TOM-Checkliste DSGVO

Systematische Prüfung aller technischen und organisatorischen Maßnahmen zur datenschutzkonformen Datenverarbeitung nach Art. 32 DSGVO für Unternehmen jeder Größe mit praxisorientierten Kontrollpunkten.

Diese Checkliste hilft Ihnen, alle erforderlichen technischen und organisatorischen Maßnahmen (TOM) nach DSGVO systematisch zu prüfen. Haken Sie alle umgesetzten Maßnahmen ab und identifizieren Sie Optimierungspotenziale.

1. Zutrittskontrolle

Unbefugten den physischen Zugang zu Datenverarbeitungsanlagen verwehren

- ☐ Alarmanlagen, Chipkarten oder Sicherheitsschlösser installiert
- ☐ Besucheranmeldung und Besucherprotokolle vorhanden
- ☐ Ausweispflicht für Besucher geregelt
- ☐ Serverräume und Datenschränke physisch gesichert

2. Zugangskontrolle

Unbefugte an der Nutzung von Datenverarbeitungssystemen hindern

- ☐ Passwortrichtlinien definiert und durchgesetzt (Länge, Komplexität, Wechselintervalle)
- ☐ Firewall und Anti-Viren-Software aktiv
- ☐ VPN-Zugang für Remote-Arbeit eingerichtet
- ☐ Automatische Bildschirmsperre bei Inaktivität aktiv
- ☐ Mobile Geräte verschlüsselt

3. Zugriffskontrolle

Nur berechtigte Nutzer auf bestimmte Daten zugreifen lassen

- ☐ Berechtigungskonzept definiert (Rollen, Zugriffsrechte)
- ☐ Minimierung der Admin-Zugänge umgesetzt
- ☐ Zugriffsprotokollierung aktiv
- ☐ Datenschutzkonforme Datenvernichtung geregelt

4. Weitergabekontrolle

Daten bei Übertragung und Transport schützen

- ☐ E-Mail-Verschlüsselung (TLS/SSL) eingerichtet
- ☐ VPN-Technologie für Datenübertragung genutzt
- ☐ Übermittlungsprotokolle geführt
- ☐ Datenempfänger dokumentiert

5. Eingabekontrolle

Nachvollziehbarkeit von Datenänderungen gewährleisten

- ☐ Protokollierung aller Änderungen eingerichtet
- ☐ Individuelle Benutzernamen für alle Mitarbeiter
- ☐ Differenzierte Zugriffsberechtigungen vergeben

6. Auftragskontrolle

Weisungsgemäße Verarbeitung durch Auftragsverarbeiter sicherstellen

- ☐ Auftragsverarbeitungsverträge (AVV) mit allen Dienstleistern geschlossen
- ☐ TOM der Auftragsverarbeiter vor Vertragsabschluss geprüft
- ☐ Schriftliche Weisungen an Auftragsverarbeiter erteilt
- ☐ Regelmäßige Kontrollen durchgeführt

7. Verfügbarkeit & Wiederherstellbarkeit

Daten gegen Verlust schützen und nach Störungen wiederherstellen

- ☐ Backup-Strategie definiert und umgesetzt
- ☐ Regelmäßige Wiederherstellungstests durchgeführt
- ☐ Unterbrechungsfreie Stromversorgung (USV) installiert
- ☐ Feuer- und Rauchmelder in Serverräumen
- ☐ Notfallpläne vorhanden und getestet

8. Trennungskontrolle

Daten verschiedener Zwecke getrennt verarbeiten

- ☐ Mandantentrennung bei Datenbanken umgesetzt
- ☐ Zweckspezifische Datenbankrechte vergeben
- ☐ Verschlüsselung zweckgebundener Datensätze

9. Dokumentation & Nachweis

Lückenlose Nachweisführung sicherstellen

- ☐ Verzeichnis von Verarbeitungstätigkeiten (VVT) vollständig
- ☐ TOM in allen Verarbeitungsverzeichnissen dokumentiert
- ☐ Risikoanalyse durchgeführt und dokumentiert
- ☐ Datenschutz-Folgenabschätzung (DSFA) bei Hochrisikoverarbeitungen
- ☐ Mitarbeiter-Schulungen nachweisbar dokumentiert
- ☐ Regelmäßige TOM-Überprüfung (mindestens jährlich) geplant

---