Technische und organisatorische Maßnahmen des Auftragnehmers (TOM) gem. / i. S. d. Art. 5 Abs 1 f, Art. 24, 25, 32, 35, 36 DSGVO

Meinders & Elstermann GmbH & Co. KG
Weberstr. 7
49191 Belm

Versions-Stand: Januar 2022 – 38.1

Inhaltsverzeichnis

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze (DSGVO, BDSG) zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

I. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle der Zutritt durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Server- oder Netzwerkschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen z.B.: Dienstanweisungen zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption mit Pförtner
☒ Chipkarten / Transpondersysteme	☒ Besucherbuch / Protokollierung der Besucher
☒ Manuelles Schließsystem	☒ Mitarbeiter / Besucherausweise
☒ Sicherheitsschlösser	☒ Besucher nur in Begleitung durch Mitarbeiter
☒ Schließsystem durch Codesperre	☒ Sorgfalt bei der Auswahl des Wachpersonals
☒ Absicherung der Gebäudeschächte	☒ Sorgfalt bei der Auswahl der Reinigungsdienste
☒ Türen mit Knauf an der Außenseite	☐
☒ Klingelanlage mit Kamera	☐
☒ Videoüberwachung der Eingänge	☐
☒ Sicherheitsschleusen zu Druck- und Produktionsräumen	☐
☐ Biometrische Zugangssperre	☐
☐	☐

Weitere Maßnahmen bitte hier beschreiben:
-Das Gelände ist komplett umzäunt und Videoüberwacht-

II. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssystem und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B.: Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines sicheren Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername u. Passwort, technisch erzwungen	☒ Verwalten von Benutzerberechtigungen
☐ Login mit biometrischen Daten	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren Lösung Server	☒ Zentrale Passwortvergabe
☒ Anti-Viren Lösung Clients	☒ Richtlinie „Sicheres Passwort“
☒ Anti-Viren Lösung für Mobile Devices	☒ Richtlinie “Löschen / Vernichten“
☒ Firewall	☒ Richtlinie „Clean Desk“
☒ Intrusion Detection Systeme	☒ Allgemeine Richtline Datenschutz und Sicherheit
☒ Mobile Device Management	☐ Mobile Device Policy
☒ Einsatz von VPN Tunneln bei Remote-Zugriffen, Fernwartungstätigkeiten	☒ Anleitung „Manuelle Desktopsperre“
☒ Verschlüsselung von Datenträgern	☐
☐ Verschlüsselung Smartphones	☐
☐ Gehäuseverriegelung, Verplombungen	☐
☐ BIOS Schutz durch extra Passwort	☐
☒ Sperre externer Schnittstellen (USB)	☐
☒ Automatische Desktopsperre	☐
☐ Verschlüsselung von Laptops / Tabletts	☐
☐	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

III. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die Ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen, als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B.: bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Aktenvernichter (min. Stufe 3, cross cut)	☒ Einsatz von Berechtigungskonzepten
☒ Externer Aktenvernichter (Dienstleister) nach DIN 32757	☒ Minimale Anzahl von Administratoren
☒ Protokollierung von Zugriffen	☒ Verwaltung der Benutzerrechte durch entsprechende Verantwortliche
☒ Physische Löschung von Datenträgern	☐ Datenschutztresor
☒ Checkup der Benutzerrollen durch IT Management-Routinen	☐
☐	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

IV. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Trennung von Produktiv- und Testumgebungen	☒ Steuerung über Berechtigungskonzepte
☒ Physikalische Trennung (Systeme, Datenbanken, Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Datensätze sind mit Zweckattributen versehen
☒ Interne / Externe Mandantenfähigkeit	☐ Trennung Pseudonym-Zuordnungsmerkmale
☒ Einsatz von Subnetzen	☐
☒	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

V. Pseudonymisierung gem. Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehen 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.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung der Zuordnungsdaten und Aufbewahrung in einem getrennten und abgesicherten System (je nach Aufwand auch möglichst verschlüsselt)	☒ Interne Anweisungen, personenbezogene Daten im Fall einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
☐	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

2. Integrität gem. Art. 32 Abs 1 lit. b DSGVO

I. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B.: Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. der Datenweitergabe sind Transitbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ E- Mail Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Einsatz von VPN	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒ Protokollierung der Zugriffe und Abrufe	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☐ Persönliche Übergabe mit Protokoll

