

TOM – Technische und organisatorische Maßnahmen

Beispiel für eine Darstellung und für mögliche Maßnahmen. Die Maßnahmen sind weder vollständig, noch abschließend.

HINWEIS: Das Dokument ist unbedingt auf die tatsächlichen Gegebenheiten Ihres Unternehmens anzupassen!

1. Organisation - Organisatorische Maßnahmen sollen einen Schutz der Daten durch Struktur, Aufklärung, Schulung, Vorgaben und Verpflichtungen gewährleisten.

* Es wurde geprüft, ob der Unternehmen gemäß der DSGVO einen Datenschutzbeauftragten benennen muss
* Verantwortlichkeiten zum Datenschutz wurden bestimmt
* Eine zuständige Ansprechperson für Datenschutz ist intern und extern kommuniziert
* Verantwortlichkeiten zur IT-Sicherheit und Administration von Software wurden bestimmt
* Alle Beschäftigten werden bei Aufnahme ihrer Tätigkeit schriftlich auf die Vertraulichkeit bei der Verarbeitung von personenbezogenen Daten verpflichtet
* Alle Beschäftigten wurden über den Umgang mit Betroffenenrechten informiert
* Alle Beschäftigten wurden darüber informiert, was im Fall von Sicherheitsvorfällen und Datenschutzvorfällen zu tun ist
* Es gibt gesonderte Datenschutzschulungen für neue Beschäftigte, sofern es für die jeweilige Funktion und Tätigkeit relevant ist
* Es gibt Regelungen zum Einsatz privater IT-Geräte und der Arbeit in privaten Räumlichkeiten (Home Office / Mobiles Arbeiten)
* Es gibt eine Regelung zum Speichern von Daten
* Es gibt eine Reglung zum Vernichten und Löschen von Dokumenten und Daten
* Die Auswahl von Reinigungsdiensten, Wachpersonal und Datenvernichtungsfirma erfolgt mit Sorgfalt

1. Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

**2.1 Zutritt - Die Maßnahmen zum Zutritt sollen einen unbefugten physikalischen Zutritt zu Räumlichkeiten verhindern, in denen personenbezogene Daten verarbeitet oder verwahrt werden.**

* Der Zutritt in die Geschäftsräume erfolgt mit einem Transponderchip bzw. mit einem Schlüssel
* Die Tür zu den Geschäftsräumen ist verschlossen. Besucher müssen klingeln und werden während des Besuches durch die Geschäftsräume begleitet
* Eine Videoüberwachung des Gewerbehofes erfolgt über den Vermieter
* Der Zutritt zu den Büro-Arbeitsplätzen erfolgt nur mit Schlüssel zum Büro für die dafür befugten Personen
* Der Zutritt zu Räumen mit IT-Technik oder/und Telefonanlage und Archiv erfolgt nur für einen eingeschränkten Personenkreis
* IT-Technik ist in abschließbaren IT-Gehäusen untergebracht

**2.2 Zugang - Die Maßnahmen zum Zugang sollen einen unbefugten Zugang auf personenbezogene Daten und an Datenverarbeitungsgeräten verhindern.**

* Die Anmeldung / Authentifizierung am Büro-Arbeitsplatz erfolgt mit einem individuellen Benutzernamen und Passwort
* Es existiert eine Passwortregelung, welche bei bestimmten Systemen um eine technisch erzwungene Passwortregelung unterstützt wird
* Arbeitscomputer enthalten eine technisch erzwungene Bildschirmsperre
* Benutzerberechtigungen für die IT-Systeme sind dokumentiert und werden zentral verwaltet
* Einsatz von Anti-Viren-Software auf Servern, Clients, Mobilen Geräten
* Einsatz von Firewalls
* Grundsätzliche Festplattenverschlüsselung der mobilen Geräte (Laptops) mit BitLocker
* Alle Büro-Arbeitsplätze wurden auf Thin-Clients umgestellt
* USB-Schnittstellen sind grundsätzlich gesperrt
* Alle Aktenschränke sind grundsätzlich abschließbar und stehen in den jeweiligen Büros zur Verfügung
* Für alle Büro-Arbeitsplätze und für Aushängbereiche existiert eine „Clean-Desk-Policy“
* Kopiergeräte und Multifunktionsgeräte stehen in geschützten Bereichen und sind grundsätzlich nicht für Dritte zugänglich

2.3 Zugriff - Die Maßnahmen zum Zugriff sollen den direkten auf die personenbezogenen Daten verhindern bzw. erschweren sollen.

* Die Anmeldung / Authentifizierung für die jeweilig genutzte Software erfolgt mit einem individuellen Benutzernamen und Passwort
* Für die Erteilung und Entziehung von Zugriffsrechten einzelner Ordner und Softwareanwendungen existiert ein interner Freigabe- und Prüf-Prozess
* Jeder Standort verfügt über einen Shredder der Schutzklasse IV

2.4 Trennungskontrolle - Die Trennungskontrolle soll sicherstellen, dass Datenbestände für unterschiedliche Zwecke getrennt verarbeitet werden.

* Die eingesetzte Software verfügt über eine Mandantentrennung
* Unterschiedliche Personenkategorien werden in getrennten Datenbeständen verarbeitet (Beschäftigtendaten / Kundendaten / Kontaktdaten für Newsletter / Lieferantendaten)
* Unterschiedliche Verarbeitungszwecke werden mit eingegrenzten Zugriffsrechten durchgeführt und der Zugriff aus Daten wird minimiert

2.5 Pseudonymisierung - Bei einer Pseudonymisierung können die Daten nicht mehr einer spezifischen Person zugeordnet werden, ohne dass zusätzliche Informationen hinzugezogen werden müssen. Der Zugriff auf diese zusätzlichen Informationen ist entsprechend zu reglementieren.

* Im Falle einer Pseudonymisierung werden die Zuordnungsdaten in getrennten Systemen gespeichert und ein Zugriff reduziert
* Im Falle einer Pseudonymisierung von besonderen Kategorien von Daten (z.B. Gesundheitsdaten) werden die Zuordnungsdaten in getrennten Systemen gespeichert, verschlüsselt und ein Zugriff reduziert

1. Maßnahmen zur Integrität

3.1 Weitergabekontrolle - Die Maßnahmen zur Weitergabekontrolle sollen sicherstellen, 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.

* Einsatz von Signaturverfahren
* Verschlüsselung von Datenübermittlung mit sensiblen Daten (z.B. Sozialdaten, Lohnangaben)
* Protokollierung von Zugriffen, Änderungen in Softwareanwendungen
* Einsatz von VPN auf das Firmennetzwerk
* Bereitstellung verschlüsselter Internet-Verbindungen über ssl, https, sftp

3.2 Eingabekontrolle - Die Maßnahmen zur Eingabekontrolle sollen sicherstellen, dass – im Nachhinein - nachgeprüft werden kann, ob und vom wem Daten z.B. gelöscht oder verändert wurden.

* Automatisierte Protokollierung von Zugriffen und Änderungen in Softwareanwendungen
* Kontrolle der Protokolldateien im Verdachtsfall
* Automatisierte Kontrolle der Protokolldaten

1. Maßnahmen zur Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

4.1 Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit - Diese Maßnahmen sollen sicherstellen, dass die Daten stets für die relevante Verarbeitung und auch in Stoßzeiten verfügbar sind und bei Verlust oder Zerstörung schnell wiederhergestellt werden können.

* Für Räume mit IT-Technik sind folgende Maßnahmen erfolgt:
  + Trockene Umgebung ohne Sanitäre Anschlüsse
  + Feuer- und Rauchmelder
  + Klimaanlage und Temperaturanzeiger
  + Unterbrechungsfreie Stromversorgung (USV) des Servers
  + Restriktive Zutrittsrechte
  + Begleitung von Wartung- und Reinigungspersonal
* Regelmäßiges Einspielen von Sicherheitssoftware (Patchen)
* Ausreichende und skalierbare Rechnerkapazitäten
* Regelmäßige Datenspeicherung auf Grundlage eines Back-Up-Konzeptes
* Regelmäßige Tests zur Widerherstellung von Daten
* Es existiert ein Notfallhandbuch
* Unser IT-Dienstleister verfügt über alle relevanten IT-Sicherheitszertifikate