Technisch-organisatorische Maßnahmen

gemäß DSGVO

Inhaltsverzeichnis

Datenverarbeiter

InterMedia Solutions GmbH
(nachstehend IMS genannt)
Ahornstr. 7, 82041 Oberhaching bei München

Ansprechpartner: Robert Holzer
Tel: +49 89-244 151 51
E-Mail: datenschutz@intermedia-solutions.de

1.0 Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen: Klingelanlage mit Kamera, Sicherheitsschlösser, Manuelles Schließsystem, Alarmanlage, Videoüberwachung der Eingänge.

Organisatorische Maßnahmen: Besucher in Begleitung durch Mitarbeiter, Sorgfalt bei Auswahl Reinigungsdienste, Schlüsselregelung

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen: Login mit Benutzername + Passwort, Anti-Viren-Software Server, Anti-Viren-Software Clients, Firewall, Einsatz VPN bei Remote-Zugriffen, Verschlüsselung von Datenträgern, Automatische Desktopsperre, Verschlüsselung von Notebooks,

Organisatorische Maßnahmen: Erstellen von Benutzerprofilen, Zentrale Passwortvergabe, Richtlinie „Sicheres Passwort", Allg. Richtlinie Datenschutz

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, 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.

Technische Maßnahmen: Protokollierung von Zugriffen

Organisatorische Maßnahmen: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen: Trennung von Produktiv- und Testumgebung, Physikalische Trennung (Systeme / Datenbanken / Datenträger)

Organisatorische Maßnahmen: Steuerung über Berechtigungskonzept, Festlegung von Datenbankrechten

2.0 Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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.

Technische Maßnahmen: Technische Protokollierung der Eingabe, Änderung und Löschung von Daten, Manuelle oder automatisierte Kontrolle der Protokolle

Organisatorische Maßnahmen: Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts, Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

2.2 Eingangskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
Technische Maßnahmen: Email-Verschlüsselung, Einsatz von VPN, Protokollierung der Zugriffe und Abrufe, Bereitstellung über verschlüsselte Verbindungen wie sftp und https, elektronische Signaturen

Organisatorische Maßnahmen: Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen, Weitergabe in anonymisierter oder pseudonymisierter Form, Sorgfalt bei Auswahl von Transport Personal und Fahrzeugen

3.0 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen: Feuer- und Rauchmeldeanlagen, Feuerlöscher, Serverraumüberwachung, Serverraum klimatisiert, RAID System / Festplattenspiegelung, unterbrechungsfreie Stromversorgung
Organisatorische Maßnahmen: Backup-Strategie (online/offline; on-site/off-site), Kontrolle des Sicherungsvorgangs, Getrennte Partitionen für Betriebssysteme und Daten

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Technische Maßnahmen: Datenschutz-Management, Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

Organisatorische Maßnahmen: Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet, Regelmäßige Sensibilisierung der Mitarbeiter, die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

4.2 Incident-Response-Management

Technische Maßnahmen: Einsatz von Firewall und regelmäßige Aktualisierung, Einsatz von Spamfilter und regelmäßige Aktualisierung, Einsatz von Virenscanner und regelmäßige Aktualisierung

Organisatorische Maßnahmen: Vorgehensweise zum Umgang mit Sicherheitsvorfällen, Dokumentation von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen: Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind, Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

4.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Organisatorische Maßnahmen: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.