Technische und organisatorische Maßnahmen zur Wahrung des Datenschutzes

handwerk-digital.nrw

Organisatorische Maßnahmen

- Benennung betrieblicher oder externer Datenschutzbeauftragter
- Nachweisliche Schulung der Angestellten hinsichtlich Datenschutzrecht und IT-Sicherheit
- Nachweisliche Vertraulichkeitsverpflichtung der Angestellten
- Bestehendes Datenschutzkonzept, Informationssicherheitskonzept
- Auditierung oder Zertifizierung
- Verhaltensregeln

Vertraulichkeit

Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle

- Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums, Räume mit Datenverarbeitungsanlagen
- Alarmanlage
- Automatisches Zutrittskontrollsystem, Ausweisleser
- Türsicherung (elektrischer Türöffner, Zahlenschloss o. Ä.)
- Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe o. Ä.)
- Sicherheitsschlösser
- Chipkarten-/ Transponder-Schließsystem
- Biometrie
- Manuelles Schließsystem
- Schranken und Vereinzelungsanlagen, wie Drehkreuze o. Ä.
- Magnetschleusen
- Werkschutz und/ oder Pförtner
- Empfang mit Anmeldung
- Sorgfältige Auswahl von Wach- und Reinigungspersonal
- Lichtschranke und/ oder Bewegungsmelder
- Feuerfeste Türen
- Absicherung von Gebäudeschächten
- Fenstervergitterung
- Panzerglas
- Zugangs-Videoüberwachung
- Tragepflicht von Mitarbeiter- bzw. Gästeausweisen
- Gästeprotokollierung

Zugangs- und Benutzerkontrolle

- Passwortvergabe mit vorgegebenen starken Parametern
- Chipkarte mit PIN oder Passwort
- Authentifikation mit Benutzername und Passwort
- Biometrisches Merkmal mit PIN oder Passwort

Handwerkskammer Ostwestfalen-Lippe zu Bielefeld

Gefördert durch: Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

- Einsatz von VPN-Technologie
- Verschlüsselung von Smartphone-Inhalten
- Verschlüsselung von mobilen Datenträgern
- Einsatz von Mobile Device Management

Zugriffskontrolle

- Schriftliches Berechtigungskonzept
- Erstellen von Benutzer-Profilen und Zuordnung von Benutzer-Rechten
- Verwaltung durch Systemadministrator
- Anzahl der Administratoren auf das Nötigste reduzieren
- Gesicherte Nutzung von USB-Schnittstellen oder Sperrung von USB-Ports
- Automatisches Sperren des PC-Arbeitsplatzes
- Protokollierung von Zugriffen auf Anwendungen
- Einsatz von Akten- und Datenträgervernichtern bzw. externen Dienstleistern zur Vernichtung von Akten und Datenträgern
- Verschlüsselung von Datenträgern und Endgeräten
- Sichere Aufbewahrung von Datenträgern
- Löschkonzept für Daten
- Vernichtungsprotokolle

Transport- und Übertragungskontrolle

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- E-Mail-Verschlüsselung
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Protokollierungen von Übermittlungen
- Erstellen einer Übersicht von Datenträgern, Aus- und Eingang
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- Sicherung von Datenträgertransporten (verschließbarer Transportbehälter), auch für Papier

Auftragskontrolle

- Vorhandene Vereinbarungen zur Auftragsverarbeitung
- Kontrolle der Vertragsausführung
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Regelung zu Wartungen (speziell Fernwartung)
- Vorherige Prüfung der bei dem Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechende Dokumentation
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Handwerkskammer Ostwestfalen-Lippe zu Bielefeld
Gefördert durch: Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Integrität

handwerk-digital.nrw

Eingabe- bzw. Verarbeitungskontrolle

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Protokollauswertungsroutinen und -systeme
- Aufbewahrungs- bzw. Löschfristen für Protokolle

Dokumentationskontrolle

- Führung eines Verarbeitungsverzeichnisses
- Dokumentation der eingesetzten IT-Systeme und deren Systemkonfiguration
- Zulässigkeit eines Datentransfers in Drittländer ist gegeben

Verfügbarkeitskontrolle

- Unterbrechungsfreie Stromversorgung (USV)
- Überspannungsschutz
- Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmierung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Viren- und Malwareschutzsystem
- Spiegelung von Festplatten (z. B. RAID-Verfahren)
- Konzept für Katastrophenfall vorhanden

Trennungsgebot

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Versehen der Datensätze mit Zweckattributen bzw. Datenfeldern
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem
- Festlegung Technologie von Datenbankrechten
- Trennung von Daten verschiedener Auftraggeber

Handwerkskammer Ostwestfalen-Lippe zu Bielefeld

Gefördert durch: Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen