Technische und organisatorische Maßnahmen

Inhalt

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:

- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- 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 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 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.

Zutrittskontrolle

- Besucher nur in ständiger Begleitung
- Einbruchmeldeanlage
- Chipkarten-/Transponder-Schließsystem
- Dauerhaft Personal anwesend
- Empfang / Pforte / Rezeption
- Gesicherter Serverraum
- Klingelanlage
- Schlüsselregelung /-verwaltung /-organisation
- Videoüberwachung
- Zutrittsberechtigungskonzept (Intern)
- Zoneneinteilung der/im Gebäude

Zugangskontrolle / Zugriffskontrolle

- Aktenschredder
- Allg. Richtlinie Datenschutz / IT-Sicherheit
- Authentifikation mit Benutzer und Passwort und bei erhöhtem Schutzbedarf durch eine zusätzliche Multifaktor-Authentisierung
- Anti-Viren Software Clients
- Einsatz von VPN-Technologie
- Protokollierung von An- und Abmeldungen
- Richtlinie "Sicheres Passwort"
- Stets aktueller Virenschutz
- Stets aktuelle Softwareversionen
- Firewall (Software)
- Physische Löschung / Vernichtung von Datenträgern
- Minimale Anzahl an Administratoren

- Firewall (Hardware)
- Checkliste für Mitarbeiteraustritt
- Ordnungsgemäße Vernichtung von Datenträgern

Weitergabekontrolle

1. Dedizierte Weitergabeberechtigungen
2. Verschlüsselung von Datenträgern und Verbindungen
3. Festlegung und Dokumentation der Empfänger
4. Kontrolle des Versands von Datenträgern
5. Einsatz von VPN

Eingabekontrolle

i. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
ii. Protokollierung von Dateneingaben-, Änderungen und Löschungen

Auftragskontrolle

a. Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten
b. Schriftliche Festlegung der Weisungen

Verfügbarkeitskontrolle / Integrität

1. Sicherstellung einer funktionsfähigen Klimatisierung
2. Ständig kontrolliertes Backup- und Recoverykonzept
3. Unterbrechungsfreie Stromversorgung und Überspannungsschutz
4. Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten
5. Einsatz von Festplattenspiegelung

Gewährleistung des Zweckbindungs-/Trennungsgebotes

1. Trennung von Produktiv- und Testsystem
2. Logische Mandantentrennung (Software)