



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

1.0 Vertraulichkeit

- 1.1 Zutrittskontrolle
- 1.2 Zugangskontrolle
- 1.3 Zugriffskontrolle
- 1.4 Trennungskontrolle
- 1.5 Pseudonymisierung

2.0 Integrität

- 2.1 Weitergabekontrolle
- 2.2 Eingangskontrolle

3.0 Verfügbarkeit und Belastbarkeit

- 3.1 Verfügbarkeitskontrolle

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- 4.1 Datenschutz-Maßnahmen
- 4.2 Incident-Response-Management
- 4.3 Datenschutzfreundliche Voreinstellungen
- 4.4 Auftragskontrolle (Outscoring an Dritte)

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
<input checked="" type="checkbox"/> Alarmanlage	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input checked="" type="checkbox"/> Automatisches Zugangskontrollsystem	<input checked="" type="checkbox"/> Empfang / Rezeption mit Pförtner
<input checked="" type="checkbox"/> Chipkarten / Transpondersysteme	<input checked="" type="checkbox"/> Besucherbuch / Protokollierung der Besucher
<input checked="" type="checkbox"/> Manuelles Schließsystem	<input checked="" type="checkbox"/> Mitarbeiter / Besucherausweise
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Besucher nur in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Schließsystem durch Codesperre	<input checked="" type="checkbox"/> Sorgfalt bei der Auswahl des Wachpersonals
<input checked="" type="checkbox"/> Absicherung der Gebäudeschächte	<input checked="" type="checkbox"/> Sorgfalt bei der Auswahl der Reinigungsdienste
<input checked="" type="checkbox"/> Türen mit Knauf an der Außenseite	<input type="checkbox"/>
<input checked="" type="checkbox"/> Klingelanlage mit Kamera	<input type="checkbox"/>
<input checked="" type="checkbox"/> Videoüberwachung der Eingänge	<input type="checkbox"/>
<input checked="" type="checkbox"/> Sicherheitsschleusen zu Druck- und Produktionsräumen	<input type="checkbox"/>
<input type="checkbox"/> Biometrische Zugangssperre	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

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

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
<input checked="" type="checkbox"/> Aktenvernichter (min. Stufe 3, cross cut)	<input checked="" type="checkbox"/> Einsatz von Berechtigungskonzepten
<input checked="" type="checkbox"/> Externer Aktenvernichter (Dienstleister) nach DIN 32757	<input checked="" type="checkbox"/> Minimale Anzahl von Administratoren
<input checked="" type="checkbox"/> Protokollierung von Zugriffen	<input checked="" type="checkbox"/> Verwaltung der Benutzerrechte durch entsprechende Verantwortliche
<input checked="" type="checkbox"/> Physische Löschung von Datenträgern	<input type="checkbox"/> Datenschutztresor
<input checked="" type="checkbox"/> Checkup der Benutzerrollen durch IT Management-Routinen	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

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
<input checked="" type="checkbox"/> Trennung von Produktiv- und Testumgebungen	<input checked="" type="checkbox"/> Steuerung über Berechtigungskonzepte
<input checked="" type="checkbox"/> Physikalische Trennung (Systeme, Datenbanken, Datenträger)	<input checked="" type="checkbox"/> Festlegung von Datenbankrechten
<input checked="" type="checkbox"/> Mandantenfähigkeit relevanter Anwendungen	<input checked="" type="checkbox"/> Datensätze sind mit Zweckattributen versehen
<input checked="" type="checkbox"/> Interne / Externe Mandantenfähigkeit	<input type="checkbox"/> Trennung Pseudonym-Zuordnungsmerkmale
<input checked="" type="checkbox"/> Einsatz von Subnetzen	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>



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
<input checked="" type="checkbox"/> Trennung der Zuordnungsdaten und Aufbewahrung in einem getrennten und abgesicherten System (je nach Aufwand auch möglichst verschlüsselt)	<input checked="" type="checkbox"/> Interne Anweisungen, personenbezogene Daten im Fall einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
<input type="checkbox"/>	<input type="checkbox"/>

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
<input checked="" type="checkbox"/> E- Mail Verschlüsselung	<input checked="" type="checkbox"/> Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
<input checked="" type="checkbox"/> Einsatz von VPN	<input checked="" type="checkbox"/> Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
<input checked="" type="checkbox"/> Protokollierung der Zugriffe und Abrufe	<input type="checkbox"/> Weitergabe in anonymisierter oder pseudonymisierter Form
<input type="checkbox"/> Sichere Transportbehälter	<input type="checkbox"/> Persönliche Übergabe mit Protokoll



<input checked="" type="checkbox"/> Bereitstellung der Daten über verschlüsselte Verbindungen wie sftp, https (soweit gefordert)	<input type="checkbox"/> Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
<input checked="" type="checkbox"/> Nutzung von Signaturverfahren	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Ihre Maßnahmen bitte hier beschreiben:

-keine-

II. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob 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
<input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
<input checked="" type="checkbox"/> Manuelle oder automatisierte Kontrolle der Protokolle	<input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
<input type="checkbox"/>	<input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
<input type="checkbox"/>	<input checked="" type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in die automatisierte Verarbeitung übernommen wurden
<input type="checkbox"/>	<input checked="" type="checkbox"/> Klare Zuständigkeiten für Datenlöschungen
<input type="checkbox"/>	<input type="checkbox"/>

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, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Festplattenspiegelungen, etc.

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

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

Ihre Maßnahmen bitte hier beschreiben:

-keine-



II. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

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

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
<input checked="" type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	<input type="checkbox"/>
<input checked="" type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahme(n)	<input type="checkbox"/>



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
<input type="checkbox"/>	<input checked="" type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
<input type="checkbox"/>	<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
<input type="checkbox"/>	<input checked="" type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. der EU-Standardvertragsklauseln
<input type="checkbox"/>	<input checked="" type="checkbox"/> Schriftliche Weisungen an alle Auftragnehmer
<input type="checkbox"/>	<input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
<input type="checkbox"/>	<input checked="" type="checkbox"/> Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Bestellpflicht
<input type="checkbox"/>	<input checked="" type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
<input type="checkbox"/>	<input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
<input type="checkbox"/>	<input checked="" type="checkbox"/> 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
-