TOM

Technisch organisatorische Maßnahmen gemäß DSGVO

die netztaucher GmbH

Am Gutshof 36
16278 Angermünde

AG Neuruppin

HRB 10596
USt-ID: DE291904918

Bankverbindung

DE23170560600101008872
BIC/SWIFT: WELADED1UMP

Kontakt

+49 3331 • 2502520
www.netztaucher.com

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

1.1 Zutrittskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
• Alarmanlagen • Zäune, Pforten und andere räumliche Begrenzungen • Sicherheitsverglasung • Sicherung von Gebäudeschächten, Fenstern und Türen • Bewegungsmelder und Lichtschranken • Sicherheitsschlösser • Schließsysteme mit Codesperren • Chipkarten für verschlossene Bereiche • Zugangssperren, mit biometrischen Merkmalen abgesichert • datenschutzkonforme Videoüberwachung	• Besucheranmeldung • Besucherbücher und Besucherprotokolle • Verpflichtung für Mitarbeiter und Gäste, Ausweise zu tragen • Empfangspersonal zur Personenkontrolle und Pförtner • sorgfältige Auswahl von Reinigungs- und Wachpersonal

1.2 Zugangskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
• sichere VPN-Verbindung • Verschlüsselung von Datenträgern und mobilen Endgeräten • sichere Firewall • Chipkarten • Anti-Viren-Software • Sperrung von USB-Anschlüssen und anderen externen Schnittstellen • Verriegelung von Gerätegehäusen • Authentifikation mittels Passworteingabe oder biometrischer Scans • Sicherheitsschlösser • Zwei-Faktor-Authentifizierung	• Schlüsselregelungen • Passwortregeln inkl. Vorgaben für die Komplexität des Passwortes • vertrauenswürdiges Personal für die Bereiche Sicherheit und Reinigung • Generierung von Benutzerprofilen • Zuordnung von Benutzerrechten

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	Organisatorische Maßnahmen
• Protokollierung der Zugriffe auf Anwendungen und Prozesse wie z.B. der Datenvernichtung • datenschutzkonforme Vernichtung von Datenträgern (Akten, Laufwerke etc.) • Verschlüsselung von Datenträgern und mobilen Endgeräten • Identifizierungs- und Authentifizierungssystem • sichere Aufbewahrung von Datenträgern	• Passwortregeln • Berechtigungskonzepte • Anpassung der Anzahl an Administratoren, die die volle Zugriffsberechtigung haben • datenschutzkonforme Passwortregel • Protokollierung von Zugriffe • Vier-Augen-Prinzip bei Spezialanwendungen

1.4 Trennungskontrolle

Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist zu garantieren!

Technische Maßnahmen	Organisatorische Maßnahmen
• Verschlüsselung von Datensätzen, die aus dem selbem Zweck verarbeitet werden • klare Trennung der für verschiedene Zwecke gespeicherten Daten	• Mandantentrennun auf die jeweiligen Datensätze angepasste Datenbankrechte und Berechtigungskonzepte • Steuerung über Berechtigungskonzept

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen	Organisatorische Maßnahmen
• automatische Verschlüsselung von Datensätzen inkl. Ablage des Entschlüsselung-Schlüssels mit Zugriffsberechtigung	• manuelle Kürzung von Datensätzen • manuelle Überschreibung von Datensätzen inkl. Wiederherstellungsprozess mit Berechtigung

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

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	Organisatorische Maßnahmen
• gesicherte Transportbehälteri • sichere VPN-Technologie • E-Mail-Verschlüsselung • elektronische Signatur	• Einsatz von vertrauenswürdigem Transportpersonal • regelmäßige Überprüfung von Abruf- und Übermittlungsvorgängen • Anfertigung eines Verfahrensverzeichnisses • Kontrolle der Datenempfänger und entsprechende Dokumentation dieser Empfänger

2.2 Eingabekontrolle

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	Organisatorische Maßnahmen
• Anfertigung eines Protokolls bezüglich der Eingabe, Veränderung und Löschung von Daten • digitales Berechtigungskonzept	• Einrichtung und Verwendung von individuellen Benutzernamen • Vergabe von Zugriffsberechtigungen

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

3.1 Verfügbarkeitskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
• Backups • Diebstahlsicherungen • Klimatisierung des Serverraums • unterbrechungsfreie Stromversorgung • Feuer- und Rauchmelder • Feuerlöscher • Notfall-Management • Virenschutz • Firewall/ IDS	• Alarmanlagen • Schutz des Serverraums vor Risiken, z.B. durch Hochwasser, Brände oder gefährlich platzierte Sanitäranlagen • Erstellung von Backups der Daten • Zyklus der Backup-Anfertigung • Tests für Datenwiederherstellungen

3.2 Wiederherstellbarkeit

Maßnahmen, die die rasche Wiederherstellung der Verfügbarkeit von Daten nach deren zwischenzeitlichen Verlust oder Beschädigung gewährleisten.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Technische Maßnahmen	Organisatorische Maßnahmen
• Verfügbarkeit eines Notfall-RZ	• Notfallkonzept/ Notfallplan

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

4.1 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Technisch-organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Data Privacy by Design and by Default

Technische Maßnahmen	Organisatorische Maßnahmen
• Pseudonymisierung	• Beschränkung der Speicherfrist • Beschränkung der Zugänglichkeit • Beschränkung des Umfangs der Verarbeitung der erhobenen Daten

4.2 Auftragskontrolle

Maßnahmen, die gewährleisten, dass im Rahmen der Auftragsdatenverarbeitung personenbezogenen Daten nur nach Weisung des Auftraggebers verarbeitet werden (können)!

Technische Maßnahmen	Organisatorische Maßnahmen
	• sorgfältige Auswahl des Auftragnehmers • Überprüfung der Datenvernichtung nach Auftragsende • Vertragsstrafen • schriftliche Weisungen an den Auftragnehmer • Vereinbarung von wirksamen Kontrollrechten bezüglich des Auftragnehmers • dauerhafte Überprüfung des Auftragnehmers