tickaroo

TECHNISCH-ORGANISATORISCHE MASSNAHMEN

1) Zutrittskontrolle

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt.

- Zutrittsregelung für betriebsfremde Personen
- Protokollierung von Besuchern und externen Dienstleistern
- Zentraler Empfangsbereich vorhanden
- Aufenthalt betriebsfremder Personen nur in Anwesenheit von Mitarbeitern
- Gebäudeüberwachung durch Video *
- Maßnahmen zur Objektsicherung bei Fenstern *
- Automatische Türsicherungen *
- Manuelles Schließsystem
- Festgelegte Serverraum-Zutrittsberechtigungen einschl. Schlüsselregelung und Zutrittsprotokollierung *

2) Zugangskontrolle

Es wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Authentifikation mit individuellem Benutzernamen und Passwort
- Regelung zur Passwortvergabe (Art, Dauer, Sperrung)
- Zuordnen von Benutzerprofilen zu IT-Systemen
- Automatische, passwortgeschützte Rechnersperre
- Regelung für die Löschung von Berechtigungen ausgeschiedener Mitarbeiter
- Verbindliches Verfahren zur Vergabe von Berechtigungen
- Einsatz von Anti-Viren-Software
- Sicherung interner Netze gegen unberechtigte Zugriffe von extern (Firewall)
- Externer Zugriff auf interne Netze durch VPN-Technologie

3) Zugriffskontrolle

Es wird gewährleistet, 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.

- Erstellung von Benutzerprofilen
- Erstellen eines Berechtigungskonzepts mit differenzierten Berechtigungsstufen
- Dokumentation der Berechtigungen
- Regelung zum Kopieren von Daten
- Protokollierung und datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger
- Personen mit Administratorenrolle erhalten lediglich diejenigen Berechtigungen, die für ihre Tätigkeit notwendig sind.
- Berechtigungen werden regelmäßig und anlassbezogen geprüft und angepasst.

4) Weitergabekontrolle

Es wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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.

- Zugriff auf personenbezogene Daten nur über authentifizierte Kanäle
- Dokumentation von Datenempfängern bei Transport oder Übermittlung
- Dokumentation der Abruf- und Übermittlungsprogramme
- Führen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Automatische Sperre bei mehrmaliger fehlerhafter Authentifizierung
- Bei physischem Transport sichere Transportbehälter/-verpackungen
- Datenschutzgerechte Vernichtung von Datenträgern

5) Eingabekontrolle

Es wird gewährleistet, 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
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Übersicht, mit welchen Applikationen Daten eingegeben, geändert oder gelöscht werden können
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen werden
- Löschungsregelung für Protokolldaten

6) Auftragskontrolle

Es wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Kontrolle der Datensicherheitsvorkehrungen und schriftlicher Nachweis
- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf Vertraulichkeit der Daten gem. Art. 5 Abs. 1 DSGVO
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7) Verfügbarkeitskontrolle

Es wird gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Notfallkonzept bei IT-Störungen vorhanden
- Redundante Absicherung von Servern und Datenbeständen
- Unterbrechungsfreie Stromversorgung (USV) in Serverräumen *
- (Redundante) Klimaanlage in Serverräumen *
- Automatische Feuer- und Rauchmeldeanlagen *
- Feuerlöscheinrichtungen im Serverraum *
- Alarmmeldungen bei unberechtigten Zutritten zu Serverräumen *
- Sicherungs- und Wiederherstellungskonzept von Daten *
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort *
- Rekonstruktion von Datenbeständen und Test der Datenbestände *
- Richtlinien zur Wartung und Durchführung von Updates
- Automatisches und permanentes Monitoring zur Erkennung von Störungen

8) Trennungskontrolle

Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Logische Mandantentrennung
- Berechtigungskonzept mit Festlegung der Zugriffsrechte
- Trennung von Produktiv- und Testsystem

9) Infrastruktur

Es wird gewährleistet, dass die Infrastruktur stets in einem definierten Zustand und vor unberechtigtem Zugriff geschützt ist. Ausfällen wird nach Möglichkeit (Stand der Technik) proaktiv vorgebeugt.

- Infrastruktur wird über Infrastructure as Code (IaC) definiert. Diese Definitionen unterliegen Reviews und Tests. Abweichungen von der Definition werden automatisch korrigiert.
- Zugriff auf Infrastrukturkonsolen des Hosters erfolgt per Zwei-Faktor-Authentifizierung (2FA).
- Kritische Tätigkeiten (wie initiales Anlegen einer Infrastruktur, grundlegende Änderungen einer Infrastruktur, etc.) erfolgen durch einen Senior Software Engineer nach Möglichkeit im Beisein des CTO oder seines Vertreters.
- Kritische Leistungsparameter der Infrastruktur werden automatisiert überwacht. Eine Benachrichtigung der Administratoren erfolgt selbsttätig. Diese entscheiden im Einzelfall über das angemessene weitere Vorgehen.
- Konfigurationen von Testsystemen erfolgen stets identisch mit Live-Systemen.

10) **Datenschutzfreundliche Voreinstellungen**

Es bestehen Maßnahmen nach Stand der Technik für datenschutzfreundliche Voreinstellungen.

- Es werden nur tatsächlich benötigte Daten erhoben.
- Die Datenverarbeitung ist soweit eingeschränkt, dass nur die minimal erforderlichen Funktionen für die Verarbeitung personenbezogener Daten verwendet werden können.
- Verarbeitung kann durch Voreinstellung ausschließlich dem Verarbeitungszweck entsprechend erfolgen.
- Zur Datenminimierung werden Daten – wo anwendbar – so früh wie möglich pseudonymisiert.
- Es besteht Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten.

* im Rechenzentrum bei AWS

Es bestehen interne Prüfungsverfahren auf Einhaltung der festgelegten Prozesse, interner Vorgaben und der TOMs, sowie auf deren Wirksamkeit.

Datenschutzbeauftragter der Tickaroo GmbH

Matthias Baumgartner
Projekt 29 GmbH & Co. KG
Ostengasse 14
93047 Regensburg