Buch & Berger

Buch & Berger e.U. Die Buchwebagentur Lindengasse 16/2/8 A-1070 Wien
Kontakt: Mag. Stefan Buchberger E-Mail: agentur@buchundberger.net
Telefon: 0043 (0)699 1958 5048 Web: www.buchundberger.net

# Technische und organisatorische Maßnahmen (TOM) gemäß DSGVO

Stand: 18.08.2018

## 1. Vertraulichkeit

- **Zutrittskontrolle**: Unsere Büroräume werden nur von der Geschäftsführung genutzt; Besucher sind nie alleine in den Räumlichkeiten; Zutritt nur mit Schlüssel.
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung (Kennwörter, automatische Sperrmechanismen, Fingerprint); Anti-Viren-Software, Firewall, Richtlinie *Sicheres Passwort*.
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems; verschlüsselter Zugriff auf Entwicklungsserver und Kundenwebspaces; Meldung von Zugriffen fremder Geräte; Protokollierung von Zugriffen; Berechtigungsprofile; Verwaltung von Benutzerrechten durch Administrator.
- **Trennungskontrolle**: Trennung von Produktiv- und Testumgebung; Mandantenfähigkeit relevanter Anwendungen

## 2. Integrität

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport; Bereitstellung über verschlüsselte Verbindungen wie SFTP und HTTPS; Protokollierung der Zugriffe und Abrufe.
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind; Protokollierung; Nachvollziehbarkeit durch Benutzernamen.

## 3. Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle**: regelmäßige verschlüsselte Backups in die Cloud und auf externe Festplatten; Aufbewahrung von Sicherungsmedien an einem sicheren Ort außerhalb der Büroräumlichkeiten; getrennte Partitionen für Betriebssysteme und Daten.

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Datenschutz-Management**: Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet, Regelmäßige Sensibilisierung der Mitarbeiter.
- **Incident-Response-Management**: Virenschutz, Firewall, Spamfilter.
- **Datenschutzfreundliche Voreinstellungen**: Es werden nicht mehr personenbezogene Daten erhoben als erforderlich; einfache Ausübung des Widerrufsrechts des Betroffenen.
- **Auftragskontrolle**: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers; Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen; Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung.