

Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DS-GVO

Name des Verantwortlichen:

Stand: -----

Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO, 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 DSGVO zu gewährleisten. Erforderlich sind diese Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Der o. g. Verantwortliche erfüllt diesen Anspruch durch folgende Maßnahmen: **1.**

Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DS-GVO

1.1. 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 des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
E Alarmanlage	E Schlüsselregelung / Liste
E Automatisches Zugangskontrollsystem	E Empfang / Rezeption / Pförtner
E Biometrische Zugangssperren	E Besucherbuch / Protokoll der Besucher
E Chipkarten / Transpondersysteme	E Mitarbeiter- / Besucherausweise
E Manuelles Schließsystem	E Besucher in Begleitung durch Mitarbeiter
E Sicherheitsschlösser	E Sorgfalt bei Auswahl des Wachpersonals
E Schließsystem mit Codesperre	E Sorgfalt bei Auswahl Reinigungsdienste
E Absicherung der Gebäudeschächte	E
E Türen mit Knäuf Außenseite	E
E Klingelanlage mit Kamera	E
E Videoüberwachung der Eingänge	E
E	E

1.2. 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 Betriebssysteme 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 „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Login mit Benutzername + Passwort	<input type="checkbox"/> Verwalten von Benutzerberechtigungen
<input type="checkbox"/> Login mit biometrischen Daten	<input type="checkbox"/> Erstellen von Benutzerprofilen
<input type="checkbox"/> Anti-Viren-Software Server	<input type="checkbox"/> Zentrale Passwortvergabe
<input type="checkbox"/> Anti-Virus-Software Clients	<input type="checkbox"/> Richtlinie „Sicheres Passwort“
<input type="checkbox"/> Anti-Virus-Software mobile Geräte	<input type="checkbox"/> Richtlinie „Löschen / Vernichten“
<input type="checkbox"/> Firewall	<input type="checkbox"/> Richtlinie „Clean desk“
<input type="checkbox"/> Intrusion Detection Systeme	<input type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input type="checkbox"/> Mobile Device Management	<input type="checkbox"/> Mobile Device Policy
<input type="checkbox"/> Einsatz VPN bei Remote-Zugriffen	<input type="checkbox"/> Anleitung „Manuelle Desktopsperre“
<input type="checkbox"/> Verschlüsselung von Datenträgern	<input type="checkbox"/>
<input type="checkbox"/> Verschlüsselung Smartphones	<input type="checkbox"/>
<input type="checkbox"/> Gehäuseverriegelung	<input type="checkbox"/>
<input type="checkbox"/> BIOS Schutz (separates Passwort)	<input type="checkbox"/>
<input type="checkbox"/> Sperre externer Schnittstellen (USB)	<input type="checkbox"/>
<input type="checkbox"/> Automatische Desktopsperre	<input type="checkbox"/>
<input type="checkbox"/> Verschlüsselung von Notebooks / Tablet	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.3. 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 type="checkbox"/> Aktenschredder (mind. Stufe 3, cross cut)	<input type="checkbox"/> Einsatz Berechtigungskonzepte
<input type="checkbox"/> Externer Aktenvernichter (DIN 32757)	<input type="checkbox"/> Minimale Anzahl an Administratoren
<input type="checkbox"/> Physische Löschung von Datenträgern	<input type="checkbox"/> Datenschutztesor
<input type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.4. 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 type="checkbox"/> Trennung von Produktiv- und Testumgebung	<input type="checkbox"/> Steuerung über Berechtigungskonzept
<input type="checkbox"/> Physikalische Trennung (Systeme / Datenbanken / Datenträger)	<input type="checkbox"/> Festlegung von Datenbankrechten
<input type="checkbox"/> Mandantenfähigkeit relevanter Anwendungen	<input type="checkbox"/> Datensätze sind mit Zweckattributen versehen
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	<input type="checkbox"/> Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Email-Verschlüsselung (S/MIME / PGP) <input type="checkbox"/> Email-Signatur (S/MIME / PGP)	<input type="checkbox"/> Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
<input type="checkbox"/> Einsatz von VPN	<input type="checkbox"/> Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
<input type="checkbox"/> Protokollierung der Zugriffe und Abrufe	<input type="checkbox"/> Weitergabe in anonymisierter oder pseudonymisierter Form
<input type="checkbox"/> Sichere Transportbehälter	<input type="checkbox"/> Sorgfalt bei Auswahl von Transport-

	Personal und Fahrzeugen
<input type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	<input type="checkbox"/> Persönliche Übergabe mit Protokoll
<input type="checkbox"/> Nutzung von Signaturverfahren	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

2.2. 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 type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input type="checkbox"/> Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
<input type="checkbox"/> Manuelle oder automatisierte Kontrolle der Protokolle	<input type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
<input type="checkbox"/>	<input type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
<input type="checkbox"/>	<input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
<input type="checkbox"/>	<input type="checkbox"/> Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1. 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, Raidssysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Feuer- und Rauchmeldeanlagen	<input type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input type="checkbox"/> Feuerlöscher Serverraum	<input type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input type="checkbox"/> Serverraumüberwachung Temperatur und Feuchtigkeit	<input type="checkbox"/> Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
<input type="checkbox"/> Serverraum klimatisiert	<input type="checkbox"/> Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
<input type="checkbox"/> USV	<input type="checkbox"/> Keine sanitären Anschlüsse im oder

	oberhalb des Serverraums
<input type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT Grundsatz 100-4)
<input type="checkbox"/> Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quellsicherung etc.)	<input type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten
<input type="checkbox"/> RAID System / Festplattenspiegelung	<input type="checkbox"/>
<input type="checkbox"/> Videoüberwachung Serverraum	<input type="checkbox"/>
<input type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Software-Lösungen für Datenschutz-Management im Einsatz	<input type="checkbox"/> Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
<input type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	<input type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
<input type="checkbox"/> Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundsatz oder ISIS12 <input type="checkbox"/> Alternatives Informationssicherheitskonzept	<input type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
<input type="checkbox"/> Anderweitiges dokumentiertes Sicherheitskonzept	<input type="checkbox"/> Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt
<input type="checkbox"/> Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	<input type="checkbox"/> Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
<input type="checkbox"/>	<input type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DS-GVO nach
<input type="checkbox"/>	<input type="checkbox"/> Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung	<input type="checkbox"/> Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
<input type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	<input type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
<input type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	<input type="checkbox"/> Einbindung von <input type="checkbox"/> DSB und <input type="checkbox"/> ISB in Sicherheitsvorfälle und Datenpannen
<input type="checkbox"/> Intrusion Detection System (IDS)	<input type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
<input type="checkbox"/> Intrusion Prevention System (IPS)	<input type="checkbox"/> Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	<input type="checkbox"/>
<input type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.4 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 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 type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
<input type="checkbox"/>	<input type="checkbox"/> Auswahl des Auftragnehmers unter

	Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
<input type="checkbox"/>	<input type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
<input type="checkbox"/>	<input type="checkbox"/> Schriftliche Weisungen an den Auftragnehmer
<input type="checkbox"/>	<input type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
<input type="checkbox"/>	<input type="checkbox"/> Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellopflicht
<input type="checkbox"/>	<input type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
<input type="checkbox"/>	<input type="checkbox"/> Regelung zum Einsatz weiterer Subunternehmer
<input type="checkbox"/>	<input type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
<input type="checkbox"/>	<input type="checkbox"/> Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

alternativ:

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

5. Anlagen (optional)

- ☐ Verzeichnis zu den Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten (Art. 30 Abs. 2 DS-GVO)
- ☐ Liste der eingesetzten Subunternehmer mit Tätigkeiten für Sie als Auftraggeber
- ☐ Richtlinie Datenschutz
- ☐ Richtlinie Umgang mit Datenpannen
- ☐ Übersicht der Sensibilisierungs- und Schulungsmaßnahmen der letzten 24 Monate
- ☐
- ☐

Bitte fügen Sie nichts bei, was bei unberechtigter Kenntnisnahme ein Sicherheitsrisiko für Ihre Organisation darstellen kann.

Ausgefüllt für die Organisation durch:

Name	:
Funktion	:
Rufnummer	:
Email	:

Seite 7 | 8

Ort, Datum -----

Vom Auftraggeber auszufüllen:

Geprüft am -----durch -----

Ergebnis(se):

☐ Es besteht noch Klärungsbedarf zu -----

☐ TOM sind für den angestrebten Schutzzweck ausreichend.