zertifikate, Referenzen, Sicherheitsmaßnahmen).

Schriftliche Weisungen (AVV)
Alle Unterauftragnehmer, die personenbezogene Daten verarbeiten, erhalten schriftliche Weisungen in Form eines Auftragsverarbeitungsvertrags (AVV) gemäß Art. 28 DS-GVO.

Kontrolle der Einhaltung
Wir überprüfen regelmäßig (mindestens jährlich), ob Unterauftragnehmer die vereinbarten Sicherheitsmaßnahmen einhalten (z. B. durch Audits, Zertifikats-Reviews).

Datenlöschung nach Vertragsende
Nach Beendigung des Auftrags stellen wir sicher, dass der Unterauftragnehmer alle Daten sicher löscht oder zurückgibt. Wir erhalten eine Löschbestätigung.

Liste der Unterauftragnehmer
Wir führen eine dokumentierte Liste aller Unterauftragnehmer mit Tätigkeitsbeschreibung. Diese Liste wird Ihnen auf Anfrage zur Verfügung gestellt.

7. Verfügbarkeitskontrolle / Integrität

Festplattenspiegelung (RAID)
Alle wichtigen Server nutzen RAID-Systeme (Festplattenspiegelung). Bei Ausfall einer Festplatte bleiben Daten verfügbar und können ohne Unterbrechung wiederhergestellt werden.

Backup- und Recovery-Konzept
Wir erstellen täglich Backups aller produktiven Systeme (RPO: 24 Stunden). Die Wiederherstellbarkeit wird quartalsweise durch Test-Restores überprüft und dokumentiert.

Offsite-Backup
Zusätzliche Sicherungskopien werden an geografisch getrennten Orten (Offsite) gelagert. Bei Brand oder Naturkatastrophe am Hauptstandort bleiben Daten verfügbar.

Unterbrechungsfreie Stromversorgung (USV)
Alle kritischen IT-Systeme sind an eine USV (unterbrechungsfreie Stromversorgung) angeschlossen. Bei Stromausfall läuft der Betrieb ohne Unterbrechung weiter.

Überspannungsschutz
Alle Systeme sind durch Überspannungsschutz gegen Schäden durch Blitzeinschlag oder Stromschwankungen gesichert.

Klimatisierung
Das Rechenzentrum ist mit redundanter Klimatisierung ausgestattet. Bei Ausfall einer Klimaanlage übernimmt automatisch die zweite, um Überhitzung zu verhindern.

Notfallkonzept (BCM)
Wir haben ein dokumentiertes Business-Continuity-Management-System (BCM). Im Notfall (Brand, Ausfall) können wir den Betrieb an Ausweichstandorten fortsetzen.

Belastbarkeitstests
Wir führen regelmäßig Tests durch (z. B. Restore-Tests, Failover-Tests), um sicherzustellen, dass unsere Notfallpläne funktionieren.

8. Zweckbindungs-/Trennungsgebot

Physische Mandantentrennung
Für Kunden mit hohem Schutzbedarf bieten wir dedizierte Hardware (eigene Server, eigene Netzwerke). Ihre Daten teilen sich keine physische Hardware mit anderen Kunden.

Logische Mandantentrennung
In Multi-Tenant-Umgebungen (z. B. Cloud-Systeme) werden Kundendaten logisch voneinander getrennt (z. B. durch Datenbank-Schemas, Kubernetes-Namespaces). Ein Kunde kann nicht auf Daten anderer Kunden zugreifen.

Trennung Produktiv-/Testsystem
Produktivsysteme (mit echten Kundendaten) sind strikt von Test- und Entwicklungssystemen getrennt. Auf Testsystemen werden keine produktiven personenbezogenen Daten verarbeitet.

Trennung pseudonymisierter Daten
Wenn Daten pseudonymisiert werden, wird die Zuordnungsdatei (die den Pseudonym-Schlüssel enthält) getrennt und besonders geschützt aufbewahrt.

9. Informationssicherheitsmanagement

ISO/IEC 27001 Zertifizierung
Wir betreiben ein zertifiziertes Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001. Die Zertifizierung wird jährlich durch externe Auditoren überprüft.

BSI C5-Testat
Wir halten ein BSI C5-Testat (Cloud Computing Compliance Controls Catalogue) vor, das die Einhaltung der Anforderungen des Bundesamts für Sicherheit in der Informationstechnik für Cloud-Dienste bestätigt.

Bereitstellung von Nachweisen
Auf Anfrage stellen wir Ihnen aktuelle Zertifikate, Testate, Auditberichte und Dokumentationen zu unseren Sicherheitsmaßnahmen zur Verfügung.

10. NIS-2 und Incident Management

24/7 Security Monitoring
Wir überwachen unsere Systeme rund um die Uhr auf sicherheitsrelevante Vorfälle. Verdächtige Aktivitäten werden sofort erkannt und untersucht.

Incident-Response-Prozess
Wir haben einen dokumentierten Prozess zur Behandlung von Sicherheitsvorfällen (Erkennung, Analyse, Eindämmung, Behebung, Lessons Learned). Verantwortlichkeiten sind klar geregelt.

24h-Erstmeldung bei Cyber-Incidents
Erhebliche Cyber-Incidents (gemäß NIS-2-Kriterien) melden wir innerhalb von 24 Stunden als Erstmeldung an die zuständige Behörde (BSI/CSIRT).

72h-Detailbericht
Nach der Erstmeldung folgt innerhalb von 72 Stunden ein detaillierter Incident-Report mit Ursachenanalyse und getroffenen Maßnahmen.

Kundeninformation bei Vorfällen
Wenn ein Sicherheitsvorfall Ihre Systeme oder Daten betrifft, informieren wir Sie unverzüglich (innerhalb von 24 Stunden) und erläutern die Situation sowie getroffene Maßnahmen.

Eskalationsplan
Wir haben einen Eskalationsplan mit definierten Rollen, Verantwortlichkeiten und Benachrichtigungswegen für verschiedene Incident-Schweregrade (z. B. Low, Medium, High, Critical).

Incident-Dokumentation
Alle Sicherheitsvorfälle werden vollständig dokumentiert und archiviert. Wir führen Post-Incident-Reviews durch, um aus Vorfällen zu lernen und Prozesse zu verbessern.

Jährliche Incident-Response-Übungen
Wir führen mindestens jährlich Incident-Response-Übungen durch, um die Wirksamkeit unserer Prozesse zu überprüfen und Mitarbeiter zu trainieren.

11. Verschlüsselung und Kryptographie

TLS 1.3 für Datenübertragungen
Alle Datenübertragungen im Internet erfolgen verschlüsselt mit TLS 1.2 oder höher (bevorzugt TLS 1.3). Veraltete Protokolle (TLS 1.0/1.1, SSL) sind deaktiviert.

AES-256-Verschlüsselung
Gespeicherte Daten (at-rest) werden mit AES-256 verschlüsselt, einem der sichersten verfügbaren Verschlüsselungsstandards.

Key-Management-System (KMS)
Alle kryptographischen Schlüssel werden in einem separaten, besonders geschützten Key-Management-System (KMS) verwaltet. Schlüssel werden regelmäßig rotiert.

Public-Key-Infrastruktur (PKI)
Wir betreiben eine eigene Public-Key-Infrastruktur (PKI) für die Ausstellung und Verwaltung digitaler Zertifikate. Zertifikate werden automatisch erneuert.

SSH-Schlüsselrotation
SSH-Schlüssel für Systemzugriffe werden regelmäßig (mindestens jährlich) erneuert, um das Risiko kompromittierter Schlüssel zu minimieren.

Verbot veralteter Algorithmen
Wir setzen keine veralteten oder unsicheren Verschlüsselungsalgorithmen ein (z. B. DES, 3DES, MD5, SHA-1). Nur aktuelle, als sicher geltende Algorithmen werden verwendet.

12. Backup, Recovery und BCM

RPO: 24 Stunden
Wir erstellen täglich Backups aller produktiven Systeme. Der Recovery Point Objective (RPO) beträgt 24 Stunden – im Worst Case können Daten des letzten Tages wiederhergestellt werden.

