

Technisch- und organisatorische Maßnahmen

Security allgemein		
Informationssicherheitsleitlinie	Security Policy	Art. 32 (1) lit. d DSGVO
Definierte Verantwortlichkeiten	Incident Management - Workflow	Art. 32 (1) lit. d DSGVO
Definierte Verantwortlichkeiten	Incident Management - Verantwortlichkeiten und Vorgaben	Art. 32 (1) lit. d DSGVO
Definierte Verantwortlichkeiten	Compliance Prüfungen	Art. 32 (1) lit. d DSGVO
End User		
Sichere Infrastruktur	Verwendung sicherer Systeme	Art. 32 (1) lit. b DSGVO
Sichere Infrastruktur	nur ausgewählte Personen haben	Art. 32 (1) lit. b DSGVO
Zugangskontrolle	benutzerspezifische Passwortvergabe für Clients	Art. 32 (1) lit. b DSGVO
Zugangskontrolle	sichere Passwortvergabe / Änderung	Art. 32 (1) lit. b DSGVO
Zugangskontrolle	Passwortpolicy mit mind. 3 Komplexitätsanforderungen	Art. 32 (1) lit. b DSGVO
Zugangskontrolle	Sperrung des Accounts bei zu vielen ungültigen Anmeldeversuchen	Art. 32 (1) lit. b DSGVO
Zugangskontrolle	Kontosperrung größer 30 Minuten bei zu vielen ungültigen Anmeldeversuchen	Art. 32 (1) lit. b DSGVO
Zugangskontrolle	Zentrale Benutzerverwaltung	Art. 32 (1) lit. b DSGVO
Zugriffskontrolle	Berechtigungsverwaltung für Laufwerke und Applikationen	Art. 32 (1) lit. b DSGVO
Zugriffskontrolle	Berechtigungsverwaltung gruppenbasiert	Art. 32 (1) lit. b DSGVO
Virenschutz	Virenschutzkonzept	Art. 32 (1) lit. b DSGVO
Virenschutz	Incident Management	Art. 32 (1) lit. b DSGVO
Change Management	Regelmäßige Betriebssystemupdates	Art. 32 (1) lit. b DSGVO
Change Management	Regelmäßige Updates der Applikationen	Art. 32 (1) lit. b DSGVO
Laptops		
Verschlüsselung	Übertragungsverschlüsselung	Art. 32 (1) lit. a DSGVO
Endpoint Security	weitere Schutzmaßnahmen am Client	Art. 32 (1) lit. b DSGVO
Mobile Endgeräte		
Sichere Infrastruktur	Sichere Administration	Art. 32 (1) lit. b DSGVO
Zugriffskontrolle	Passwortschutz / Pin	Art. 32 (1) lit. b DSGVO
Sichere Verwaltung der Mobilgeräte	Device Management	Art. 32 (1) lit. b DSGVO
Sichere Verwaltung der Mobilgeräte	Change Management bei Änderungen	Art. 32 (1) lit. b DSGVO
Zugangskontrolle	Berechtigungsverwaltung bei Zugriffen auf Unternehmensressourcen	Art. 32 (1) lit. b DSGVO
Dokumentation der IT	Arbeitsanweisungen	Art. 32 (1) lit. c DSGVO
Dokumentation der IT	Netzpläne	Art. 32 (1) lit. c DSGVO
Selbstkontrolle	Serverraum	Art. 32 (1) lit. d DSGVO
Zutritt		
Zutrittskontrolle	Schlüssel / ID	Art. 32 (1) lit. b DSGVO
Zutrittskontrolle	Berechtigte Personen werden erfasst	Art. 32 (1) lit. b DSGVO
Zutrittskontrolle	Berechtigungsvergabe mit Freigabe	Art. 32 (1) lit. b DSGVO
Brandmeldeanlage		
Brandschutz	Brandmeldeanlage / Rauchmelder	Art. 32 (1) lit. b DSGVO
Definierte Verantwortlichkeiten	Incident Management	Art. 32 (1) lit. d DSGVO
Bandschutz	Feuerlöscher	Art. 32 (1) lit. b DSGVO
USV / Notstrom		

