Risikoanalyse und technisch-organisatorische Maßnahmen (TOMs)

In Art 32 Abs 1 Datenschutz-Grundverordnung wird die „Sicherheit der Verarbeitung" behandelt. Es wird darauf hingewiesen, dass sogenannte „technisch-organisatorische Maßnahmen" (kurz TOMs) getroffen werden müssen, um eine sichere Datenverarbeitung zu gewährleisten und das Risiko für die Rechte und Freiheiten von Betroffenen zu minimieren.

Dafür kann es, je nach Risiko der Datenverarbeitung und der verarbeiteten Datenkategorien, unterschiedliche Notwendigkeiten geben. Die folgende Checkliste bietet eine Auswahl möglicher technisch-organisatorischer Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme auf Dauer sicherzustellen.

TOMs	Ja	Nein	Notizen/Ergänzungen
Zugangskontrolle			
Personenkontrolle beim Empfang			
Besucherprotokoll			
Schlüsselmanagement			
Videoüberwachung des Eingangsbereichs			
Sichtbare Ausweispflicht			
Sicherheitsschlösser			
Chipkartensysteme			
Automatische Schließsysteme			
Sicherheitspersonal			
Benutzerverwaltung			
Zugriffsrechte und -verwaltung			
Anmeldeprotokolle			
Datenträgerkontrolle			
Bestandslisten			
Datenträgerarchiv			
Versperrte Aufbewahrung für Datenträger			
Versperrte Gehäuse			
Kopierkontrolle und Dokumentation			
Verschlüsselung von gespeicherten Daten auf Datenträgern			
Adäquate Datenträgerentsorgung			
Sicheres Löschen von Datenträgern vor Wiederverwendung			
Speicherkontrolle			
Identifikationssysteme für Benutzerzugriffe			
Eingeschränkte Lese- und Schreibrechte			
Protokollierung des Benutzerverhaltens			
Automatische Bildschirmsperrung nach Inaktivität			

TOMs	Ja	Nein	Notizen/Ergänzungen
Zugriffsprotokoll			
Starke Verschlüsselung			
Benutzerkontrolle			
Individuelle Benutzerprofile			
Rollenbasierte Zugangsbeschränkungen			
Passwortregelungen			
Authentifikation mit Benutzer-ID und Passwort			
Authentifikation mit biometrischen Daten			
Verschlüsselung			
Kopierprotokolle			
Clear-Desk-Policy			
Zugriffskontrolle			
Sicherung von Schnittstellen (z.B. USB)			
Unberechtigte Netzwerkzugriffe per MAC-Adressensperrung verhindern			
Trennung Gast-WLAN und internes Netzwerk			
Automatisierte Berechtigungsprüfung			
Berechtigungsmanagementsystem			
Zeitliche Begrenzung von Zugriffen			
Kontrolle der Datenvernichtung			
Übertragungskontrolle			
Klare Richtlinien für Datenweitergabe intern/extern			
Übermittlungsprotokoll			
Dokumentierte Empfangsbestätigungen			
Eingabekontrolle			
Benutzerauthentifizierung			
Änderungs- und Löschprotokolle			
Protokollauswertungssysteme mit Plausibilitätsprüfung			
Individuelle elektronische Signaturen bzw. Benutzer			
Richtlinien zur Softwarenutzung für Erstellung und Änderung von Dokumenten			
Transportkontrolle			
Einsatz von Transportverschlüsselung (https)			
E-Mail-Verschlüsselung (PGP, S/Mime)			
Nutzung von VPNs zur verschlüsselten Datenübertragung			
Vollverschlüsselung von Datenträgern			

TOMs	Ja	Nein	Notizen/Ergänzungen
Sicheres Löschen vor und nach Datenträgernutzung			
Verwendung von vertrauenswürdigen Botendiensten			
Gesicherte Transportbehälter			
Siegelsysteme			
Überwachung des Transportweges und der Transportzeit			
Protokollierung des Ein- und Ausganges von Datenträgern			
Wiederherstellung			
Automatisierte und regelmäßige Datensicherung			
Integritätstests der Sicherungskopien			
Redundante IT-Systeme			
Einsatz von RAID-Systemen			
Regelmäßige Überprüfung des Backupmanagements			
Sichere Lagerung von Backupdatenträgern			
Datenintegrität			
Änderungsprotokolle			
Signatur und Hashwerte von gespeicherten Dateien			
Vier-Augen-Prinzip			
Einsatz von Firewalls			
DDOS-Schutz			
Notfall- und Backuppläne			