TOM

Technische und organisatorische Maßnahmen.

userwerk GmbH | Ehinger Straße 19 | 89077 Ulm
Geschäftsführer: Dr. Markus Kalb, Daniel Speyer | USt-IdNr.: DE 314162223 | HRB 735644 Ulm

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**
  Direktive IT und Informationssicherheit, Standard Betrieb und Sicherheit, Richtlinie Serverraumsicherheit, auszugsweise: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

- **Zugangskontrolle**
  Direktive IT und Informationssicherheit, Standard Betrieb und Sicherheit, Richtlinie Netzwerksicherheit, auszugsweise: Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

- **Zugriffskontrolle**
  Direktive IT und Informationssicherheit, Standard Betrieb und Sicherheit, Richtlinie Vergabe von Berechtigungen, auszugsweise: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

- **Trennungskontrolle**
  Direktive IT und Informationssicherheit, Standard Betrieb und Sicherheit, auszugsweise: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**
  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.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
  Direktive IT und Informationssicherheit, Standard Betrieb und Sicherheit, IT-Endbenutzerrichtlinie, auszugsweise: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

- **Eingabekontrolle**
  Direktive IT und Informationssicherheit, Standard Betrieb und Sicherheit, auszugsweise: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

3. Verfügbarkeit & Belastbarkeit

(Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**
  Direktive IT und Informationssicherheit, Standard Betrieb und Sicherheit, auszugsweise: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.

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

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- **Datenschutz-Management**
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO)
- **Auftragskontrolle**
  Direktive IT und Informationssicherheit, Standard Betrieb und Sicherheit, Richtlinie Sicherheitsregeln für Kooperation mit externen IT Dienstleistern, auszugsweise: 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.