

## Technische und organisatorische Maßnahmen nach Art. 32 der DSGVO

Art. 32 der DSGVO verpflichtet Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Diese Dokumentation wird fortlaufend ergänzt und angepasst. Sie ist unter gleicher URL in der jeweils aktuellen Fassung abrufbar.

### 1. Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird.

technische Maßnahme	organisatorische Maßnahme
Transponder-Schließsystem für Bürokomplex	Besucher bewegen sich in den Räumlichkeiten ausschließlich mit zugewiesenen Mitarbeitern.
Sicherheitsschlösser	Schlüsselbuch
	Rückgabe Transponder/Schlüssel bei Ausscheiden eines Mitarbeiters.

### 2. Datenträgerkontrolle

Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können.

technische Maßnahme	organisatorische Maßnahme
VPN-Tunnel	
Standleitung	
Aktenvernichter	

### 3. Speicherkontrolle

Die Speicherkontrolle soll verhindern, dass Unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern und löschen können.

technische Maßnahme	organisatorische Maßnahme
Einsatz von Anti-Viren-Software	Passwortrichtlinie/Passwortregeln inkl. Passwortlänge, Passwortwechsel.
Einsatz von Firewalls	Benutzerberechtigungen verwalten
Einsatz von VPN-Technologie	Differenzierte Berechtigung für Daten, Anwendungen und Betriebssystem
	Bildschirm Sperre aufheben nur mit Benutzer und Passwort
	Differenzierte Berechtigung für Daten, Anwendungen und Betriebssystem

4. Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberichtigung umfassten personenbezogenen Daten Zugang haben.

technische Maßnahme	organisatorische Maßnahme
	Passwortrichtlinie/Passwortregeln inkl. Passwortlänge, erzwungener Passwortwechsel.
Einsatz von Anti-Viren-Software	Benutzerberechtigungen verwaltet durch Systemadministrator
Einsatz von Firewalls	Differenzierte Berechtigung für Daten, Anwendungen und Betriebssystem
Einsatz von Mobile Device Management	Bildschirm Sperre aufheben nur mit Benutzer und Passwort
Einsatz von VPN-Technologie	Besucher bewegen sich in den Räumlichkeiten ausschließlich mit zugewiesenen Mitarbeitern.
	Anzahl der Administratoren auf das „Notwendigste“ reduziert

5. Wiederherstellbarkeit

Die Wiederherstellbarkeit soll gewährleisten, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

technische Maßnahme	organisatorische Maßnahme
	Backup & Recoverykonzept
	Testen von Datenwiederherstellungen
	Erstellen eines Notfallplans

6. Zuverlässigkeit

Die Zuverlässigkeit soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

technische Maßnahme	organisatorische Maßnahme
	Backup & Recoverykonzept
	Testen von Datenwiederherstellungen
	Monitoring