☒ Bereitstellung der Daten über verschlüsselte Verbindungen wie sftp, https (soweit gefordert)	☐ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Nutzung von Signaturverfahren	☐
☐	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

II. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, on und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B.: Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass / Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
☐	☒ Aufbewahrung von Formularen, von denen Daten in die automatisierte Verarbeitung übernommen wurden
☐	☒ Klare Zuständigkeiten für Datenlöschungen
☐	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

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

I. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Festplattenspiegelungen, etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup Recovery Konzept (ausformuliert)
☒ Feuerlöscher vor und / oder im Serverraum	☒ Regelmäßige Tests zur Datenwiderherstellung und Protokollierung der Ergebnisse
☒ Serverraumüberwachung, Temperatur	☒ Aufbewahrung von Sicherungsmedien außerhalb des Serverraums
☒ Klimatisierter Serverraum	☒ Aufbewahrung von Sicherungsmedien in einem anderen Brandschutzbereich
☒ USV (unterbrechungsfreie Stromversorgung) – keine Generatoren	☐ Existenz eines (kommunizierten) Notfallplans / Eskalationsplans (Z.B.: DSI IT Grundschutz 1004)
☒ Schutzsteckdosenleisten im Serverraum	☒ Kontrolle des Sicherungsvorgangs
☐ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quell-Dichtung, etc.)	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ RAID Systeme	☒ Getrennte Partitionen für Betriebssysteme und Daten
☐ Videoüberwachung in Serverräumen	☐
☒ Alarm-Meldungen bei unberechtigtem Zutritt zum Serverraum	☐
☐	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

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

I. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Software Lösung für das Datenschutz Management im Einsatz (beim externen Datenschützer)	☒ Ein externes Datenschutzunternehmen wurde bestellt
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf / Berechtigung (z.B.: Intranet, Wikki, etc.)	☒ Mitarbeiter sind geschult und auf Vertraulichkeit und das Datengeheimnis verpflichtet
☒ Anderweitig dokumentiertes Sicherheitskonzept	☒ Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird min. jährlich durchgeführt und dokumentiert	☒ Interner / Externer Informationssicherheits-Beauftragter
☐	☒ Die Datenschutzfolgenabschätzung (DSFA) wird bei Bedarf durchgeführt
☐	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
☐	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

II. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen
☒ Einsatz von Spamfiltern und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen gegenüber den Aufsichtsbehörden
☒ Einsatz von Virenscannern und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Intrusion Detection System (IDS)	☒ Einbindung von DSB und ISB bei Daten-Pannen und Sicherheitsvorfällen
☒ Intrusion Prevention System (IPS)	☒ Dokumentation via Ticketsystem
☐	☒ Formeller Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Daten-pannen
☐	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

III. Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DSGVO (Privacy by design / Privacy by default)

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐
☒ Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahme(n)	☐

Ihre Maßnahmen bitte hier beschreiben:
-keine-

IV. **Auftragskontrolle** (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Remote / Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☐	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
☐	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. der EU-Standardvertragsklauseln
☐	☒ Schriftliche Weisungen an alle Auftragnehmer
☐	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
☐	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Bestellpflicht
☐	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☒ Sicherstellung der Vernichtung von daten nach Beendigung des Auftrags
☐	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Ihre Maßnahmen bitte hier beschreiben:
-keine-

Sonstige Punkte als Ergänzungen:

-keine-

Alternativ:

☒ Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.

Als Datenschutzbeauftragter wurde benannt:
trans-acta Datenschutz GmbH
Egbert-Snoek-Str. 1
48155 Münster
datenschutz@trans-acta.de
0251-70 38 99-0

Ausgefüllt für die Organisation durch:
trans-acta Datenschutz GmbH
Bernd van Straelen
Egbert-Snoek-Str. 1
48155 Münster
datenschutz@trans-acta.de
0251-70 38 99-0

Vom Auftraggeber auszufüllen:

Geprüft am: _____ durch: _____

Ergebnis(se):

Es besteht noch Klärungsbedarf zu: _____

☐ TOM sind für den angestrebten Schutzzweck ausreichend

☐ Vereinbarung zur Auftragsverarbeitung kann geschlossen werden