Köln, den 18.01.2022

Auskunft über technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

Inhaltsverzeichnis

I. Vertraulichkeit (Art. 32 Abs. 1lit. b DSGVO)

Zutrittskontrolle

Nachfolgende Themen wurden aus Gründen der Sicherheit (von außen nach innen) betrachtet:

Ausreichende Absicherung der Zugänge:

Bewachung:

Schriftliche Dokumentation, Anweisung:

Überwachungseinrichtungen zur Sicherstellung der Zutrittskontrolle für kritische Sicherheitsbereiche, wie z.B. für Serverräume:

Kriterien für die Zugangsberechtigung:

Sicherheitsbetrachung der Arbeitsplätze:

Dokumentation der Zutritte:

Zugangskontrolle

Benutzeridentifikation und Passwortverfahren:

Automatische Sperrung der Bildschirme:

Einrichtung eines Benutzerstammsatzes pro User:

Verbot der Passwortweitergabe:

Verschlüsselung von Datenträgern:

Zugriffskontrolle

Schutz gegen unberechtigte interne und externe Zugriffe, Firewall:

Verschlüsselung zum Schutz gegen unberechtigte interne und externe Zugriffe:

Berechtigungskonzept für Zugriffsrechte:

Regelungen zur Überwachung und Protokollierung: ; - Aufbewahrung der Protokolle zwischen 30 Tagen u. 12 Monaten, abhaengig vom System

Schriftliche Dokumentation von Datenträgern:

Datenträgerverwaltung:

Regelung zum Umgang mit Datenträgern:

Regelung zur Datenträgernutzung:

Der Umgang mit Datenträgern ist geregelt:

Pseudonymisierung

Pseudonymisierung personenbezogener Daten: „Pseudonymisierung“ wird in Art. 4 Nr. 5 DS-GVO definiert als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer

spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“

Trennungsgebot

Umsetzung des Trennungsgebots:

Regelung der Trennung:

Mandatentrennung auf den Systemen:

Sicherstellung der Datenschutzkonformität:

II. Integrität (Art. 32 Abs. 1lit. b DSGVO)

Weitergabekontrolle

Übermittlung: - per Datenleitung

Datenschutzkonformität durch: - sichere Versendungsform, VPN (Virtual Private Network)

Eingabekontrolle

Datenschutzkonforme Eingabekontrolle:

III. Verfügbarkeit und Belastbarkeit - von Systemen und Diensten (Art. 32 Abs. 1lit. b DSGVO)

Verfügbarkeit und Belastbarkeit

Überwachung kritischer Bereiche und aller ausfallkritischen Infrastruktursysteme:

Konzept zum regelmäßigen Backup:

Die Belastbarkeit der Systeme und Dienste wird regelmäßig überpfüft bzw. getestet:

(als belastbar werden IT-Systeme bezeichnet, sofern diese ausreichend widerstandsfähig sind, um auch trotz Störungen und Fehlern bei hoher Belastung (zB. bei DDoS–Attacken) funktionsfähig zu bleiben und, mit Blick auf die Verarbeitung personenbezogener Daten, Sicherheit garantiert werden kann. In diesem Sinne meint ‚Belastbarkeit’ Robustheit)

Konzept für regelmäßigen Sicherheits-Updates: Updates werden, abhängig vom System, wöchentlich, monatlich oder wenn erforderlich, installiert.

IV. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Rasche Wiederherstellbarkeit

Checkliste zur Prüfung des Notfallkonzepts

V. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Überprüfung der technischen und organisatorischen Maßnahmen

Rechenschaftspflicht (Art. 5 Abs. 2 EU-DSGVO)

Aufbauorganisation:

Datenschutzleitlinie im Unternehmen

Datenschutzbeauftragter ist bestellt und der Aufsichtsbehörde gemeldet

Aufgaben des Datenschutzbeauftragten sind definiert

Einheitliches Datenschutzkonzept für alle Standorte

Konzept für Aufgaben / Schulung zum Datenschutz

Regelungen für Interne Kontrollen

Regelungen für den Umgang mit Datenschutzberichten

Regelungen für die Zusammenarbeit der Abteilungen mit DSB

Basis-Anforderungen

Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)

Einheitliches Risikomodell

Datenschutzkonforme Verarbeitung

Umgang mit Betroffenenrechten

Umgang mit Datenschutzverletzungen

Einsatz von Subunternehmern

Ist ein Auftragnehmer als Auftragsverarbeiter nach Art. 28 DS-GVO tätig, verarbeitet der Auftragnehmer personenbezogene Daten nur entsprechend den vertraglichen Vorgaben des Auftraggebers.

Bei zusätzlichen Aufträgen z.B. „Remote Hands“, die die Verarbeitung oder den physischen Zugriff auf Datenträger von personenbezogenen Daten beinhalten oder nicht ausschließen können, werden ggfs. gesonderte Verträge gemäß DS-GVO Art. 28 abgeschlossen oder bestehende Verträge ergänzt.

Mit Subunternehmern werden, sofern erforderlich, datenschutzkonforme Verträge nach DS-GVO Art. 28 geschlossen. Die Auswahl von Dienstleistern erfolgt sorgfältig.

Mit freundlichen Grüßen

gridscle GmbH