Business Continuity Management (BCM)	Notstrom - USV Vorhanden	Art. 32 (1) lit. c DSGVO
Business Continuity Management (BCM)	Notstrom - USV überbrückt bei Stromausfall Zeit bis zum Herunterfahren der Server oder bis zur Übernahme eines Notstromaggregats	Art. 32 (1) lit. c DSGVO
Definierte Verantwortlichkeiten	Incident Management	Art. 32 (1) lit. d DSGVO
Kühlung		
Business Continuity Management (BCM)	Temperaturregulierung	Art. 32 (1) lit. c DSGVO
Business Continuity Management (BCM)	Temperaturüberwachung	Art. 32 (1) lit. c DSGVO
Server		
Sichere Infrastruktur	OnPremise Systeme werden sicher administriert	Art. 32 (1) lit. b DSGVO
Business Continuity Management (BCM)	Redundante Stromversorgung	Art. 32 (1) lit. c DSGVO
Business Continuity Management (BCM)	Redundante Netzwerkanbindung	Art. 32 (1) lit. c DSGVO
Change Management	Regelmäßige Betriebssystemupdates	Art. 32 (1) lit. b DSGVO
Definierte Verantwortlichkeiten	Benannte Serveradministratoren	Art. 32 (1) lit. d DSGVO
Zugriffskontrolle	Berechtigte Personen haben administrative Rechte für einzelne Aufgaben (z.B. Applikationen)	Art. 32 (1) lit. b DSGVO
Virenschutz	Virenschutzkonzept	Art. 32 (1) lit. b DSGVO
Definierte Verantwortlichkeiten	Incident Management	Art. 32 (1) lit. d DSGVO
System-Monitoring	Serverüberwachung	Art. 32 (1) lit. d DSGVO
Sichere Infrastruktur	E-Mail System	Art. 32 (1) lit. b DSGVO
Verschlüsselung	Übertragungsverschlüsselung	Art. 32 (1) lit. a DSGVO
Sichere Infrastruktur	ERP System	Art. 32 (1) lit. b DSGVO
Sichere Infrastruktur	Serverapplikationen	Art. 32 (1) lit. b DSGVO
Backup		
Backup-Konzept	Backup-System	Art. 32 (1) lit. b DSGVO
Backup-Konzept	Backup erfolgt auf eigenes Medium	Art. 32 (1) lit. b DSGVO
Backup-Konzept	Backup Monitoring	Art. 32 (1) lit. b DSGVO
Backup-Konzept	Incident Management	Art. 32 (1) lit. b DSGVO
Backup-Konzept	Berechtigte Personen werden bei nicht erfolgreicher Sicherung informiert	Art. 32 (1) lit. b DSGVO
Backup-Konzept	Wiederherstellung wird geprüft	Art. 32 (1) lit. b DSGVO
Netzwerk		
Firewall		
Sichere Infrastruktur	Firewall	Art. 32 (1) lit. b DSGVO
Business Continuity Management (BCM)	Notstrom	Art. 32 (1) lit. c DSGVO
Sichere Infrastruktur	Netzwerkadministratoren (personalisiert)	Art. 32 (1) lit. b DSGVO
Sichere Infrastruktur	Passwortschutz für die Firewall	Art. 32 (1) lit. b DSGVO
Sichere Infrastruktur	getrennte Netze (extern / Intern)	Art. 32 (1) lit. b DSGVO
Backup-Konzept	Firewallbackup	Art. 32 (1) lit. b DSGVO
System-Monitoring	Firewallmonitoring	Art. 32 (1) lit. d DSGVO
WLAN		
Sichere Infrastruktur	WLAN für Clients aktiv	Art. 32 (1) lit. b DSGVO
Verschlüsselung	WLAN Verschlüsselung	Art. 32 (1) lit. a DSGVO
Zugangskontrolle	Authorisierung	Art. 32 (1) lit. b DSGVO

LAN		
Definierte Verantwortlichkeiten	Netzwerkadministratoren	Art. 32 (1) lit. d DSGVO
Zugangskontrolle	Netzwerkadministratoren	Art. 32 (1) lit. b DSGVO
Zugangskontrolle	Passwortschutz (individuelle Passwörter)	Art. 32 (1) lit. b DSGVO
Business Continuity Management (BCM)	Notstrom	Art. 32 (1) lit. c DSGVO
Physikalische Sicherheit		
Gebäude		
Zutrittskontrolle	Gebäude	Art. 32 (1) lit. b DSGVO
Zutrittskontrolle	Schlüssel / ID	Art. 32 (1) lit. b DSGVO
Zutrittskontrolle	Dokumentation der Rechtevergabe	Art. 32 (1) lit. b DSGVO
Einbruch und Feuerschutz		
Brandschutz	Rauchmelder	Art. 32 (1) lit. b DSGVO
Weitere Schutzmaßnahmen		
Trennungskontrolle	Mandantenfähigkeit, Sandboxing	Art. 32 (1) lit. b DSGVO