Anhang 2 – Technische und organisatorische Maßnahmen

Stand: Juli 2026

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, die pixx.io zum Schutz personenbezogener Daten implementiert hat. Die Maßnahmen dienen der Gewährleistung eines angemessenen Schutzniveaus für die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten gemäß Art. 32 DSGVO.

Die beschriebenen Maßnahmen entsprechen dem zum Zeitpunkt der Leistungserbringung bestehenden Sicherheitsniveau. pixx.io überprüft die Maßnahmen regelmäßig und entwickelt diese bei Bedarf weiter, um technische, organisatorische oder rechtliche Entwicklungen zu berücksichtigen. Das Schutzniveau der Maßnahmen wird hierbei nicht wesentlich reduziert.

Die nachfolgend aufgeführten Maßnahmen stellen eine Beschreibung der wesentlichen Sicherheitsvorkehrungen dar und begründen keinen Anspruch auf die Umsetzung bestimmter technischer Lösungen oder Produkte.

1. Vertraulichkeit

1.1. Zutrittskontrolle

- Betrieb der Systeme in physisch gesicherten Rechenzentren.
- Beschränkung des Zutritts zu sicherheitsrelevanten Bereichen auf autorisierte Personen.
- Kontrolle und Dokumentation von Besucherzugängen.

1.2. Zugangskontrolle

- Zugriff auf Systeme ausschließlich über individuelle Benutzerkennungen.
- Einsatz angemessener Authentifizierungsverfahren.
- Vergabe und Überprüfung von Zugriffsrechten nach dem Need-to-know-Prinzip.

1.3. Zugriffskontrolle

- Rollen- und Berechtigungskonzepte zur Beschränkung des Datenzugriffs.
- Beschränkung administrativer Zugriffe auf berechtigte Personen.
- Verpflichtung der Mitarbeitenden auf Vertraulichkeit.

1.4 Trennungskontrolle

- Maßnahmen zur logischen Trennung von Daten unterschiedlicher Kunden.
- Berechtigungskonzepte zur Vermeidung unbefugter Zugriffe zwischen Mandanten.
- Getrennte Verarbeitung entsprechend den jeweiligen Verarbeitungszwecken.

2. Integrität

2.1. Weitergabekontrolle

- Schutz personenbezogener Daten bei der Übertragung durch geeignete technische Maßnahmen.
- Einsatz angemessener Verschlüsselungsverfahren bei Datenübertragungen.
- Authentifizierte und autorisierte Zugriffe auf Systeme und Schnittstellen.
- Verfahren zur Vermeidung unbefugter Offenlegung personenbezogener Daten.

2.2. Eingabekontrolle

- Nachvollziehbarkeit relevanter Systemaktivitäten.
- Protokollierung sicherheitsrelevanter Ereignisse und administrativer Tätigkeiten.
- Dokumentierte Prozesse zur Verwaltung von Berechtigungen und Änderungen.

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

- Maßnahmen zur Sicherstellung der Verfügbarkeit der Systeme.
- Regelmäßige Datensicherungen.
- Schutz vor Verlust, Zerstörung oder Beschädigung von Daten.

3.2. Wiederherstellbarkeit

- Verfahren zur Wiederherstellung von Daten und Systemen nach Störungen.
- Regelmäßige Überprüfung der Sicherungs- und Wiederherstellungsprozesse.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Regelmäßige Überprüfung und Weiterentwicklung der Sicherheitsmaßnahmen.
- Sensibilisierung und Schulung von Mitarbeitenden.
- Prozesse zur Erkennung, Meldung und Behandlung von Sicherheits- und Datenschutzvorfällen.
- Dokumentierte Verantwortlichkeiten im Bereich Informationssicherheit und Datenschutz.

5. Auftragskontrolle

- Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen.
- Auswahl und Kontrolle von Unterauftragsverarbeitern nach datenschutzrechtlichen Anforderungen.
- Vertragliche Verpflichtung von Unterauftragsverarbeitern auf angemessene Datenschutz- und Sicherheitsstandards.
- Regelmäßige Überprüfung der von Unterauftragsverarbeitern bereitgestellten Sicherheits- und Datenschutzinformationen.

6. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

- Berücksichtigung von Datenschutzanforderungen bei Entwicklung und Betrieb der Dienste.
- Verarbeitung nur der für den jeweiligen Zweck erforderlichen personenbezogenen Daten.
- Möglichkeiten zur rollenbasierten Steuerung von Zugriffs- und Sichtbarkeitsrechten.