cluster.at

EDV-Dienstleistungen
Ing. Christian Kaiserseder
Währingerstraße 88/7
1180 Wien

Anlage ./1 zum Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

1. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b DSGVO

1.1. Zutrittskontrolle

Der Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen ist gewährleistet durch:

- Portier, Sicherheitspersonal und Sicherheitsschleuse mit mehrstufigem Zugangskontrollsystem
- Videoüberwachung des Eingangsbereichs und aller Korridore
- Manuelle Schließsysteme (Versperrte Server-Schränke)
- Dritte werden nur auftrags-/projektbezogen in Begleitung von Mitarbeitern tätig
- Protokollierung der Besucher

1.2. Zugangskontrolle

Maßnahmen, um die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern:

- Ausschließlich kabelbasierte Netzwerke (kein WLAN)
- Betrieb und Updates von Firewalls
- Zugang zu Datenverarbeitungssystemen mit persönlicher Benutzerkennung und privatem Schlüssel oder sicherem Passwort
- Branchenübliche Kennwort Richtlinien
- Protokollierung der Logins und fehlgeschlagener Logins

1.3. Zugriffskontrolle

Maßnahmen, um sicherzustellen, dass jeder für die Datenverarbeitungssysteme berechtigte Benutzer ausschließlich auf die ihm berechtigten Daten zugreifen kann und personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Verwendung von Standard Berechtigungsprofilen
- Eigene Zugänge für Applikationen, Datenbanken und Webcontent

1.4. Trennung

Maßnahmen, um sicherzustellen, dass Daten, welche zu unterschiedlichen Zwecken erhoben wurden, getrennt gespeichert werden:

- Logische Kundentrennung (Serverkonfiguration, chroot-Technologie)
- Trennung durch eigene System- und FTP-Benutzer
- Separation der Daten unterschiedlicher Kunden in getrennten Verzeichnissen (Shared Webhosting- und Shared E-Mail-Hosting-Dienstleistungen) und auf eigenen Partitionen

2. Integrität gemäß Art. 32 Abs. 1 lit. b DSGVO

2.1. Weitergabekontrolle

Maßnahmen, um sicherzustellen, dass personenbezogene Daten bei elektronischer Übertragung oder Speicherung sowie beim Transport der Datenträger nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Abhängig vom Projekt):

- Zugang über SSH, SCP und sFTP
- Nutzung von Verbindungsverschlüsselung bei Systemüberträgen
- Verbindungssicherheit zwischen Webbrowser und Webserver mittel SSL-Verschlüsselung (https://)
- Verbindungssicherheit bei Mailservern mittels SSL/STARTLS für IMAPs, POP3s und sec. SMTP

2.2. Eingabekontrolle

Maßnahmen um sicherzustellen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, bearbeitet und entfernt worden sind:

- Protokollierung von Verbindungsdaten/Zugriffen bei Shared Webhosting- und Shared E-Mail-Server-Dienstleistungen
- Regelungen zum Zugriff auf Protokolle und zur Löschung von Protokollen

2.3. Systemsicherheit

- Betrieb von Virenscannern und weiterer Software zur Schadsoftware-Erkennung
- Nutzung von Firewalls und Intrusion Detection Systemen
- Regelmäßige Sicherheitsupdates von Web- und Systemsoftware

2.4. Softwaresicherheit

- Bei Shared Webhosting Dienstleistungen und Managed-Servern übernimmt der Auftragnehmer die laufende Wartung des Betriebssystems und der damit verbundenen Basis-Software (z.B. Systembibliotheken).
- Bei Shared Webhosting-Dienstleistungen werden Skriptsprachen und Datenbanktechnologien in aktuellen (vom Hersteller gepflegten) Fassungen zur Verfügung gestellt. Die Auswahl aktueller Skriptsprachen und Datenbanktechnologien und die Verwendung aktueller Versionen der Anwendungssoftware (CMS, Onlineshop-, Blog-Systeme, etc.) und deren regelmäßige Wartung obliegen dem Verantwortlichen/Webmaster.

3. Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

3.1. Verfügbarkeit

Maßnahmen, um sicherzustellen, dass personenbezogene Daten vor zufälliger oder mutwilliger Zerstörung und Verlust geschützt sind:

- Serverbetrieb im Interxion Rechenzentrum Louis-Häfligergasse, 1210 Wien, Schutzmaßnahmen im Datencenter:
  - redundante Stromversorgung (USV, Dieselaggregate)
  - Überspannungsschutz
  - Klimaanlage und Luftentfeuchtung
  - Brandschutz und Halonlöschanlage
  - Redundante Netzwerkanbindung
  - Ausfallssicherheit durch Hardware-RAID (redundante Festplattensysteme)
  - Ersatzteile für Serverkomponenten lagernd

3.2. Belastbarkeit

- Vorhalten von Ersatz-Hardware um bei Hardwareschäden einen Notfallbetrieb zu gewährleisten

3.3. Wiederherstellbarkeit

- Regelmäßige Backups von Webcontent, Webdatenbanken und Mailboxen

Stand 20.05.2018