serverloft

DOKUMENTATION TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

In Bezug auf Artikel 32 DSGVO

V 1.0

serverloft

Host Europe GmbH

Hansestr. 111

51149 Köln

Der Schutz der Daten unserer Kunden hat für uns Priorität. Unter Berücksichtigung der Best Practices, der Kosten der Umsetzung, und der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen unternehmen wir folgende technische und organisatorische Maßnahmen. Bei Auswahl dieser Maßnahmen werden Vertraulichkeit, Vollständigkeit, Verfügbarkeit und Belastbarkeit der Systeme in Betracht gezogen. Eine schnelle Wiederherstellung nach einem physischen oder technischen Zwischenfall ist garantiert.

Datenschutzprogramm

Unser Datenschutzprogramm ist darauf ausgerichtet, eine globale Data-Governance-Struktur aufrechtzuerhalten und Informationen über den gesamten Lebenszyklus hinweg zu schützen.Dieses Programm wird vom Datenschutzbeauftragten geleitet, der für die Umsetzung der Praktiken des Datenschutzes und der Sicherheitsmaßnahmen verantwortlich ist. Wir prüfen und bewerten regelmäßig die Wirksamkeit des Datenschutzprogramms und der Sicherheitsstandards.**1. Vertraulichkeit.** *"Vertraulichkeit bezieht sich auf den Schutz personenbezogener Daten vor unberechtigter Offenlegung."*

Wir nutzen eine Reihe physischer und digitaler Maßnahmen, um die Vertraulichkeit der personenbezogenen Daten unserer Kunden zu schützen. Zu diesen Maßnahmen gehören:

<u>Physische Sicherheit</u>

- Systeme für die Kontrolle des Zugangs sind vorhanden (Badge-Zugangskontrolle, Überwachung von Zwischenfällen bei der Sicherheit usw.)
- Überwachungssysteme mit Alarm und CCTV-Monitoring (wenn angemessen)
- Clean-Desk-Richtlinien und Kontrollen sind vorhanden (Verschluss unbeaufsichtigter Computer, von Schränken usw.)
- Verwaltung des Zugriffes für Besucher
- Vernichten von Daten auf physischen Speichermedien und Dokumenten (schreddern, entmagnetisieren usw.)

<u>Zugangskontrolle und Vorbeugung vor unberechtigtem Zugriff</u>

- Beschränkung des Zugriffs für Nutzer und Zugriffsberechtigungen auf Basis von Rollen werden auf Grundlage des Prinzips der Aufgabentrennung vergeben/ geprüft
- Wirksame Methoden der Authentifizierung und Autorisierung (mehrstufige Authentifizierung, Autorisierung über Zertifikate, automatische Deaktivierung oder Abmeldung usw.)
- Zentrale Verwaltung von Passwörtern und Richtlinien für starke/komplexe Passwörter (minimale Länge, Komplexität der Zeichen, Ablauf von Passwörtern usw.)
- Kontrolle des Zugriffs auf E-Mails und Internet
- Antiviren-Management
- Schutz vor Eindringlingen

<u>Verschlüsselung</u>

- Verschlüsselung interner und externer Kommunikationen mittels starker kryptographischer Protokolle
- Verschlüsselung gespeicherter PII/SPII Daten (Datenbanken, geteilte Verzeichnisse usw.)
- Vollständige Verschlüsselung der Datenträger von Firmen-PCs und -Laptops
- Verschlüsselung von Speichermedien
- Remote-Verbindungen mit den Netzwerken des Unternehmens sind per VPN verschlüsselt
- Schutz von Chiffrierschlüsseln in der gesamten Laufzeit

Daten-Minimierung

- PII/SPI-Minimierung bei Anwendung, Debugging und Sicherheitsprotokollen
- Anonymisierung personenbezogener Daten zur Verhinderung direkter Identifizierung natürlicher Personen
- Trennung gespeicherter Daten nach Funktion (Test, Staging, Live)
- Logische Abtrennung von Daten durch Zugriffsrechte auf Basis von Rollen
- Festgelegte Zeiträume für die Aufbewahrung personenbezogener Daten

Sicherheitstests

- Eindring-Tests für wesentliche Plattformen und Netzwerke des Unternehmens, die personenbezogene Daten hosten
- Regelmäßige Scans des Netzwerkes und auf Anfälligkeit

2. Integrität. *"Integrität bezieht sich auf die Gewährleistung der Richtigkeit (Intaktheit) von Daten und der korrekten Funktion von Systemen. Wird der Begriff „Integrität" in Verbindung mit dem Begriff „Daten" genutzt, bringt er zum Ausdruck, dass die Daten vollständig und unverändert sind."*

Angemessene Kontrollen von Änderungen und Protokollverwaltung sind vorhanden, neben Zugriffskontrollen, um die Integrität personenbezogener Daten zu erhalten, wie:

Verwaltung von Änderungen und Freigaben

- Verwaltungsverfahren für Änderungen und Freigaben (Analyse von Auswirkungen, Genehmigungen, Tests, Sicherheitsprüfungen, Staging, Monitoring usw.)
- Rollen-/Funktionsbasierter (Aufgabentrennung) Zugang in der Produktion

Protokolle und Monitoring

- Protokolle des Zugriffs auf und der Änderung von Daten
- Zentrale Audit- und Sicherheitsprotokolle
- Überwachung der Vollständigkeit und Richtigkeit der Datenübertragung (vollständige Prüfung)

3. Verfügbarkeit. *"Die Verfügbarkeit von Diensten und IT-Systemen, IT-Anwendungen und IT-Netzwerkfunktionen sowie von Daten ist garantiert, wenn die Nutzer jederzeit in der Lage sind, sie wie vorgesehen zu nutzen."*

Wir implementieren angemessene Maßnahmen gegen Unterbrechungen und für den Schutz, um die Verfügbarkeit der Dienste und der Daten in diesen Diensten zu gewährleisten:

- Regelmäßige Failover-Tests (Ausfallsicherung) für entscheidende Dienste
- Umfassende Überwachung und Berichte der Leistung und Verfügbarkeit entscheidender Systeme
- Programm für die Reaktion auf Zwischenfälle
- Entscheidende Daten werden entweder dupliziert oder erhalten ein Backup (Cloud-Backups/Festplatten/Datenbank-Duplizierung.)
- Planmäßige Wartung von Software, Infrastruktur und Sicherheit ist vorhanden (Software-Aktualisierungen, Sicherheits-Patches usw.)
- Redundante und widerstandsfähige Systeme (Servercluster, gespiegelte DBs, Setups mit hoher Verfügbarkeit etc.) an Außenstandorten oder separaten Standorten
- Nutzung von unterbrechungsfreier Stromversorgung, ausfallsicherer Hardware und Netzwerksystemen
- Vorhandene Alarmsystem
- Physische Schutzmaßnahmen für entscheidende Standorte (Schutz vor Überspannung, erhöhte Böden, Kühlsysteme, Sensoren für Feuer und Rauch, Löschsysteme usw.)
- DDOS-Schutz zur Aufrechterhaltung der Verfügbarkeit
- Belastungstests (Lade- und Stress-Tests)

4. Anweisungen zur Datenverarbeitung. *'Anweisungen zur Datenverarbeitung' bezieht sich auf die Gewährleistung, dass personenbezogene Daten ausschließlich gemäß der Anweisungen des Datenverantwortlichen und einschlägigen Maßnahmen des Unternehmens verarbeitet werden.*

Wir haben interne Datenschutzrichtlinien und Verträge für den Datenschutz eingeführt und schulen unsere Mitarbeiter regelmäßig bezüglich des Datenschutzes, um sicherzustellen, dass personenbezogene Daten in Übereinstimmung mit den Einstellungen und Einwilligungen der Kunden verarbeitet werden.

- Klauseln bezüglich Datenschutz und Vertraulichkeit in Arbeitsverträgen
- Regelmäßige Schulungen der Mitarbeiter über Datenschutz und Sicherheit
- Angemessene vertragliche Regelungen zu den Vereinbarungen mit Auftragnehmern zur Aufrechterhaltung der Anweisungsrechte
- Regelmäßige Prüfungen des Datenschutzes unserer externen Dienstleister
- Kunden haben die vollständige Kontrolle über ihre Datenverarbeitung
- Regelmäßige Sicherheitsüberprüfungen