REISSWOLF Digital Services GmbH

Anlage 1i. Technisch-organisatorische Maßnahmen (TOM) nach Art. 32 Abs. 1 DSGVO

Übersicht der Maßnahmen:

1. Pseudonymisierung personenbezogener Daten

Maßnahmen, die sicherstellen, dass die Identifizierung der betroffenen Personen wesentlich erschwert wird.
Zum Beispiel: durch Trennung von Daten und Identifikationsmerkmalen.

- ☐ Trennung von Kundenstammdaten und Kundenumsatzdaten
- ☒ Verwendung von Personal-, Kunden-, Patienten-Kennziffern statt Namen
- ☐ Trennung von Patienten-Kontaktdaten und Behandlungsdaten/Befunden

2. Verschlüsselung personenbezogener Daten

Maßnahmen, die sicherstellen, dass personenbezogene Daten in stationären und mobilen Speicher- und Verarbeitungsmedien verschlüsselt werden.

- ☒ Verschlüsselung aller eingesetzten Laptops/Notebooks
- ☐ Verwendung von verschlüsselten USB-Sticks
- ☒ VPN-Tunnel (IPSec)
- ☐ Verschlüsselung von Smartphone-Inhalten

3. Gewährleistung der Vertraulichkeit der Systeme und Dienste

3.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☒ Alarmanlage
- ☐ Absicherung von Gebäudeschächten
- ☒ Automatisches Zugangskontrollsystem
- ☒ Chipkarten-/Transponder-Schließsystem
- ☐ Schließsystem mit Codesperre
- ☒ Manuelles Schließsystem
- ☐ Biometrische Zugangssperren
- ☒ Videoüberwachung der Zugänge
- ☒ Lichtschranken / Bewegungsmelder
- ☐ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☒ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☒ Tragepflicht von Berechtigungsausweisen

3.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☒ Zuordnung von Benutzerrechten
- ☒ Erstellen von Benutzerprofilen / Einzelfallentscheidungen
- ☒ Passwortvergabe
- ☐ Authentifikation mit biometrischen Verfahren
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Zuordnung von Benutzerprofilen / Einzelfallentscheidungen zu IT-Systemen
- ☐ Gehäuseverriegelungen
- ☒ Einsatz von VPN-Technologie mit 2-Faktor Authentifizierung
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☐ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☒ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☒ Tragepflicht von Berechtigungsausweisen
- ☒ Einsatz von Intrusion-Detection-Systemen
- ☒ Verschlüsselung von mobilen Datenträgern (teilweise)
- ☒ Einsatz von Anti-Viren-Software
- ☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☒ Einsatz einer Hardware-Firewall
- ☐ Einsatz einer Software-Firewall
- ☒ Verschlüsselung von Datenträgern in Laptops / Notebooks

3.3. Zugriffskontrolle

Maßnahmen die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ physische Löschung von Datenträgern vor Wiederverwendung
- ☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒ Protokollierung der Vernichtung

☒ Verschlüsselung von Datenträgern

3.4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ E-Mail-Verschlüsselung
- ☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –Fahrzeugen
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☒ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen

3.5. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Erstellung eines Berechtigungskonzepts
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☒ Festlegung von Datenbankrechten
- ☒ Logische Mandantentrennung (softwareseitig)
- ☒ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☒ Trennung von Produktiv- und Testsystem

4. Gewährleistung der Integrität der Systeme und Dienste

4.1. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☒ 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
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Einsatz einer revisionssicherer Dokumentenmanagement Software (ELO)

5. Gewährleistung der Verfügbarkeit der Systeme und Dienste

5.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Klimaanlage in Serverräumen
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Testen von Datenwiederherstellung
- ☒ Erstellen eines Notfallplans
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Serverräume nicht unter sanitären Anlagen
- ☒ In Hochwassergebieten: Serverräume über der Wassergrenze

5.2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.
REISSWOLF ist Auftragsverarbeiter. Sollte REISSWOLF als Verantwortlicher tätig werden, werden bei der Auftragsvergabe nachstehende Kontrollpunkte umgesetzt.

- ☒ Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DS-GVO
- ☒ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- ☐ Vertragsstrafen bei Verstößen
- ☒ vorherige Prüfung und ggf. Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- ☒ Verpflichtung auf Vertraulichkeit der Mitarbeiter des Auftragsverarbeiters nach Art. 28 DS-GVO
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

6. Gewährleistung der Belastbarkeit der Systeme und Dienste

Maßnahmen, die sicherstellen, dass die Systeme und Dienste so ausgelegt sind, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben. Die Maßnahmen beziehen sich auf Speicher-, Zugriffs- und Leitungskapazitäten

- ☒ Die eingesetzten Storage-Systeme weisen den Stand der Technik (bzgl. Toleranz und Resilienz gegenüber Fehlern und Störungen) auf.
- ☒ Es sind Strategien zur Disaster Recovery und Business Continuity vorhanden
- ☒ Backup Hard- und Software sind nach Stand der Technik ausgewählt/eingesetzt

7. Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall

Maßnahmen, die sicherstellen, dass der Zugang zu und die Verfügbarkeit von personenbezogenen Daten nach Zwischenfällen so rasch wie möglich erfolgt

- ☒ Notfallplan
- ☐ BCM (Kontinuitätsmanagement) -Konzept
- ☐ Redundante Datenspeicherung
- ☒ Cloud Services
- ☒ Externe RZ, gespiegelte RZ
- ☐ Redundante IT-Infrastruktur

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM's

Maßnahmen, die sicherstellen, dass eine systematische und regelmäßige Überprüfung sowie eine sach- und fachgerechte Bewertung und Behandlung der Wirksamkeit technischer und organisatorischer Maßnahmen erfolgt

- ☒ Datenschutzmanagementsystem etabliert
- ☒ Interne Audits
- ☐ Audits durch DSB
- ☒ Zertifizierung nach ISO 27001 (für den Bereich IT)
- ☒ Regelmäßige Tests inkl. Dokumentation (für den Bereich IT)
- ☐ Zertifizierung nach DIN 66399
- ☒ Dokumentierte Risikoanalyse (für den Bereich IT)