ratiokontakt GmbH

Technisch-organisatorische Maßnahmen (TOM)

Technisch-organisatorische Maßnahmen (TOM)

Einleitung

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.

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.

Technische Maßnahmen:

- elektronisches Zugangskontrollsystem
- Manuelles Schließsystem
- Sicherheitsschlösser
- Türen mit Knauf Außenseite
- Videoüberwachung

Organisatorische Maßnahmen:

- Schlüsselregelung und dokumentierte Schlüsselvergabe
- Richtlinien für betriebsfremde Personen, z. B. durchgängige Besucheraufsicht
- Sorgfalt bei der Dienstleister-Auswahl

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen:

- Passwortrichtlinien
- Anti-Viren-Software
- Firewall-Systeme
- Geräteverschlüsselung
- BIOS-Schutz
- Automatische Displaysperren

Organisatorische Maßnahmen:

- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Allgemeine Sicherheitsrichtlinien, z. B. für Passwörter, Löschung und „Clean Desk“
- Mobile Device Policies

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.

Technische Maßnahmen:

- Aktenvernichter
- Physische Löschung von Datenträgern
- Protokollierungen

Organisatorische Maßnahmen:

- Einsatz von Berechtigungskonzepten
- Minimale Anzahl an Administratoren
- Verwaltung der Benutzerrechte durch Administratoren

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen:

- Trennung von Produktiv- und Testumgebungen

- Trennung von Netzen und Systemen
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)

Organisatorische Maßnahmen:

- Steuerung über Berechtigungskonzept
- Mandantenfähigkeit relevanter Anwendungen

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 im getrennten und abgesicherten System (mögl. verschlüsselt)
- Transportverschlüsselung

Organisatorische Maßnahmen:

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

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.

Technische Maßnahmen:

- Einsatz von VPN
- Einsatz sicherer Transportbehälter
- Verschlüsselungen und Passwortschutz

Organisatorische Maßnahmen:

- Dokumentation der Datenempfänger, geplanten Überlassung bzw. der Löschfristen
- Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- Weitergabe in anonymisierter oder pseudonymisierter Form
- Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
- Bereitstellung über verschlüsselte Verbindungen
- Persönliche Übergabe mit Protokoll

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.

Technische Maßnahmen:

- Technische Protokollierungen
- 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

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.

Technische Maßnahmen:

- Feuer- und Rauchmeldeanlagen, Feuerlöscher
- Serverraumüberwachung Temperatur und Feuchtigkeit / Klimatisierung
- Schutzsteckdosenleisten, Überspannungsschutz
- RAID-Systeme / Festplattenspiegelung
- Unterbrechungsfreie Stromversorgung (USV)
- Notstromversorgung (Dieselgenerator)

Organisatorische Maßnahmen:

- Backup- und Recovery-Konzept
- Monitoring
- Notfallplan
- Videoüberwachung

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

DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

Technische Maßnahmen:

- Software-Lösung für Datenschutz-Management
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter
- Sicherheitszertifizierung nach ISO 27001
- Regelmäßige Überprüfung der Wirksamkeit

Organisatorische Maßnahmen:

- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter
- Die Datenschutz-Folgenabschätzung (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

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen:

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung

Organisatorische Maßnahmen:

- Prozess zur Erkennung und Meldung von Sicherheitsvorfällen
- Prozess zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
- Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

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

Privacy by design / Privacy by default

Technische Maßnahmen:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

4.4. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Organisatorische Maßnahmen:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Auswahl unter Sorgfaltsgesichtspunkten in Bezug auf Datenschutz und Datensicherheit
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Vereinbarung von Kontrollrechten gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers