Technische und organisatorische Maßnahmen (TOM)
i.S.d. Art. 32 DSGVO

Der Organisation

_____

Stand

_____

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 zu gewährleisten.
Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o. g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

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

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

- ☐ Alarmanlage
- ☐ Automatisches Zugangskontrollsystem
- ☐ Biometrische Zugangssperren
- ☐ Chipkarten / Transpondersysteme
- ☐ Manuelles Schließsystem
- ☐ Sicherheitsschlösser
- ☐ Schließsystem mit Codesperre
- ☐ Absicherung der Gebäudeschächte
- ☐ Türen mit Knauf Außenseite
- ☐ Klingelanlage mit Kamera
- ☐ Videoüberwachung der Eingänge

// Organisatorische Maßnahmen

- ☐ Schlüsselregelung / Liste
- ☐ Empfang / Rezeption / Pförtner
- ☐ Besucherbuch / Protokoll der Besucher
- ☐ Mitarbeiter- / Besucherausweise
- ☐ Besucher in Begleitung durch Mitarbeiter
- ☐ Sorgfalt bei Auswahl des Wachpersonals
- ☐ Sorgfalt bei Auswahl Reinigungsdienste

Weitere Maßnahmen: _____

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

- ☐ Login mit Benutzername + Passwort
- ☐ Login mit biometrischen Daten
- ☐ Anti-Viren-Software Server
- ☐ Anti-Virus-Software Clients
- ☐ Anti-Virus-Software mobile Geräte
- ☐ Firewall
- ☐ Intrusion Detection Systeme
- ☐ Mobile Device Management
- ☐ Einsatz VPN bei Remote-Zugriffen
- ☐ Verschlüsselung von Datenträgern
- ☐ Verschlüsselung Smartphones
- ☐ Gehäuseverriegelung
- ☐ BIOS Schutz (separates Passwort)
- ☐ Sperre externer Schnittstellen (USB)
- ☐ Automatische Desktopsperre
- ☐ Verschlüsselung von Notebooks / Tablet

// Organisatorische Maßnahmen

- ☐ Verwalten von Benutzerberechtigungen
- ☐ Erstellen von Benutzerprofilen
- ☐ Zentrale Passwortvergaber
- ☐ Richtlinie „Sicheres Passwort"
- ☐ Richtlinie „Löschen / Vernichten"
- ☐ Richtlinie „Clean desk"
- ☐ Allg. Richtlinie Datenschutz und / oder Sicherheit
- ☐ Mobile Device Policy
- ☐ Anleitung „Manuelle Desktopsperre"

Weitere Maßnahmen: _____

_____

_____

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 zurichten.

// Technische Maßnahmen

- ☐ Aktenschredder (mind. Stufe 3, cross cut)
- ☐ Externer Aktenvernichter (DIN 32757)
- ☐ Physische Löschung von Datenträgern
- ☐ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

// Organisatorische Maßnahmen

- ☐ Einsatz Berechtigungskonzepte
- ☐ Minimale Anzahl an Administratoren
- ☐ Datenschutztresor
- ☐ Verwaltung Benutzerrechte durch Administratoren

Weitere Maßnahmen: _____

_____

_____

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

- ☐ Trennung von Produktiv- und Testumgebung
- ☐ Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- ☐ Mandantenfähigkeit relevanter Anwendungen

// Organisatorische Maßnahmen

- ☐ Steuerung über Berechtigungskonzept
- ☐ Festlegung von Datenbankrechten
- ☐ Datensätze sind mit Zweckattributen versehen

Weitere Maßnahmen: _____

_____

_____

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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

- ☐ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)

// Organisatorische Maßnahmen

- ☐ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

Weitere Maßnahmen: _____

_____

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.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 zurichten.

// Technische Maßnahmen

- ☐ Email-Verschlüsselung
- ☐ Einsatz von VPN
- ☐ Protokollierung der Zugriffe und Abrufe
- ☐ Sichere Transportbehälter
- ☐ Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- ☐ Nutzung von Signaturverfahren

// Organisatorische Maßnahmen

- ☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- ☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- ☐ Weitergabe in anonymisierter oder pseudonymisierter Form
- ☐ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
- ☐ Persönliche Übergabe mit Protokoll

Weitere Maßnahmen: _____

_____

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

- ☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☐ Manuelle oder automatisierte Kontrolle der Protokolle

// Organisatorische Maßnahmen

- ☐ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- ☐ 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 Berechtigungskonzepts
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- ☐ Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen: _____

_____

_____

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

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, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

// Technische Maßnahmen

- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Feuerlöscher Serverraum
- ☐ Serverraumüberwachung Temperatur und Feuchtigkeit
- ☐ Serverraum klimatisiert
- ☐ USV
- ☐ Schutzsteckdosenleisten Serverraum
- ☐ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)
- ☐ RAID System / Festplattenspiegelung
- ☐ Videoüberwachung Serverraum
- ☐ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum

// Organisatorische Maßnahmen

- ☐ Backup & Recovery-Konzept (ausformuliert)
- ☐ Kontrolle des Sicherungsvorgangs
- ☐ Regelmäßige Tests zur Datenwiederher-Herstellung und Protokollierung der Ergebnisse
- ☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- ☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- ☐ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
- ☐ Getrennte Partitionen für Betriebssysteme und Daten

Weitere Maßnahmen: _____

_____

_____

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

4.1. Datenschutz-Managemen

// Technische Maßnahmen

- ☐ Software-Lösungen für Datenschutz-Management im Einsatz
- ☐ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)
- ☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12
- ☐ Anderweitiges dokumentiertes Sicherheits-Konzept
- ☐ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

// Organisatorische Maßnahmen

- ☐ Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
- ☐ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
- ☐ Regelmäßige Sensibilisierung der Mitarbeiter/ mindestens jährlich
- ☐ Interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt
- ☐ Die Datenschutz- Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- ☐ Die Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach
- ☐ Formalisierter Prozeß zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Weitere Maßnahmen: _____

_____

_____

4.2. Datenschutz-Managemen

// Technische Maßnahmen

- ☐ Einsatz von Firewall und regelmäßige Aktualisierung
- ☐ Einsatz von Spamfilter und regelmäßige Aktualisierung
- ☐ Einsatz von Virenscanner und regelmäßige Aktualisierung
- ☐ Intrusion Detection System (IDS)
- ☐ Intrusion Prevention System (IPS)

// Organisatorische Maßnahmen

- ☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Melde-- pflicht gegenüber Aufsichtsbehörde)
- ☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ☐ Einbindung von ☐ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen
- ☐ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
- ☐ Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheits- vorfällen und Datenpannen

Weitere Maßnahmen: _____

_____

_____

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

// Technische Maßnahmen

- ☐ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- ☐ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

// Organisatorische Maßnahmen

- ☐ -

Weitere Maßnahmen: _____

_____

_____

4.4. Datenschutz-Management

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

- ☐ 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. EU Standard-Vertragsklauseln
- ☐ Schriftliche Weisungen an den Auftragnehmer
- ☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- ☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
- ☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- ☐ Regelung zum Einsatz weiterer Subunternehmer
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen: _____

_____

_____

Alternativ:

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

Ausgefüllt für die Organisation durch

Name _____

Funktion _____

Rufnummer _____

Email _____

Ort, Datum _____

Unterschrift _____

// Vom Auftraggeber auszufüllen:

Geprüft am _____ durch _____

Ergebnis(se):

☐ Es besteht noch Klärungsbedarf zu _____

☐ TOM sind für den angestrebten Schutzzweck ausreichend

☐ Vereinbarung Auftragsverarbeitung kann geschlossen werden

Unterschrift _____

Format GmbH | Industriestraße 10-24 | D-37235 Hessisch Lichtenau
Tel.: 05602 939-69 | info@format-tresorbau.de | www.format-tresorbau.de