Appendix 2 – Technical and Organizational Measures

As of July 2026

This document is provided in English for convenience only. The German version is the legally binding version. In the event of any discrepancy or inconsistency between the English and German versions, the German version shall prevail.

This appendix describes the technical and organizational measures that pixx.io has implemented to protect personal data. These measures are intended to ensure an appropriate level of protection for the confidentiality, integrity, availability, and resilience of the systems and services related to the processing of personal data in accordance with Article 32 of the GDPR.

The measures described correspond to the security level in effect at the time the services are provided. pixx.io regularly reviews these measures and refines them as necessary to account for technical, organizational, or legal developments. The level of protection provided by these measures is not significantly reduced in the process.

The measures listed below describe the essential security precautions and do not constitute a commitment to implement specific technical solutions or products.

1. Confidentiality

1.1. Access Control

- Operation of the systems in physically secured data centers.
- Restriction of access to security-sensitive areas to authorized personnel.
- Monitoring and documentation of visitor access.

1.2. Access Control

- Access to systems exclusively via individual user IDs.
- Use of appropriate authentication procedures.
- Granting and reviewing access rights according to the need-to-know principle.

1.3. Access Control

- Role- and permission-based concepts to restrict data access.
- Restriction of administrative access to authorized individuals.
- Requiring employees to maintain confidentiality.

1.4 Segregation of duties

- Measures for the logical separation of data from different clients.
- Authorization concepts to prevent unauthorized access between clients.
- Separate processing in accordance with the respective processing purposes.

2. Integrity

2.1. Disclosure Control

- Protection of personal data during transmission through appropriate technical measures.
- Use of appropriate encryption methods for data transmissions.
- Authenticated and authorized access to systems and interfaces.
- Procedures to prevent unauthorized disclosure of personal data.

2.2. Input Controls

- Traceability of relevant system activities.
- Logging of security-related events and administrative activities.
- Documented processes for managing permissions and changes.

3. Availability and Resilience

3.1. Availability Control

- Measures to ensure system availability.
- Regular data backups.
- Protection against loss, destruction, or damage to data.

3.2. Recoverability

- Procedures for restoring data and systems after disruptions.
- Regular review of backup and recovery processes.

4. Procedures for regular review, assessment, and evaluation

- Regular review and refinement of security measures.
- Awareness-raising and training for employees.
- Processes for detecting, reporting, and handling security and data protection incidents.
- Documented responsibilities in the area of information security and data protection.

5. Control of Processing

- Processing of personal data exclusively in accordance with documented instructions from the controller.
- Selection and oversight of subprocessors in accordance with data protection requirements.
- Contractual obligation of subprocessors to adhere to appropriate data protection and security standards.
- Regular review of the security and data protection information provided by subprocessors.

6. Data Protection through Technology Design and Privacy-Friendly Defaults

- Consideration of data protection requirements during the development and operation of the services.
- Processing only the personal data necessary for the respective purpose.
- Options for role-based control of access and visibility rights.