

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

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

a. Zutrittskontrolle

Unter Zutrittskontrollen sind Maßnahmen verstehen, 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
<input checked="" type="checkbox"/> Alarmanlage	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input checked="" type="checkbox"/> Automatisches Zugangskontrollsystem	<input checked="" type="checkbox"/> Empfang / Rezeption / Pförtner
<input checked="" type="checkbox"/> Biometrische Zugangssperren	<input type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input checked="" type="checkbox"/> Chipkarten / Transpondersysteme	<input checked="" type="checkbox"/> Mitarbeiter- / Besucherausweise
<input type="checkbox"/> Manuelles Schließsystem	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals
<input checked="" type="checkbox"/> Schließsystem mit Codesperre	<input type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input type="checkbox"/> Absicherung der Gebäudeschächte	
<input checked="" type="checkbox"/> Türen mit Knauf Außenseite	
<input checked="" type="checkbox"/> Klingelanlage mit Kamera	
<input checked="" type="checkbox"/> Videoüberwachung der Eingänge	

b. Zugangskontrolle

Unter Zugangskontrollen sind Maßnahmen zu verstehen, 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 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 checked="" type="checkbox"/> Login mit Benutzername + Passwort	<input 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-Software Server	<input checked="" type="checkbox"/> Zentrale Passwortvergabe
<input checked="" type="checkbox"/> Anti-Virus-Software Clients	<input checked="" type="checkbox"/> Richtlinie „Sicheres Passwort“
<input type="checkbox"/> Anti-Virus-Software mobile Geräte	<input 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"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input type="checkbox"/> Mobile Device Management	<input type="checkbox"/> Mobile Device Policy

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

<input checked="" type="checkbox"/> Einsatz VPN bei Remote-Zugriffen	<input checked="" type="checkbox"/> Anleitung „Manuelle Desktopsperre“
<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern	
<input type="checkbox"/> Verschlüsselung Smartphones	
<input type="checkbox"/> Gehäuseverriegelung	
<input type="checkbox"/> BIOS Schutz (separates Passwort)	
<input type="checkbox"/> Sperre externer Schnittstellen (USB)	
<input checked="" type="checkbox"/> Automatische Desktopsperre	
<input checked="" type="checkbox"/> Verschlüsselung von Notebooks / Tablet	

c. Zugriffskontrolle

Unter Zugriffskontrollen sind Maßnahmen zu verstehen, 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"/> Aktenschredder (mind. Stufe 3, cross cut)	<input checked="" type="checkbox"/> Einsatz Berechtigungskonzepte
<input type="checkbox"/> Externer Aktenvernichter (DIN 66399)	<input checked="" type="checkbox"/> Minimale Anzahl an Administratoren
<input checked="" type="checkbox"/> Physische Löschung von Datenträgern	<input type="checkbox"/> Datenschutztresor
<input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren

d. Trennungskontrolle

Unter Trennungskontrollen sind Maßnahmen zu verstehen, 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 Testumgebung	<input checked="" type="checkbox"/> Steuerung über Berechtigungskonzept
<input checked="" type="checkbox"/> Physikalische Trennung (Systeme / Datenbanken / Datenträger)	<input checked="" type="checkbox"/> Festlegung von Datenbankrechten
<input checked="" type="checkbox"/> Mandantenfähigkeit relevanter Anwendungen	<input type="checkbox"/> Datensätze sind mit Zweckattributen versehen

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

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

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

a. Weitergabekontrolle

Unter Weitergabekontrolle sind Maßnahmen zu verstehen, 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 checked="" type="checkbox"/> Email-Verschlüsselung	<input 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 checked="" 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 checked="" type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	<input checked="" type="checkbox"/> Persönliche Übergabe mit Protokoll
<input type="checkbox"/> Nutzung von Signaturverfahren	<input type="checkbox"/>

b. Eingabekontrolle

Unter Eingabekontrolle sind Maßnahmen zu verstehen, 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

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

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 type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	<input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	<input checked="" type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	<input checked="" type="checkbox"/> Klare Zuständigkeiten für Löschungen

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

a. Verfügbarkeitskontrolle

Unter Verfügbarkeitskontrolle sind Maßnahmen zu verstehen, 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, Raidsysteme, Plattenspiegelungen etc.. Diese Angaben beziehen sich auf das Rechenzentrum.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen	<input checked="" type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input checked="" type="checkbox"/> Feuerlöscher Serverraum	<input checked="" type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input checked="" type="checkbox"/> Serverraumüberwachung Temperatur und Feuchtigkeit	<input checked="" type="checkbox"/> Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
<input checked="" type="checkbox"/> Serverraum klimatisiert	<input checked="" type="checkbox"/> Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
<input checked="" type="checkbox"/> USV	<input type="checkbox"/> Keine sanitären Anschlüsse im oder oberhalb des Serverraums
<input checked="" type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input checked="" type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
<input type="checkbox"/> Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quellsicherung etc.)	<input checked="" type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten
<input checked="" type="checkbox"/> RAID System / Festplattenspiegelung	
<input checked="" type="checkbox"/> Videoüberwachung Serverraum	
<input checked="" type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

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

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

a. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Software-Lösungen für Datenschutz-Management im Einsatz	<input checked="" type="checkbox"/> Interner / externer Datenschutzbeauftragter Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 5 93047 Regensburg Tel.: 0941-298693-0 Fax: 0941-298693-16 Mail: info@projekt29.de Web: www.projekt29.de
<input type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	<input checked="" type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
<input type="checkbox"/> Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	<input checked="" type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
<input type="checkbox"/> Anderweitiges dokumentiertes Sicherheits-Konzept	<input type="checkbox"/> Interner / externer Informationssicherheits- Beauftragter/ CISO Name / Firma Kontakt
<input checked="" type="checkbox"/> Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	<input checked="" type="checkbox"/> Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	<input checked="" type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	<input type="checkbox"/> Formalisierter Prozeß zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

b. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" 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 checked="" type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	<input type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

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

<input checked="" type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Einbindung von <input checked="" type="checkbox"/> DSB und <input checked="" type="checkbox"/> ISO in Sicherheitsvorfälle und Datenpannen
<input checked="" type="checkbox"/> Intrusion Detection System (IDS)	<input checked="" type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
<input checked="" type="checkbox"/> Intrusion Prevention System (IPS)	<input type="checkbox"/> Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

c. Datenschutzfreundliche Voreinstellungen (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"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	

d. Auftragskontrolle (Outsourcing an Dritte)

Unter Auftragskontrolle sind Maßnahmen zu verstehen, 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 checked="" type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	<input checked="" type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard Vertragsklauseln
	<input checked="" type="checkbox"/> Schriftliche Weisungen an den Auftragnehmer
	<input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	<input checked="" type="checkbox"/> Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht

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

	<input checked="" type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	<input checked="" type="checkbox"/> Regelung zum Einsatz weiterer Subunternehmer
	<input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	<input checked="" type="checkbox"/> Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus