Uplinked UG (haftungsbeschränkt) - Waisenhofstraße 19 - 23554 Lübeck
E-Mail: info@uplinked.net

Anlage 1 zum Auftragsverarbeitungsvertrag – Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1. Vertraulichkeit

Die Rechenzentren unserer Subunternehmer entsprechen stets dem Stand der Technik und sind nach ISO 27001 zertifiziert. Über die genauen technischen und organisatorischen Maßnahmen und die geschlossenen Verträge geben wir auf Anfrage Auskunft. Details können ebenfalls online bei den jeweiligen Subunternehmen eingesehen werden.

Der Zutritt zu den Servern ist wie folgt gesichert:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um das Betriebsgelände
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen

Zugangskontrolle zu Cloud-Servern:

Der Server-Login ist nach dem aktuellen Stand der Technik gesichert. Ein Zugang kann nur durch einen personalisierten SSH Sicherheitsschlüssel erfolgen. Der Zugriff erfolgt durch ein Berechtigungssystem nur auf streng abgegrenzte Bereiche.

Zugangskontrolle zu Nextcloud-Instanzen:

Der Zugang zu den Nextcloud-Instanzen ist passwortgeschützt. Zugriff seitens des Auftragnehmers besteht nur für berechtigte Administratoren. Verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert.

Datenträgerkontrolle

Für die sichere Weiterverwendung oder Entsorgung der eingesetzten Festplatten sind die Subunternehmen zuständig. Diese setzen Verfahren gemäß dem Stand der Technik ein.

Zugriffskontrolle

Unberechtigte Zugriffe werden durch regelmäßige Sicherheitsupdates des gesamten Software-Stacks durch den Auftragnehmer verhindert.

Dem Auftraggeber obliegt die Erstellung und Vergabe sicherer Zugangsdaten für seine Nextcloud-Nutzerkonten. Die Passworte werden schon bei der Erstellung auf voreingestellte Sicherheitskriterien überprüft.

Trennungskontrolle

Daten werden physisch oder logisch von Daten anderer Kunden getrennt gespeichert. Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

Pseudonymisierung

Für die Pseudonymisierung der Nutzerkonten ist der Auftraggeber verantwortlich.

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

Weitergabekontrolle

Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DSGVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

Eingabekontrolle

Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst. Änderungen der Daten werden protokolliert.

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

Verfügbarkeitskontrolle

Durch den Auftragnehmer:

- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungs-Programme, SPAM-Filter).
- Festplattenspiegelung bei allen Servern. Spiegelung über mehrere Server für erhöhte Ausfallsicherheit.
- Automatischer Failover-Prozess bei Ausfall von Servern.
- Monitoring aller relevanten Server.

Durch Subunternehmen:

- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.

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

Incident-Response-Management ist vorhanden.

Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DSGVO).

Auftragskontrolle

Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.

Die AGB und die Datenschutzerklärung (online einsehbar) enthalten detaillierte Angaben über Art, Umfang und Zweckbindung der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.