

Fragenkatalog zu den technischen und organisatorischen Maßnahmen zur Datensicherheit (TOM)



DealerCenter Digital GmbH

Ludwig-Erhard-Straße 13a
84034 Landshut

Datenschutzbeauftragter des Unternehmens

Süddeutsche Datenschutzgesellschaft mbH
Am Pfaffensteiner Hang 17
93059 Regensburg

Telefon: +49 941-38177070

Version	2.0
Stand	08.10.2025
Status	Zwischenkontrolle

Die Aufnahme erfolgte fernmündlich und es fand keine Verifizierung vor Ort statt.
Ausgefüllt am 08.10.2025 mit Unterstützung von:

Name: Alexander Vetter
Funktion: CTO
E-Mail-Adresse: alexander.vetter@bike.center

1. Vertraulichkeit der Verarbeitung gem. Art. 32 Abs. 1 lit. b) Var. 1 DSGVO

1.1. Zugangskontrolle

Die Zugangskontrolle (vormals Zutrittskontrolle) beschreibt Maßnahmen, die Unbefugten den Zugang zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, verwehren.

Technische Maßnahmen

- Chipkarten/Transponder
- Manuelles Schließsystem oder mechatronisches Schließsystem
- Arbeitsplatzrechner sind in verschlossenen Räumen
- Keine Außenfenster im Rechenzentrum bzw. Serverraum
- Im Erdgeschoss stabile, einbruchshemmende oder vergitterte Fenster und Türen (z.B. nach DIN EN 1627)
- Maßnahmen gegen einfaches Mithören und Einsichtnahme (insb. bei Kundenempfang, Shared Spaces oder mobilem Arbeiten)
- Automatisches Sperren des Endgerätes nach einer gewissen Zeitspanne der Inaktivität (Bildschirm Sperre)
- BIOS-Schutz (separates Passwort)
- Deaktivierung von nicht genutzten Netzwerkdosen

Organisatorische Maßnahmen

- Dokumentierte Schlüsselverwaltung
 - Schließregelung
 - Gelebte Regelung für den Zutritt von Firmenfremden (z.B. Begleitung, Zutrittsverbote, Ausweise)
-

1.2. Datenträger- und Speicherkontrolle

Die Datenträgerkontrolle beschreibt Maßnahmen, die das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern verhindern. Die Speicherkontrolle beschreibt Maßnahmen zur Verhinderung der unbefugten Eingabe sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Technische Maßnahmen

Anbindung mobiler Arbeitsplätze (z. B. dienstliche Notebooks, dienstliche Smartphones) über das Internet erfolgt über verschlüsselte und auch kryptographisch authentifizierte Verbindungen (z. B. verschlüsselte VPN mit Authentifizierung mittels starken Passwörtern und kryptographischen Client-Zertifikaten)

Dokumentation der Löschung/Vernichtung von Datenträgern

Einsatz von Aktenvernichter (mind. Sicherheitsstufe DIN 66399: P4 mit max. 160 mm² pro Partikel und 6mm Streifenbreite oder P5 mit max. 30 mm² pro Partikel und 2mm Streifenbreite)

Organisatorische Maßnahmen

Umgesetzte Löschung auf Entwicklungs-, Test- und Produktivumgebungen

Sichere Verwahrung Mobiler Datenträger

Verschlüsselung gem. Art. 32 Abs. 1 lit. a) DSGVO

Einsatz starker Verschlüsselung der mobilen Endgeräte (Smartphones und Tablets) und mobilen Datenträger (z.B. USB-Sticks, Festplatten)

Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem Stand der Technik.

Starke Verschlüsselung von Datenträgern in Laptops & Clients

1.3. Benutzerkontrolle

Die Benutzerkontrolle beschreibt Maßnahmen zur Verhinderung der Nutzung von automatisierten Verarbeitungssystemen unter Einsatz von Einrichtungen zur Datenübertragung durch Unbefugte. Hierunter kann auch der Schutz vor unberechtigter Systemnutzung, sowie vor Systemeinbrüchen und -missbrauch über Netzwerke gefasst werden.

Technische Maßnahmen

- Verwendung einer Anti-Viren-Lösung auf Client-Rechnern und Notebooks mit tagesaktueller Aktualisierung der Signaturdatenbanken
 - Verwendung eines Endpoint-Protection-System auf Client-Rechnern und Notebooks mitsamt automatischen On-Access-Scans
 - Verwendung einer Anti-Viren-Lösung bzw. eines Endpoint-Protection-System auf Servern
 - Verwendung einer Anti-Viren-Lösung bzw. eines Endpoint-Protection-System auf Smartphones und Tablets
 - Prüfung eingehender E-Mails mittels Anti-Malwareschutz
 - Einsatz von Funkzugängen per WLAN nur auf aktuellen WLAN-Routern mit wirksamen Zugangsmechanismen
 - Nutzung eines WLAN-Gastzugang ohne Zugangsmöglichkeit zum internen Netzwerk
 - Es wird nur Software eingesetzt, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden.
 - Es werden ausschließlich Betriebssysteme eingesetzt, für die vom Hersteller noch Sicherheits-Updates bereitgestellt werden.
 - Es werden keine mobilen Endgeräte eingesetzt, für die es keine Sicherheitsupdates (mehr) gibt.
 - Automatische Einspielung sicherheitsrelevante Updates und Patches für Betriebssysteme von Client Rechner
 - Ordnungsgemäße Konfiguration der Softwareverteilung
 - Konfiguration der automatischen Sicherheitsupdates für Server
 - Zeitnahes manuelles Einspielen von Sicherheitsupdates auf risikoanfälligen Servern
 - Geregelter Prozess für Einspielung von Sicherheitsupdates der Browser und Basiskomponenten (z.B. Java, PDF-Reader, Fernwartungssoftware sowie wichtige Software des Unternehmens).
 - Einsatz und ordnungsgemäße Konfiguration einer Hardware und Software Firewall
 - Ein Sicherheitskonzept für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten ist vorhanden (z.B. Print-to-me, follow-me print, mit PIN)
 - Protokollierungen auf Netzwerk- und Firewall-Ebene, um unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren
-

-
- Interne Netzbereiche unterschiedlicher Sicherheitsstufen werden mittels Firewalls getrennt
-

1.4. Zugriffskontrolle

Die Zugriffskontrolle beschreibt Maßnahmen zur Sicherstellung der ausschließlichen Benutzung von automatisierten Verarbeitungssystemen durch Berechtigte unter ihrer umfassten Zugangsberechtigung und bietet damit Gewährleistung, dass die Berechtigten nur Zugang zu Daten haben, die von ihrer Berechtigung umfasst sind.

Technische Maßnahmen

- Login mit Benutzername & Passwort
 - Einsatz von biometrischen Merkmalen für den Login auf IT-Geräten oder in Sicherheitszonen (z.B. Fingerprint, FaceID etc.)
 - Bei Smartphones: Zugang ausschließlich nach Authentifizierung (z. B. PIN, Passwort)
 - Einsatz von Zwei- oder Mehr-Faktor-Authentifizierung bei Admin-Konten
 - Für die Admin-Konten der IT-Systeme werden ausschließlich starke Passwörter verwendet (z.B. mind. 16 Zeichen, komplex und ohne übliche Wortbestandteile).
 - Nicht-privilegierte Standardkonten auch für Administratoren für die sonstige Arbeit außerhalb der administrativen Tätigkeit.
 - Keine Abhängigkeit des gesamten Betriebs von einzelnen Beschäftigten mit Administratorenkennungen.
 - Sichere Aufbewahrung zentraler Administrationszugangsdaten (z. B. im Tresor) und Zugangsmöglichkeiten im Notfall.
 - Verpflichtende Verwendung starker Passwörter nach aktuellen Empfehlungen (z.B. durch BSI, NIST, ENISA)
 - Passwort Manager im Einsatz
 - Automatische Sperrung des Zugangs bei zu vielen Fehlversuchen (zeitweise oder komplett)
-

Organisatorische Maßnahmen

- Zentrale Passwortvergabe
 - Standard-Authentifizierungsinformationen durch Hersteller bei Software sollten nach Installation geändert werden
 - Verwaltung der Benutzerrechte durch den IT-Administrator
 - Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer (z.B. verschlüsselte Mail, getrennte Briefe für Benutzername und Passwort)
 - Maßnahmen zur Erkennung der Kompromittierung von Passwörtern
-

-
- Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden.

 - Dokumentiertes Berechtigungskonzept inkl. Rollenprofilen für die Beschäftigten um gezielt Zugang zu Informationen zu steuern und reglementieren und zu verwalten.

 - Keine Administratorkennungen für Nutzer, die keine administrativen Tätigkeiten ausführen.

 - Regelmäßige Überprüfung, ob die Zuweisung der Rollen den Vorgaben entspricht sowie, ob die Rollen noch den Anforderungen der Geschäftstätigkeit entspricht.

 - Anzahl der IT-Administratoren auf ein Minimum reduziert
-

1.5. Trennbarkeit

Trennbarkeit beschreibt Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Technische Maßnahmen

- Umsetzung der Mandantentrennung durch Trennung auf Systemebene

 - Umsetzung der Mandantentrennung durch Trennung auf Datenebene
-

Organisatorische Maßnahmen

- Berechtigungskonzept

 - Logische Mandantentrennung (softwareseitig)

 - Trennung von Zugriffen mittels Datenbankrechten
-

1.6 Pseudonymisierung gem. Art. 32 Abs. 1 lit. a) Alt. 1 DSGVO

Pseudonymisierung beschreibt Maßnahmen zur Verarbeitung der Daten in solch eine Form, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die Daten der betroffenen Personen senken. Die Pseudonymisierung ist hinreichend, wenn die De-Pseudonymisierung durch interne Nutzer nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

- nicht relevant, da keine Pseudonymisierung stattfindet bzw. erforderlich ist

2. Integrität der Daten gem. Art. 32 Abs. 1 lit. b) Var. 2 DSGVO

2.1. Übertragungs- und Transportkontrolle

Die Übertragungskontrolle beschreibt Maßnahmen zur Überprüfung des Adressaten der Datenübertragung. Die Transportkontrolle beschreibt Maßnahmen zur Wahrung der Vertraulichkeit und Integrität der Daten bei Transport von Datenträgern.

Technische Maßnahmen

- Transportverschlüsselung wird ausschließlich Ende-zu-Ende implementiert.
 - Bei Massen-E-Mailversand wird die Offenlegung aller Empfänger technisch oder organisatorisch verhindert.
 - Bei Messenger: Einsatz von Transport- und Inhaltsverschlüsselung der Nachrichten und Dateien nach Stand der Technik
 - Einsatz von verschlüsselten und passwortgeschützten Datencontainern (z.B. ZIP, RAR Datei)
 - Keine unverschlüsselten Protokolle (z. B. FTP, Telnet) bei Übertragung von personenbezogenen Daten verwenden
 - Fernwartung für Clients zu IT-Administratorzwecken ausschließlich über verschlüsselte Verbindungen nach Authentifizierung durch den Administrator und Freigabe durch den Nutzer.
-

Organisatorische Maßnahmen

- Sorgfältige Auswahl von Transportpersonal und Fahrzeugen
 - Sichere Transportbehälter/ -verpackungen
 - Beim physischen Transport: persönliche Übergabe mit Protokoll
-

2.2. Eingabekontrolle

Die Eingabekontrolle beschreibt Maßnahmen zur (nachträglichen) Überprüfung, welche personenbezogene Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Technische Maßnahmen

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch personalisierte (eindeutige) Kennungen bei IT-Anwendungen
 - Protokollierungen von Zugriffen auf Server und Betriebssystem, um unbefugte Zugriffe festzustellen und zu analysieren
 - Protokollierungen von Zugriffen auf IT-Applikationen mit kritischen Daten, um unbefugte Zugriffe festzustellen und zu analysieren
 - Regelmäßige anlasslose Auswertung der Protokolle (Log-Dateien) zur Erkennung von ungewöhnlichen Einträgen – bevorzugt: Automatische Heuristiken
-

2.3. Zuverlässigkeit & Datenintegrität

Die Zuverlässigkeit beschreibt Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Die Datenintegrität stellt sicher, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktion des Systems beschädigt werden können.

Technische Maßnahmen

- Nutzung von Signaturverfahren (qualifizierte elektronische Signatur) zur Digitalisierung von Dokumenten
 - Regelmäßige Aktualisierung der Firewall sowie Netzwerkkomponenten
 - Regelmäßige Aktualisierung des Spamfilters
 - Regelmäßige Aktualisierung des Virenschanners
 - Regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall (z. B. mittels Portscans auf die eigenen IP-Adressen)
 - Härtungsmaßnahmen werden umgesetzt (z.B. Einschränkung/Deaktivierung nicht notwendiger Berechtigungen, Ports, Protokolle, Server)
 - Implementierung von Fehlfunktionsalarmen für IT-Systeme, -Applikationen und bei Installation neuer Software
 - Verschlüsselung der Datenbanken von IT-Applikationen mit kritischen Daten (z.B. DATEV)
-

3. Verfügbarkeit und Belastbarkeit der Systeme (Resilienz) gem. Art. 32 Abs. 1 lit. b) Var. 3 DSGVO

3.1. Wiederherstellbarkeit gem. Art. 32 Abs. 1 lit. c) DSGVO

Die Wiederherstellbarkeit beschreibt Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

-
- Dokumentiertes Datensicherungskonzept
 - Dokumentierte Backup-Regelung für Server und Endgeräte
 - Geeigneter Schutz von Backups vor Verschlüsselung durch Ransomware
 - Dokumentiertes Wiederanlaufkonzept (Maßnahmen zur unverzüglichen Wiederherstellung der Verfügbarkeit bei Systemausfall)
 - Kontrolle des Datensicherungsvorganges
 - Regelmäßige Tests zur Datenwiederherstellung und Protokollierung des Vorgangs (Empfehlung: vierteljährlich)
 - Schnelle Wiederherstellung des Disaster Backups
-

-
- Geeignete physische Aufbewahrung von Backup-Medien an einem sicheren Ort außerhalb des Serverraums (z.B. Tresor, Feuerschutz, räumliche Trennung)
 - Aufbewahrung der Datensicherung an einem sicheren Ort, außerhalb des Unternehmens (z.B. externe verschlüsselte Festplatte oder zweiter Server)
-

3.2. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle beschreibt Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen

-
- Serverräume und/oder Rechenzentren verfügen über Rauchmeldeanlagen
 - Serverräume und/oder Rechenzentren verfügen über Feuermeldeanlagen
 - Serverräume und/oder Rechenzentren verfügen über Feuerlöscher bzw. Feuerlöschanlagen
 - Serverräume und/oder Rechenzentren verfügen über ausreichende Klimatisierung
 - Serverräume und/oder Rechenzentren verfügen über Anlagen zur Überwachung von Temperatur und Feuchtigkeit
 - Regelmäßige Kontrollen des Systemzustandes der relevanten Server (Monitoring)
 - Einsatz von Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (USV), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen
 - Serverräume und/oder Rechenzentren verfügen über Schutzsteckdosenleisten
 - RAID-System / Festplattenspiegelung
 - Datenschutzkonforme Videoüberwachung des Serverraums
 - Protokollierung der Zutritte für den Serverraum
 - Es sind keine Brandschutzrisiken vorhanden
 - Physischer Schutz des Serverraums vor Einbruch
 - Keine Risiken durch Überflutung/Starkregen, insbesondere bei Serverräumen im Keller
 - Physischer Schutz des Routers
-

Organisatorische Maßnahmen

-
- Vollständige und aktuelle Netzwerkdokumentation
 - Eine aktuelle Geräteverwaltung bzw. Dokumentation ist vorhanden.
-

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d) Var. 3 DSGVO

Organisationen müssen nicht nur angemessene Sicherheitsmaßnahmen implementieren, sondern auch sicherstellen, dass diese Maßnahmen in regelmäßigen Abständen überprüft und bewertet werden. Dieser Prozess soll sicherstellen, dass die getroffenen Maßnahmen weiterhin wirksam sind und den aktuellen Anforderungen entsprechen, um Datenschutzrisiken zu minimieren.

Organisatorische Maßnahmen

Benennung eines Datenschutzbeauftragten und Kommunikation gegenüber dem Personal.

Abschluss von Auftragsverarbeitungsverträgen mit Unterauftragnehmern gem. Art. 28 DSGVO

Überprüfung der Technisch-Organisatorischen Maßnahmen gem. Art. 32 DSGVO

Zentrale Dokumentation aller Verfahrensanweisungen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter bei Bedarf

Dokumentierter Prozess zur Erkennung, Meldung, Vorgehensweise und Nachbearbeitung von Sicherheits- und Datenschutzvorfällen.

Dokumentation von Sicherheits- und Datenschutzvorfällen (z.B. Ticketsystem)

Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Verzeichnis von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 und 2 DSGVO

5. Sicherheit der Entwicklungsumgebung

5.1. Entwicklung von Software

Datenschutz und Sicherheit müssen frühzeitig bei der Entwicklung von eigenen Softwaresystemen bzw. bei der Auswahl von Softwareprodukten im eigenen Betrieb berücksichtigt werden.

Technische Maßnahmen

- Es findet eine Trennung von Produktivsystem zu Entwicklungs-/Testsystem statt
 - System- und Sicherheitstests, wie z. B. Code-Scan und Penetrationstests werden durchgeführt
 - Der Zugang zum Source-Code bei der Entwicklung von Software ist beschränkt
 - Fortlaufendes Inventarisieren der Versionen von Software oder Komponenten (z. B. Frameworks, Bibliotheken) sowie deren Abhängigkeiten
 - Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen
 - Zeitverzögerungen zwischen mehrmaligen Login-Versuchen (insb. bei Anmeldung über das Internet)
-

Organisatorische Maßnahmen

- Dokumentation eigener IT-Anwendungen (Systembeschreibung, Berechtigungskonzept, Schnittstellen, Reports, Löschkonzept)
 - Keine personenbezogenen Daten oder Zugangsdaten in der Source-Code-Verwaltung ablegen
 - Dateneingaben werden nach semantischen Kriterien validiert (semantic input validation)
 - Zweckattribute sind für Datenfelder und –sätze definiert und umgesetzt worden
 - In der Test- und Entwicklungsumgebung werden nur synthetische Daten, also keine Echtdaten oder personenbezogene Daten verarbeitet.
 - Darstellung der Anzahl fehlgeschlagener Logins für den Nutzer, der sich erfolgreich anmeldet (Ziel: Transparenz für stattgefundene Angriffe/-versuche schaffen)
 - Relevante Mitarbeiter sind darüber geschult, dass Security by-Design (Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität) als Teilmenge von Data-Protection-By-Design eine gesetzliche Datenschutzerfordernung ist und Einfluss auf zentrale Designentscheidungen (Produktauswahl, zentral vs. dezentral, Pseudonymisierung, Verschlüsselung, Land eines Dienstleisters) hat
 - Ausreichende Testzyklen werden berücksichtigt
-

Sicherstellung, dass ein fortlaufender Plan zur Überwachung, Bewertung und Anwendung von Updates oder Konfigurationsänderungen für die gesamte Lebenszeit einer Softwareanwendung besteht

5.2. Entwicklung von Webanwendungen (z.B. Onlineshop, Apps etc.)

Webseiten und Webanwendungen stellen meist leicht zugängliche Plattformen für Angriffe dar, die mit bekannten Best-Practice-Ansätzen meist gut abgesichert werden können.

nicht relevant, da keine Entwicklung von Webanwendungen stattfindet

6. Sicherstellung von weisungsgebundener Verarbeitung gem. Art. 32 Abs. 4 DSGVO

Diese Maßnahmen schützen die Datensicherheit vor internen Beeinträchtigungen und reduzieren das Risiko der Umgehung der technischen Sicherheitsmaßnahmen durch die mit der Datenverarbeitung betrauten unterstellten, natürlichen Personen.

Organisatorische Maßnahmen

Vertraulichkeitsverpflichtung für Auftraggeber

Vertraulichkeitsverpflichtung für Auftragnehmer
