Ro-ot Service AG
UID: CHE-104.695.341
Wydenstrasse 29 | 8575 Bürglen
T +41 (0)71 634 80 40 | info@root.ch
web.root.ch

Stichtagsliste

Technische und organisatorische Massnahmen (TOM)

I Vertraulichkeit

A. Zutrittskontrolle

Folgende Massnahmen werden getroffen um einen unbefugten Zutritt zu Datenverarbeitungsanlagen (DV-Anlagen) und physischen Datenablagen zu verhindern.

- ☑ DV-Anlagen befinden sich in Sicherheitsbereichen mit eingeschränktem Zugang
- ☑ Es ist gewährleistet, dass keine betriebsfremden Personen Zutritt zu den DV-Anlagen haben
- ☑ Zutrittskontrollsysteme (ID-Lesegeräte, Magnetkarten, Chipkarten) sind vorhanden
- ☑ Schlüsselverwaltung
- ☑ Personenkontrolle durch Empfang/Portier
- ☑ Alarmanlage
- ☑ Gebäudeüberwachung
- ☑ Überwachungseinrichtungen, (Video/CCTV-Monitor, Alarmanlage, etc.);
- ☑ Für diese Bereiche werden Anwesenheits- und oder Berechtigungsnachweise geführt
- ☑ Der Zutritt durch Personen, die nicht allgemein zum Zutritt zu den Systemen befugt sind (d.h. unbefugte Mitarbeiter und externe Personen wie z.B. Wartungstechniker, Reinigungskräfte, Besucher) ist geregelt (Verträge, Stillschweigevereinbarungen, etc.)

B. Zugangskontrolle

Folgende Massnahmen werden getroffen um einen unbefugten Zugang zu Datenverarbeitungsanlagen (DV-Anlagen) und physischen Datenablagen zu verhindern.

- ☑ Benutzerautorisierung und -authentifizierung
- ☑ Sicherheitsmassnahmen hinsichtlich Nutzer-IDs/Passwörtern (z.B. Sonderzeichen, Mindestlänge, Pflicht zur Änderung von Passwörtern oder MFA)
- ☑ automatische Sperrung (z.B. Bildschirmsperre bei Auszeiten und Aufforderung zur Eingabe des Passworts)
- ☑ Wichtige Systemaktivitäten werden protokolliert.
- ☑ Überwachung von Einbruchsversuchen und automatische Sperre bei mehrfach eingegebenen falschen Passwörtern
- ☑ Verschlüsselung archivierter Datenmedien

C. Zugriffskontrolle

Folgende Massnahmen sollen gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☑ Zugriffsrechte (Profile, Rollen) basierend auf einem Rechte- und Rollenkonzept
- ☑ Überwachung und Aufzeichnung von Zugriffen, Zugriffsberichte
- ☑ Verschlüsselter Zugriff (z. B. https, SSL, etc.)
- ☑ Verfahren zur Sicherstellung für die Vernichtung von gebrauchten Medien sind eingerichtet
- ☑ Fernwartungen der IT-Systeme sind gesichert (Verschlüsselung, Einmalpasswörter, etc.)
- ☑ interne Richtlinien und Verfahren

II Trennungskontrolle

Folgende Massnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden

Stand 05.09.2023 | Version [01]

Ro-ot Service AG
UID: CHE-104.695.341
Wydenstrasse 29 | 8575 Bürglen
T +41 (0)71 634 80 40 | info@root.ch
web.root.ch

Stichtagsliste

Technische und organisatorische Massnahmen (TOM)

können.

- ☑ Trennung von Datenbanken verschiedener Organisationen
- ☑ Die für die Verarbeitung genutzten IT-Systeme sind mandantenfähig und werden entsprechend betrieben. Ist dies nicht möglich, so werden dedizierte Systeme genutzt.
- ☑ Trennung von Funktionen (Produktion/Test)

D. Pseudonymisierung
Folgende Massnahmen gewährleisten, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

III Integrität

E. Weitergabekontrolle
Folgende Massnahmen gewährleisten, dass personenbezogene Daten, die elektronisch oder auf Datenträgern (manuell oder elektronisch) gespeichert sind, bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen die personenbezogenen Daten weitergegeben wurden.

- ☑ Verschlüsselte Medien (USB-Sticks, externe Festplatten, etc.)
- ☑ Verschlüsselte Übertragungswege (SSL, HTTPS, SCP, SFTP, etc.)
- ☑ Virenschutz
- ☑ Firewalls
- ☑ Netzwerke und Netzwerkzugriffspunkte werden dokumentiert.
- ☑ VPN (Virtual Private Networks) oder Tunnel
- ☑ Inhaltsfilter / Proxy
- ☑ IPS / IDS (Systems zur Erkennung/ Verhinderung von Einbrüchen)
- ☑ Aktive Netzwerkkomponenten (z.B. Switches oder Router) sind so konfiguriert, dass wichtige Ereignisse und die Netzwerklast aufgezeichnet werden, um Angriffe, ungewöhnliche Ereignisse oder Vorfälle zu entdecken bzw. derartige Ereignisse zumindest zu analysieren.
- ☑ Soweit technisch möglich, zeichnen Betriebssysteme, Anwendungen und Dienste den Austausch von Daten auf.

IV Eingabekontrolle

Folgende Massnahmen überwachen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt (gelöscht) worden sind.

- ☑ Protokollierungs- und Berichtssysteme
- ☑ Jeder Nutzer hat ein personalisiertes Konto. Bietet eine Anwendung oder ein System keine Möglichkeit für die Verwendung von personalisierten Konten, so ist gewährleistet, dass nur diejenigen Personen, die ein Konto zur Erfüllung ihrer Pflichten zwingend nutzen müssen, Zugriff auf dieses Konto haben.
- ☑ Die Verwaltung von Nutzerkonten und Zugriffsberechtigungen ist organisiert und dokumentiert.

F. Auftragskontrolle
Folgende Massnahmen gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Datenverantwortlichen verarbeitet werden.

- ☑ Definierte Prozesse für die Beauftragung von Vertragspartnern
- ☑ Organisiertes Vertragswesen

Stand 05.09.2023 | Version [01]

Ro-ot Service AG
UID: CHE-104.695.341
Wydenstrasse 29 | 8575 Bürglen
T +41 (0)71 634 80 40 | info@root.ch
web.root.ch

Stichtagsliste

Technische und organisatorische Massnahmen (TOM)

- ☑ Kriterien zur Auswahl des Subunternehmers sind definiert
- ☑ Subunternehmer, die mit der Verarbeitung personenbezogener Daten beauftragt werden, sind vertraglich verpflichtet, die personenbezogenen Daten mindestens in dem Umfang zu schützen, wie es in diesem Vertrag vereinbart ist.

V Verfügbarkeit und Belastbarkeit

G. Verfügbarkeitskontrolle

Folgende Massnahmen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust (physisch und logisch) geschützt werden.

- ☑ Es werden regelmässige Datensicherungen durchgeführt (täglich inkrementell sowie monatlich vollständig), deren Richtigkeit und Vollständigkeit regelmässig überprüft wird.
- ☑ Speicherung von Datensicherungen an einem sicheren ausgelagerten Ort
- ☑ Spiegelung von Festplatten (z.B. RAID-Technik)
- ☑ Es besteht ein Notfall-/ Notfallwiederherstellungsplan, der den Schutz von Datenverarbeitungssystemen sowie die Speicherung personenbezogener Daten umfasst.
- ☑ Bei einem unbefugten Zutritt zu den Serverräumen wird ein Alarm ausgelöst.
- ☑ Unterbrechungsfreie Stromversorgung für Speichersysteme und Server
- ☑ Geräte zur Überwachung der Temperatur und Luftfeuchtigkeit in Serverräumen
- ☑ Klimatisierte Serverräume
- ☑ Rauch- und Brandmelder, Feuerlöschgeräte in Serverräume
- ☑ Serverräume befinden sich nicht unterhalb von Sanitärräumen

VI Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

H. Datenschutz-Management

Folgende Massnahmen gewährleisten ein effektives Datenschutzmanagement.

- ☑ Incident-Response-Management;
- ☑ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- ☑ Auftragskontrolle zwischen Auftraggeber und Auftragnehmer
- ☑ Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Stand 05.09.2023 | Version [01]