

Technische und organisatorische Maßnahmen zum Datenschutz

Da wir uns als Maßstab gesetzt haben unsere technischen und organisatorischen Maßnahmen kontinuierlich zu verbessern entnehmen Sie bitte unserer Website die aktuelle Version. Sie finden unsere Datenschutzdokumentation unter dem Menüpunkt DSGVO auf www.msp-nord.de

Vertraulichkeit

Zutrittskontrolle
Dokumentation der Vergabe von Schlüsseln
Rückgabe von Schlüsseln Austritt von Mitarbeitern
Verwendung einer Alarmanlage
Verwendung einer Video-Überwachung (Eingangsbereich, POS Bereich)
Verwendung sicherer Türen und Fenster

Zugangskontrolle
Anwendung von Maßnahmen zur Verschlüsselung von lokalen Daten (z. B. Festplatten, Server)
Automatisches Sperren von PCs/Macs nach 5 Minuten
Verwendung personalisierter Logins im Unternehmensnetzwerk
Verwendung sicherer und individueller Passwörter
Zwei-Faktor-Authentifizierung für Monitoring Plattform Solarwinds

Zugriffskontrolle
Dokumentation eingerichteter Zugänge für Mitarbeiter
Einführung von Benutzer- und Rollenkonzepten für interne Systeme
Sperrung von Zugängen nach Austritt von Mitarbeitern
Zentrale Verwaltung von Benutzerzugängen und -rechten

Weitergabekontrolle

Nutzung SSL-verschlüsselter Übertragungswege im Internet

Sicherung von Dokumenten beim Versand auf dem Postweg (z. B. undurchsichtige Versandhüllen)

Verschlüsselter Versand von E-Mails (S/MIME, PGP)

Verwendung digitaler Signaturen für Dateien und E-Mails

Verwendung von VPN-Systemen zum Login in das Firmennetzwerk

Trennungskontrolle

Einführung von Zugriffsberechtigungen für interne Systeme

Trennung von internem WLAN und Gäste-WLAN

Trennung von Live- und Entwicklungssystemen

Verbot der Nutzung von privaten Endgeräten im Firmennetzwerk

Pseudonymisierung

Trennung von Kundenstammdaten und Auftragsdaten in ERP Software

Verschlüsselung

Verwendung verschlüsselter Übertragungswege für den Datenaustausch

Verwendung von Maßnahmen zur verschlüsselten Datenspeicherung (Backup)

Verwendung von SSL-Zertifikaten für Hostingumgebungen

Integrität

Eingabekontrolle
Einführung von Benutzer- und Rollenkonzepten für interne Systeme
Einführung individueller Zugänge für interne Systeme
Protokollierung von Zugriffen im Firmennetzwerk
Verwendung personalisierter Logins im Unternehmensnetzwerk

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle
Regelmäßige Aktualisierung der Virendefinitionen
Regelmäßige Durchführung von Datensicherungen
Regelmäßige Durchführung von Updates (Windows, Mac, Linux, Desktopanwendungen)
Regelmäßige Überprüfung der erstellten Datensicherungen
Verwendung von Rauchmeldern in Räumlichkeiten
Verwendung einer Firewall (Securepoint)
Verwendung eines Intrusion Detection Systems (Securepoint)
Verwendung eines Virenschanners (Bitdefender & Securepoint)
Verwendung einer unterbrechungsfreien Stromversorgung (USV) für interne Systeme
Verwendung eines Überspannungsschutzes für interne Systeme
Verwendung von RAID-Systemen (Server und VM-Hostsysteme)

Rasche Wiederherstellbarkeit
Dokumentation und Test von Datenwiederherstellungen (automatisiert via Datto Backuplösung)
Erstellung von Notfallplänen zu kritischen Prozesse
Regelmäßiger Testdurchlauf von Notfallplänen zu kritischen Prozesse

Weitere Maßnahmen

Datenschutz-Managementsystem
Dokumentation von datenschutzrelevanten Zwischenfällen
Löschen nicht mehr benötigter Daten (z. B. veraltete Daten, Testumgebungen)
Sichere Entsorgung defekter/nicht mehr benötigter Hardware
Sichere Entsorgung von Dokumenten (externer Dienstleister)
GEO Lokalisierung von mobilen Endgeräten
GEO Lokalisierung von Firmenfahrzeugen

Auftragskontrolle
Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden
Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten
Beauftragung zertifizierter Dienstleister (z. B. TÜV-zertifiziertes Hosting)
Beratung/Aufklärung der Kunden zum Thema Datenschutz
Durchführung von stichprobenartigen Überprüfungen bei Dienstleistern
Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter
Regelmäßige Unterweisung und Fortbildung der Mitarbeiter zum Thema Datenschutz
Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter