Anlage 1 – Technisch-organisatorische Maßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der Dr. Josef Raabe Verlags GmbH zum Datenschutz gemäß Bundesdatenschutzgesetz § 9 nebst Anlage und Art. 32, 24 DSVGO betrieben werden.

1. Verschlüsslung und Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Verschlüsselung
Maßnahmen, die geeignet sind, dass Daten ohne Kenntnis des zugehörigen Schlüssels nach Möglichkeit nicht oder nur mit völlig unverhältnismäßigem Aufwand lesbar gemacht werden können.

#	Maßnahmen
1	Einsatz von HTTPS-Transportverschlüsselung
2	Aktive Verschlüsselung auf mobilen Endgeräten

Pseudonymisierung
Pseudonymisierung umfasst Maßnahmen, die geeignet sind, Unbefugten Rückschlüsse über persönlichen Informationen von Personen zu verwehren.

#	Maßnahmen
1	Eine Pseudonymisierung erfolgt, wo erforderlich und möglich im jeweiligen Verfahren im Rahmen der (verfahrens-)spezifischen technischen und organisatorischen Maßnahmen. Beispielsweise im Zuge der Software-Entwicklung und der Testumgebung.

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

Zutrittskontrolle
Maßnahmen, die gewährleisten, dass Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden.

#	Maßnahmen
1	Chipkarten-/Transponder-Schließsystem
2	Sicherheitsschlösser
3	Zutrittskontrollen des Hostingpartners siehe https://www.hetzner.com/AV/TOM.pdf

Zugangskontrolle
Maßnahmen, um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können.

#	Maßnahmen
1	Authentifikation mit Benutzer und Passwort
2	Einsatz von Antivirensoftware
3	Einsatz von Firewalls
4	Einsatz von Mobile Device Management
5	Einsatz von VPN-Technologien
6	Gehäuseverriegelung
7	Benutzerberechtigungen verwalten

8	Passwortvergabe/Passwortregeln
9	Protokollierung der Besucher/Besucherbereich
10	Sorgfältige Auswahl des Reinigungspersonals
11	Sorgfältige Auswahl des Sicherheitspersonals

Zugriffskontrolle
Maßnahmen um das unbefugte Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems verhindern.

#	**Maßnahmen**
1	Einsatz von Aktenvernichtern
2	Datenschutzkonforme Vernichtung von Datenträgern
3	Physische Löschung von Datenträgern vor deren Wiederverwendung
4	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
5	Anzahl der Administratoren auf das „Notwendigste“ reduzieren
6	Erstellen eines Berechtigungskonzepts
7	Passwortrichtlinie inkl. Länge und Wechsel
8	Sichere Aufbewahrung von Datenträgern
9	Verwaltung der Benutzerrechte durch Systemadministratoren

Maßnahmen, die die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden gewährleisten.

#	**Maßnahmen**
1	Trennung von Produktiv- und Testsystem
2	Logische Mandantentrennung (softwareseitig)

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

Weitergabekontrolle
Maßnahmen, die das unbefugte Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport verhindern.

#	**Maßnahmen**
1	Einrichtung von VPN-Tunneln

Eingabekontrolle
Maßnahmen, um festzustellen, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind.

#	**Maßnahmen**
1	Protokollierung der Eingabe, Änderung und Löschung von Daten
2	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

3	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle
Maßnahmen, die den Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust gewährleisten.

#	Maßnahmen
1	Feuerlöschgeräte in Serverräumen[1]
2	Feuer- und Rauchmeldeanlagen[1]
3	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen[1]
4	Klimaanlage in Serverräumen[1]
5	Schutzsteckdosenleisten in Serverräumen
6	Unterbrechungsfreie Stromversorgung (USV)[1]
7	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
8	Back-up- und Recoverykonzept
9	Notfallpläne
10	Testen der Datenwiederherstellung

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
Maßnahmen, die eine schnellstmögliche Wiederherstellung von Daten gewährleisten.

#	Maßnahmen
1	Back-up-Strategie

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Allgemeine organisatorische Maßnahmen
Maßnahmen, die geeignet sind die Prüfung und Kontrolle

#	Maßnahmen
1	Überprüfung auf datenschutzfreundliche Voreinstellungen der Anwendung (Art. 25 Abs. 2 DS-GVO)
2	Kontrolle der Verarbeitungstätigkeiten durch externen Datenschutzbeauftragten
3	Verpflichtung der Mitarbeiter des Auftragsnehmers auf die Wahrung der Vertraulichkeit der Daten (Datengeheimnis)

[1] Anwendung ausschließlich im RZ-Betrieb.

Auftragskontrolle
Maßnahmen, die geeignet sind, dass keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers stattfindet.

#	**Maßnahmen**
1	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
2	Laufende Überprüfung des Auftragsnehmers und seiner Tätigkeit ⇨ Vorhandensein eines aktuellen Zertifikats nach DIN/EN ISO 27001 und eines Sicherheitskonzepts
3	Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungs-vertrag) (Art. 28 DS-GVO)
4	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
5	Verpflichtung der Mitarbeiter des Auftragsnehmers auf das Datengeheimnis