# Anlagen zur Auftragsverarbeitung: 1 (UAV) und 2 (TOM)

## Anlage 1: Liste der Unterauftragsverarbeiter (UAV)

| Nr. | Service | Unterauftragsverarbeiter |
|---|---|---|
| 1 | Hosting, Backup | Netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe |
| 2 | Hosting, Backup | Strato AG, Otto-Ostrowski-Straße 7, 10249 Berlin |

## Anlage 2: Technische und Organisatorische Maßnahmen (TOM)

Verantwortliche Stelle:

**Jörg Reißland**

**Fixiso Sachkunde24.de**

**Hans-Marchwitza-Ring 1**

**14473 Potsdam**

Jörg Reißland (im nachfolgenden „Die Organisation“ genannt) erfüllt diesen Anspruch durch die folgenden Maßnahmen:

***Hinweis:***
*Die Organisation unterhält selbst keinen Server in eigenen Räumen. Die Organisation verarbeitet Informationen auf angemieteten Servern bei darauf spezialisierten und zertifizierten Organisationen gemäß **Anlage 1: Liste der Unterauftragsverarbeiter** im wechselseitigen Redundanzprinzip für Hosting und Backup-Sicherung.*

*Die Organisation schützt die im Prinzip des “Berechtigten Interesse” notwendig zugänglichen Informationen intern und auf eigenen Benutzerschnittstellen und Endgeräten mit folgenden Maßnahmen.*

## 1. Vertraulichkeit gemäß Artikel 32 Abs. 1 lit b DSGVO

### 1.1. Zutrittskontrolle

*Technische Maßnahmen*

- 2-Faktor Authentifizierung im Zugriff auf Server-Control-Panele und Systemrollenadministration

*Organisatorische Maßnahmen*

- Schlüsselregelung / Zugangsberechtigung
- Prozess- und Systemschulungen

### 1.2. Zugangskontrolle

*Technische Maßnahmen*

- Login mit Benutzername & Passwort
- Antivirus-Software Server
- Antivirus-Software Clients
- Antivirus-Software mobile Geräte
- Firewall

*Organisatorische Maßnahmen*

- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Richtlinie „Sicheres Passwort“
- Zentrale Passwortvergabe für 2. Sicherheitsebene

### 1.3. Zugriffskontrolle

*Organisatorische Maßnahmen*

- Einsatz eines Berechtigungskonzepts
- Minimale Anzahl von Administratoren
- Verwaltung von Benutzerrechten durch Administratoren

### 1.4. Trennungskontrolle

*Technische Maßnahmen*

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung von Daten (Systeme / Datenbanken / Datenträger)

- Mandantenfähigkeit relevanter Anwendungen

*Organisatorische Maßnahmen*

- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- Ausstattung der Datensätze durchgehend mit Zweckattributen

### 1.5. Pseudonymisierung (Art. 25 Abs. 1 DSGVO, Art. 32 Abs. 1 lit. a DSGVO)

*Technische Maßnahmen*

- Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (verschlüsselt)

*Organisatorische Maßnahmen*

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst automatisch anonymisieren / pseudonymisieren.

## 2. Integrität gemäß Artikel 32 Abs. 1 lit b DSGVO

### 2.1. Weitergabekontrolle

*Technische Maßnahmen*

- Email-Verschlüsselung (bei Anhängen mit personenbezogenen Daten)
- Einsatz von VPN

*Organisatorische Maßnahmen*

- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen

### 2.2. Eingabekontrolle

*Organisatorische Maßnahmen*

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer**namen** (zusätzlich zur Rechtevergabe über Benutzer**gruppen**)

## 3. Verfügbarkeit und Belastbarkeit gemäß Artikel 32 Abs. 1 lit b DSGVO

Die Organisation hat keinen Server in den eigenen Räumen. Die in 3. nachfolgend genannten TOM gelten Unterauftragsverarbeiter der **Anlage 1: Liste der Unterauftragsverarbeiter (UAV)** und werden auf die Organisation lediglich vererbt.

### 3.1 Verfügbarkeitskontrolle

*Technische Maßnahmen*

- Feuer- und Rauchmeldeanlagen
- Unterbrechungsfreie Stromversorgung (USV)

*Organisatorische Maßnahmen*

- Backup & Recovery-Konzept
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

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

### 4.1 Datenschutz-Management

*Technische Maßnahmen*

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung

*Organisatorische Maßnahmen*

- ggf. Datenschutzbeauftragter
- Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung / Nachschulung der Mitarbeiter mindestens 1x jährlich

### 4.2 Incident-Response-Management

*Technische Maßnahmen*

- Einsatz von Firewall(s), die regelmäßig aktualisiert werden
- Einsatz von Spamfiltern, die regelmäßig aktualisiert werden
- Einsatz von Virenscannern, die regelmäßig aktualisiert werden

*Organisatorische Maßnahmen*

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf eine Meldepflicht gegenüber der zuständigen Aufsichtsbehörde). Die Dokumentation wird permanent weiterentwickelt
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

**4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**

*Technische Maßnahmen*

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

*Organisatorische Maßnahmen*

- Es werden mit allen IT-Dienstleistern die eigene und eingesetzte Software-Lösungen auf „Privacy by Design“ sowie „Privacy by Default“ hin optimiert

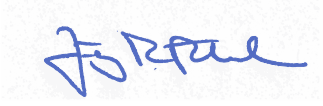
**4.4. Auftragskontrolle (Outsourcing an Dritte)**

*Organisatorische Maßnahmen*

- Auswahl von Unterauftragnehmern unter Sorgfaltsgesichtspunkten im Bezug auf Datenschutz und Datensicherheit
- Vorherige und regelmäßige Prüfung der von Unterauftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Abschluss der notwendigen Vereinbarungen zur Unterauftragsverarbeitung

Potsdam, 31.12.2022

Ort, Datum



Jörg Reißland
Fixiso - Sachkunde24