TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMs)

gemäß Art. 32 DSGVO

Anlage 1 zur Vereinbarung zur Auftragsverarbeitung (Art. 28 DSGVO), Fassung Juli 2026

Der Auftragsverarbeiter – 7pxl.de, eine Marke von SecondMay Design, Inhaber: Serge Efremov, Mühlbachstraße 18, 74842 Billigheim – hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung die folgenden technischen und organisatorischen Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

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

Snapshot-Technologie

- IP-Adressen von Endnutzern werden beim Aufruf eines Kurzlinks oder QR-Codes ausschließlich im Arbeitsspeicher verarbeitet und noch im selben Verarbeitungsschritt durch eine anonymisierte Ziffernfolge ersetzt.
- Eine Speicherung von IP-Adressen oder daraus abgeleiteten Standortdaten findet zu keinem Zeitpunkt statt.
- Gespeichert werden ausschließlich anonymisierte, aggregierte Statistikwerte (z. B. Anzahl der Zugriffe, Herkunftsland, Gerätetyp).

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

Zutrittskontrolle

- Betrieb der Infrastruktur in ISO-27001-zertifizierten Rechenzentren in Deutschland (Hosting-Provider: IONOS SE, Elgendorfer Str. 57, 56410 Montabaur).
- Physischer Zugang zu den Rechenzentren ausschließlich für autorisiertes Personal des Rechenzentrumsbetreibers; Sicherung u. a. durch Zutrittskontrollsysteme und Videoüberwachung.

Zugangskontrolle

- Personalisierte Benutzerkonten; keine Sammel-Accounts für administrative Systeme.
- Passwort-Richtlinien sowie Zwei-Faktor-Authentifizierung für administrative Zugänge.
- Automatische Sperrung inaktiver Sitzungen.
- Absicherung administrativer Arbeitsplätze: vollständige Festplattenverschlüsselung, automatische Bildschirmsperre, zeitnahe Einspielung von Sicherheitsupdates.

Zugriffskontrolle

- Rollen- und Berechtigungskonzept nach dem Least-Privilege-Prinzip.
- Granulare Team-Berechtigungen auf Plattformebene: Kontoinhaber steuern je Mitglied, welche Ressourcen (Links, QR-Codes, Projekte) eingesehen, erstellt, bearbeitet oder gelöscht werden dürfen.

Trennungskontrolle

- Logische Mandantentrennung: Daten verschiedener Kunden werden getrennt verarbeitet und sind gegeneinander abgeschottet.
- Trennung von Entwicklungs-, Test- und Produktivumgebung.

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

Weitergabekontrolle

- Transportverschlüsselung sämtlicher Verbindungen per TLS (HTTPS) – sowohl für das Kunden-Dashboard als auch für alle Link-Weiterleitungen.
- Verschlüsselte Speicherung der Kundendaten.
- Keine Weitergabe von Daten an Dritte zu Werbezwecken.

Eingabekontrolle

- Nachvollziehbarkeit von Änderungen an Konten und Ressourcen durch systemseitige Protokollierung administrativer Vorgänge.

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

- Redundante Strom- und Netzanbindung, Klimatisierung sowie Brandschutz im Rechenzentrum (RZ-Standard des Betreibers).
- Regelmäßige Datensicherungen (Backups) mit definierten Wiederherstellungsverfahren; die Wiederherstellbarkeit wird regelmäßig überprüft.
- Kontinuierliches Monitoring der Systeme; öffentlich einsehbare Verfügbarkeits-Statusseite.
- Schutzmaßnahmen auf Netzwerkebene (Firewalls, Basisschutz gegen DDoS-Angriffe).

5. Löschkonzept

- Löschung sämtlicher im Auftrag verarbeiteter personenbezogener Daten nach Beendigung des Hauptvertrages unverzüglich, spätestens innerhalb von 30 Tagen (gemäß § 11 der Vereinbarung zur Auftragsverarbeitung).
- In Datensicherungen enthaltene Daten werden spätestens mit der turnusmäßigen Überschreibung der Backups gelöscht; bis dahin sind sie dem aktiven Zugriff entzogen und werden nicht wiederhergestellt.
- Vom Kunden gelöschte Ressourcen (Links, QR-Codes, Projekte) werden aus den Produktivsystemen entfernt.
- Auf Verlangen wird die Löschung in Textform bestätigt.

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

- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design & by Default, Art. 25 DSGVO) als Entwicklungsprinzip der Plattform.
- Regelmäßige Überprüfung und Aktualisierung der technischen und organisatorischen Maßnahmen.
- Definierter Prozess zur Erkennung, Bewertung und Meldung von Datenschutzverletzungen (Art. 33, 34 DSGVO); Meldung an den Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, mit den Mindestinhalten gemäß § 8 der Vereinbarung zur Auftragsverarbeitung.
- Verpflichtung aller mit der Verarbeitung befassten Personen auf Vertraulichkeit.

7. Auftragskontrolle (Art. 28 DSGVO)

- Sorgfältige Auswahl von Subunternehmern unter besonderer Berücksichtigung von Datenschutz und Datensicherheit.
- Aktuell eingesetzter Subunternehmer: IONOS SE, Elgendorfer Str. 57, 56410 Montabaur (Hosting, Rechenzentrum in Deutschland) – siehe Anlage 2 zur Vereinbarung zur Auftragsverarbeitung.
- Vertragliche Sicherstellung eines gleichwertigen Datenschutzniveaus bei allen Subunternehmern.

- Information des Verantwortlichen über beabsichtigte Änderungen mindestens vier Wochen vorab in Textform; Widerspruchsrecht des Verantwortlichen gemäß § 6 Abs. 3 der Vereinbarung zur Auftragsverarbeitung.

Diese Übersicht wird regelmäßig überprüft und bei Bedarf an den Stand der Technik angepasst. Die jeweils aktuelle Fassung erhalten Sie über das Vertrauens-Center auf 7pxl.de oder per E-Mail an info@7pxl.de.