Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

digitalNORD GmbH (DSM)

Sicherheitskonzept

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogen und jährlich evaluiert wird.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
- Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
- Mitarbeiter werden regelmäßig zu den Themen Datenschutz und IT-Sicherheit sensibilisiert.
- Es werden Awareness-Maßnahmen (z.B. Phishing-Kamapagnen) durchgeführt.

Zutrittskontrolle

- Alarmanlage
- Sicherheitsschlösser
- Zutrittsregelungen für betriebsfremde Personen
- Geregelte Zutrittsberechtigung Serverraum
- Verschließbarer Serverschrank
- Chipkarten-/Transponder-Schließsystem
- Türen mit Knauf Außenseite
- Gebäudeschachtsicherung

Zugangskontrolle / Zugriffskontrolle

- Automatische Bildschirm-Sperrung mit Kennwortschutz (minimum 10 Minuten)
- Authentifikation mit Benutzer und Passwort und bei erhöhtem Schutzbedarf durch eine zusätzliche Multifaktor-Authentisierung (2FA)
- Festlegung der Zugriffsrechte
- Komplexe Passwörter
- Firewall (Hardware + Software)
- Stets aktueller Virenschutz
- Stets aktuelle Softwareversionen
- Ordnungsgemäße Vernichtung von Datenträgern
- Verschlüsselung von mobilen Datenträgern und mobilen Endgeräten
- Sicheres Löschen von Datenträgern (HDD, SSD, USB-Sticks, etc.) vor Weitergabe
- Berechtigungs-/ Authentifizierungskonzepte mit auf Nötigste beschränkten Zugriffsregulierungen
- Richtlinie Homeoffice/mobiles Arbeiten
- Verschlüsselung Webseite
- Einrichtung eines Gäste-WLAN
- Einsatz von VPN-Technologie
- Schnittstellensperrung
- Einsatz von Intrusion-Detection-Systemen
- WLAN mit regelmäßiger Passwortänderung
- Nutzung eines Passwortmanagers
- Protokollierung von Zugriffen auf Daten

Weitergabekontrolle

- Verschlüsselter Versand von Dateien
- Verschlüsselung von Datenträgern und Verbindungen
- Dedizierte Weitergabeberechtigungen

Eingabekontrolle

- Berechtigungskonzept
- Veränderungsprotokollierung

Auftragskontrolle

- Auswahl und Kontrolle von Auftragnehmern unter Sorgfaltsgesichtspunkten
- Schriftliche Festlegung der Weisungen
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Verfügbarkeitskontrolle / Integrität

- Notfallkonzept
- Ständig kontrolliertes Backup- und Recoverykonzept
- Dezentrale Aufbewahrung
- Unterbrechungsfreie Stromversorgung und Überspannungsschutz
- Einsatz von Festplattenspiegelung

Gewährleistung des Zweckbindungs-/Trennungsgebotes

- Logische Mandantentrennung (Software)
- Trennung von Produktiv- und Testsystem

Pseudonymisierung

- Passwortfelder
- Server-Log-Files