Backup-Vorhaltezeiten
Backups werden standardmäßig 7 Tage aufbewahrt. Produktspezifische Vorhaltezeiten können gemäß Leistungsschein vereinbart werden (z. B. 30 Tage für mIT Office).

Quartalsweise Restore-Tests
Wir testen quartalsweise die Wiederherstellbarkeit von Backups durch tatsächliche Restore-Versuche. Alle Tests werden dokumentiert.

RTO: 4 Stunden für kritische Systeme
Für kritische Systeme beträgt die Recovery Time Objective (RTO) 4 Stunden. Das bedeutet, wir können Systeme im Notfall innerhalb von 4 Stunden wiederherstellen.

Business Continuity Plan (BCP)
Wir haben einen dokumentierten Business-Continuity-Plan mit definierten Ausweichstandorten und Notfallprozeduren. Im Katastrophenfall können wir den Betrieb an alternativen Standorten fortsetzen.

Jährliche BCP-Tests
Wir führen jährlich Tests unseres Business-Continuity-Plans durch (z. B. Failover-Tests, Notfall-Übungen) und aktualisieren die Dokumentation basierend auf den Ergebnissen.

13. Protokollierung und Log-Management

90-Tage-Log-Aufbewahrung
Sicherheitsrelevante Logs (Zugriffs-, Anmelde-, Systemlogs) werden für mindestens 90 Tage aufbewahrt. Dies ermöglicht forensische Analysen bei Sicherheitsvorfällen.

Zentrale Log-Aggregation
Alle Logs werden auf zentralen, besonders geschützten Logservern gesammelt. Der Zugriff ist schreibgeschützt, sodass Manipulationen ausgeschlossen sind.

NTP-Zeitsynchronisation
Alle Systeme synchronisieren ihre Uhrzeiten über NTP (Network Time Protocol). Dadurch sind Zeitstempel in Logs präzise und über Systeme hinweg vergleichbar.

Log-Sperrung bei Incidents
Im Falle eines Sicherheitsvorfalls werden betroffene Logs gesperrt und für die Dauer der Untersuchung und etwaiger rechtlicher Aufbewahrungspflichten archiviert.

Automatische Alarmierung
Bei sicherheitskritischen Log-Ereignissen (z. B. mehrfache Fehllogins, Privilegieneskalation, ungewöhnliche Zugriffsmuster) erfolgt automatische Alarmierung des Security-Teams.

Regelmäßige Log-Reviews
Das Security-Team wertet Logs regelmäßig aus, um verdächtige Aktivitäten frühzeitig zu erkennen und Trends zu analysieren.

Verschlüsselte Log-Übertragung
Log-Daten werden verschlüsselt übertragen (TLS) und verschlüsselt gespeichert (AES-256), um Vertraulichkeit und Integrität zu gewährleisten.

14. Schwachstellenmanagement

Kontinuierliches Vulnerability-Scanning
Alle produktiven Systeme werden kontinuierlich auf bekannte Schwachstellen gescannt. Entdeckte Schwachstellen werden nach Schweregrad priorisiert und behoben.

CVE-Monitoring
Wir überwachen kontinuierlich öffentlich bekannte Schwachstellen (CVE – Common Vulnerabilities and Exposures) und prüfen, ob unsere Systeme betroffen sind.

Kritische Patches innerhalb 72h
Kritische Sicherheitslücken (CVSS-Score ≥ 9.0) werden innerhalb von 72 Stunden behoben. Hochkritische Lücken (CVSS 7.0–8.9) innerhalb von 7 Tagen, mittelschwere innerhalb von 30 Tagen.

Jährliche Penetrationstests
Mindestens einmal jährlich lassen wir externe Sicherheitsexperten Penetrationstests durchführen. Diese Tests simulieren Angriffe, um Schwachstellen aufzudecken.

Umfassender Pentest-Scope
Penetrationstests umfassen externe und interne Netzwerke, Webanwendungen, Cloud-Infrastruktur und API-Endpunkte.

