technische organisatorische Maßnahmen der Sellmore GmbH

Technische und organisatorische Maßnahmen der Sellmore GmbH

nach EU DS-GVO

Stand März 2021

1. Vertraulichkeit
(Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  - Alarmanlage
  - Sicherheitsschlösser
  - Manuelles Schließsystem
  - biometrische Zugangssperren
  - Schließsystem mit Codesperre
  - Videoüberwachung der Zugänge
  - Schlüsselregelung / Schlüsselbuch
  - Bewegungsmelder
  - Absicherung von Gebäudeschächten
  - Automatisches Zugangskontrollsystem
  - Chipkarten-/Transponder-Schließsystem
  - Cloud (RZ DPS-BS)
    - Hochsicherheitszugang
    - Alarmanlage mit Key und Pin
    - Viertürenschleusensystem
  - Sorgfältige Auswahl von Reinigungspersonal
  - Sorgfältige Auswahl von Sicherheitspersonal
  - Personenkontrolle beim Empfang
  - Protokollierung der Besucher / Besucherbuch
  - Tragepflicht von Gästeausweisen
  - Archiv
- Zugangskontrolle
  - Einsatz von Firewalls
  - Einsatz einer Hardware-Firewall
  - Einsatz einer Software-Firewall
  - Einsatz von Anti-Viren-Software
  - Einsatz von Intrusion-Detection-Systemen
  - Sperren von externen Schnittstellen (Netzwerkanschlüsse)
  - Gehäuseverriegelungen
  - Passwortvergabe / Passwortregeln
  - Einsatz von VPN-Technologie
  - WLAN
    - Zentraler und separater Internet Zugang
    - Mittels WLAN-Controler werden alle APs verwaltet.
    - Auf das Gäste-WLAN kann nur mittels Passwort und WPA2 zugegriffen werden.
    - Jeder Gast WLAN-Nutzer muss sich den internen Nutzungsbedingungen unterwerfen.
  - Erstellen von Benutzerprofilen
  - Authentifikation mit Benutzer + Passwort
  - Authentifikation mit biometrischen Daten
  - Einsatz von Anti-Viren-Software
  - Schlüsselregelung / Schlüsselbuch
  - Einsatz von Mobile Device Management
  - Verschlüsselung von mobilen Datenträgern
  - Verschlüsselung von Datenträgern in Laptops / Notebooks
  - Verschlüsselung von Datenträgern
    - IT-Grundschutzkatalogs „M 4.337 Einsatz von BitLocker Drive Encryption“:
  - RZ DPS-BS
    - biomethrische Kontrolle
    - Videoüberwachung
  - Verschlüsselung von Smartphones
  - Verschlüsselung von Smartphones durch Containerlösung für Firmendaten
  - Einsatz eines zentrale Smartphone-Managements mittels Containerlösung
  - Benutzerberechtigungen verwalten
  - Fernwartung
    - Bestandteil des Sicherheitskonzeptes
    - interner Zugangsserver
    - interne Nummernvergabe
    - interner Direktzugriff
    - Zugangsvarianten durch IT Verantwortliche
    - Berücksichtigung der Sicherheitsvorstellung des Kunden
  - Personenkontrolle beim Empfang
  - Tragepflicht von Berechtigungsausweisen
  - Sorgfältige Auswahl von Reinigungspersonal
  - Sorgfältige Auswahl von Sicherheitspersonal
  - Protokollierung der Besucher / Besucherbuch
  - Archiv
- Zugriffskontrolle
  - Einsatz von Aktenvernichtern (Fa .Reisswolf)
  - Verschlüsselung von Smartphones
  - Verschlüsselung von Datenträgern
  - Erstellen eines Berechtigungskonzepts
  - Sichere Aufbewahrung von Datenträgern
  - Passwortrichtlinie inkl. Länge
  - Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757, FA Reisswolf))
  - Verwaltung der Benutzerrechte durch Systemadministratoren
  - Anzahl der Administratoren auf das „Notwendigste“ reduzieren
  - Physische Löschung von Datenträgern vor deren Wiederverwendung
  - Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
  - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  - privacy_shield zwischen EU und US
  - Archiv
- Trennungsgebot
  - Festlegung von Datenbankrechten
  - Erstellung eines Berechtigungskonzepts
  - Trennung von Produktiv- und Testsystem
  - Logische Mandantentrennung (softwareseitig)
  - Versehen der Datensätze mit Zweckattributen/Datenfeldern
  - Verschlüsselung von Datensätzen, die versendet werden
  - Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
  - Archiv
- Pseudonymisierung
  (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  - Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der A ufbewahrung auf einem getrennten, abgesicherten IT-System
  - Die Pseudonymisierung erfolgt auf Tabellenebene in Datenbanken
  - Die Pseudonymisierung erfolgt nicht auf Dateibezeichnungsebene , um die Arbeiten der Mitarbeiter nicht zu erschweren
  - Durch Berechtigungs-Konzepte wird die Notwendigeit der Pseudonymisiserung zyklisch auf ihre Risiken geprüft
  - Eine zusätzliche Pseudonymisierung erfolgt nur bei Weitergabe von Daten. Diese weitergabe unterliegt strengen Sicherheits-Vorgaben unseres Hauses
  - Verwendung von (Personal-, Kunden-) Kennziffern statt Namen

2. Integrität
(Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  - E-Mail-Verschlüsselung mit Anlage
  - E-Mail-Verschlüsselung gesamt
  - Einrichtungen von VPN-Tunneln
  - Sichere Transportbehälter/-verpackungen
  - Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
  - Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
  - Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
  - Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
  - Archiv
- Eingabekontrolle
  - Protokollierung der Eingabe, Änderung und Löschung von Daten
  - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
  - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
  - Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
  - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
  - Archiv

3. Verfügbarkeit und Belastbarkeit
(Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeit
  - Erstellen eines Notfallplans
  - Klimaanlage in Serverräumen
  - Feuer- und Rauchmeldeanlagen
  - Feuerlöschgeräte
  - Testen von Datenwiederherstellung
  - Schutzsteckdosenleisten
  - Serverräume nicht unter sanitären Anlagen
  - Erstellen eines Backup- & Recoverykonzepts
  - Unterbrechungsfreie Stromversorgung (USV)
  - Alarmmeldung bei unberechtigten Zutritten
  - Rechenzentrum
  - In Hochwassergebieten: Serverräume über der Wassergrenze
  - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
  - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
  - Archiv
- Wiederherstellbarkeit
  (Art. 32 Abs. 1 lit. c DS-GVO)
  - Backup Konzept
    - wird durchgeführt
    - ist dokumentiert
  - Aufbewahrungs - und Löschfestlegungen
  - Redundante RZ
  - Zyklischer Wiederherstellungs Test

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Unternehmensrichtlinien (Code of Conduct)
- Sicherheitsrichtlinien
- Compliance-Management
- IT-Konzept
- Sensibilisierungskonzept
- Risiko-Management
- Notfall-Management
- Betroffenen-Management
- IT Störungs-Management
- Datenschutz-Management
- Datenschutz-Konzept
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle
  - Vertragsstrafen bei Verstößen
  - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
  - Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren
  - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
  - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
  - Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
  - Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungs-vertrag)
- Archiv

5. Datenschutz Management

- 1. Listen, Pläne, Übersichen
- 2. Interne Organisation
  - Protokolle
  - Sensibilisierung
  - TOMs
  - Risiko-Folge-Abschätzung
  - Tätigkeitsberichte des DSB
- 3. Prozesse und Verfahren
- 4. Verträge
- 5. Projekte, Anaylsen, Audits
- 6. Konzepte
- 7. Compliance
- 8. Archiv

Legende

- erfüllt
- in Bearbeitung
- Risiko
- nicht relevant