World4You Internet Services GmbH
Hafenstrasse 47-51
A-4020 Linz, Austria

Version 2018-05-24

Technische und organisatorische Maßnahmen (TOM)

gemäß Artikel 32 Abs. 1 DSGVO

---

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

1. Zutrittskontrolle - kein unbefugter Zutritt zu Datenverarbeitungsanlagen
    1. Alarmanlagen in den Büroräumlichkeiten mit entsprechenden Meldern inkl. Anbindung an Wachdienste
    2. Elektronische Zugangskontrollsysteme mit Berechtigungen je nach Aufgabenerfüllung
    3. Videoüberwachungsanlagen
2. Zugangskontrolle - keine unbefugte Systemnutzung
    1. sichere Kennwörter
    2. automatische Sperrmechanismen
    3. Firewall und IDS Systeme
    4. Einsatz von Verschlüsselung und VPN-Technologien
    5. für Kundenverwaltungssysteme bei Bedarf Zwei-Faktor Authentifizierung
3. Zugriffskontrolle - kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
    1. Umfassende Protokollierung
    2. Einsatz von Aktenvernichtern
    3. Sichere Aufbewahrung von Datenträgern
    4. Ordnungsgemäße Vernichtung von Datenträgern
    5. Sichere Löschung von Datenträgern vor einer etwaigen Wiederverwendung
    6. bedarfsgerechte, restriktive Zugriffsrechte
4. Trennungskontrolle - zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet
    1. Trennung von Entwicklungs- und Produktivumgebung durch Segmentierung von Netzen und Einsatz von Firewalls
    2. Produktivdaten dürfen nicht als Kopie für Testzwecke verwendet werden, ebenso dürfen Testdaten nicht in der Produktivumgebung eingesetzt werden.

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

1. Weitergabekontrolle - kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
    1. Verschlüsselung
    2. Einsatz von VPN Technologien
    3. Authentifizierung

2. Eingabekontrolle - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
    1. Berechtigungssystem
    2. Protokollierung der Eingabe, Änderung oder Löschung von Daten

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Verfügbarkeitskontrolle - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
    1. Backup-Strategie (online/offline; on-site/off-site) durch Datenverteilung auf verschiedene Rechenzentren
    2. unterbrechungsfreie Stromversorgung (USV, Notstromaggregate)
    3. Notfallpläne
    4. Klimatisierte Serverräume
    5. Feuer- und Rauchmeldeanlagen in den Rechenzentren

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

1. Datenschutz-Management
2. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
3. Incident-Response-Management
4. Auftragskontrolle - Keine Auftragsdatenverarbeitung im Sinne Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers
    1. Eindeutige Vertragsgestaltung
    2. strenge Auswahl von Dienstleistern
    3. Maßnahmen gemäß Ziff 1,2 und 3 der TOM sowie des AV-Vertrages