Dokumentation und Remediation
Alle Ergebnisse von Penetrationstests werden dokumentiert. Gefundene Schwachstellen werden priorisiert behoben und die Behebung wird nachverfolgt.

Ad-hoc-Pentests bei Änderungen
Nach wesentlichen Infrastrukturänderungen (z. B. neue Systeme, größere Updates) führen wir Ad-hoc-Penetrationstests durch, um neue Schwachstellen auszuschließen.

Responsible Disclosure
Wir haben einen Prozess für externe Sicherheitsforscher, um Schwachstellen verantwortungsvoll zu melden (Responsible Disclosure). Meldungen werden zeitnah bearbeitet.

15. KI-Infrastruktur (spezifisch)

Logische Isolation von KI-Workloads
KI-Workloads verschiedener Auftraggeber werden auf Namespace- und Netzwerkebene (z. B. Kubernetes Network Policies) strikt voneinander isoliert. Ein Kunde kann nicht auf KI-Ressourcen anderer Kunden zugreifen.

Keine dauerhafte Prompt-Speicherung
Eingabedaten (Prompts) und Modell-Ausgaben werden nicht dauerhaft durch uns gespeichert, sofern dies nicht für den Infrastrukturbetrieb technisch erforderlich ist.

Zugriff nur nach Weisung
Wir greifen auf KI-Infrastrukturkomponenten ausschließlich nach dokumentierter Weisung des Auftraggebers zu. Jeder Zugriff wird protokolliert.

Privileged Access Management (PAM) für KI
Administrativer Zugriff auf KI-Systeme erfolgt über ein Privileged Access Management (PAM)-System. Zugriffe sind zeitlich begrenzt, werden protokolliert und erfordern Vier-Augen-Prinzip.

Separate GPU-Sicherheitszonen
GPU-Ressourcen für KI-Workloads befinden sich in separaten Sicherheitszonen im Rechenzentrum mit verstärkten physischen und logischen Zugangskontrollen.

Anomalie-Monitoring für KI-Workloads
KI-Workloads werden auf Anomalien überwacht (z. B. ungewöhnliche Ressourcennutzung, verdächtige Zugriffsmuster). Abweichungen lösen Alarme aus.

Verschlüsselung von Modell-Artefakten
KI-Modelle und Trainingsdaten werden im Speicher verschlüsselt (at-rest), um unbefugten Zugriff zu verhindern.

Datenfluss-Dokumentation für KI
Wir dokumentieren die Datenflüsse zwischen KI-Komponenten (Eingabe → Modell → Ausgabe) für Transparenz und Auditierbarkeit gemäß AI Act.

Sicherheitsprüfung von Container-Images
Alle eingesetzten Container-Images und KI-Frameworks werden regelmäßig auf Sicherheitslücken gescannt. Nur geprüfte Images werden in Produktion eingesetzt.

Keine eigenständige Datenauswertung
Die mitteldeutsche-IT GmbH führt keine eigenständige Auswertung oder Nutzung der in KI-Anwendungen verarbeiteten personenbezogenen Daten durch. Wir sind reiner Infrastrukturanbieter.

16. RZ Leipzig (spezifisch)

Dauerhaft Personal anwesend (24/7)
Das Rechenzentrum Leipzig ist rund um die Uhr (24/7/365) besetzt. Personal vor Ort kann sofort auf Vorfälle reagieren.

Wachpersonal
Zusätzlich zum technischen Personal ist Wachpersonal vor Ort, das für physische Sicherheit sorgt.

Fenstersicherung
Alle Fenster im Rechenzentrum sind gegen Einbruch gesichert (Vergitterung, bruchsicheres Glas).

Videoüberwachung
Das gesamte Rechenzentrum ist videoüberwacht. Aufnahmen werden für 30 Tage gespeichert und können bei Vorfällen ausgewertet werden.

4. Gültigkeit und Kontakt

Diese TOM-Übersicht ist ab dem 14.03.2026 gültig und wird mindestens jährlich sowie bei wesentlichen Änderungen der Infrastruktur oder der Rechtslage aktualisiert. Die jeweils aktuelle Fassung ist Bestandteil des Auftragsverarbeitungsvertrags (AVV).