ioFM Privacy Policy

Effective Date: 8.12.2025
Version: V1, last updated 8.12.2025
Provider: ioLabs AG ("ioLabs"), Schübelstrasse 6, 8700 Küsnacht, Switzerland

This Privacy Policy ("Policy") explains how ioLabs AG ("Company") collects, uses, discloses and protects personal data in connection with the ioFM platform and related websites, applications and services (collectively, the "Services").

The Company is committed to protecting personal data and to complying with applicable data protection laws, including the EU General Data Protection Regulation (GDPR) and relevant national legislation.

1. Who is responsible for your data?

For most processing activities described in this Policy (website, marketing, user accounts, support), the data controller is: ioLabs AG, Schübelstrasse 6, 8700 Küsnacht, Switzerland, Email: info@iolabs.ch, Phone: +41 77 44 24 259. When our customers use ioFM to process their own data (e.g. building, project and room information), the Company generally acts as a data processor and processes personal data on behalf of the customer, who remains the data controller.

2. Scope and who this Policy applies to

This Policy applies to personal data relating to visitors of ioFM-related websites and landing pages, to business contacts and prospects (including individuals acting on behalf of customers, partners or suppliers), to registered users of the ioFM platform such as administrators, facility managers, consultants and project team members, and to individuals whose data may be included in customer content uploaded or integrated into ioFM (for these individuals, our customer is usually the primary controller). This Policy does not apply to information that cannot be linked to an identified or identifiable individual (anonymised data).

3. What data we collect

The Company may collect and process the following types of personal data:

3.1 Data you provide directly

Contact and identification data: name, company, business email address; account data: username, password (stored as a cryptographic hash), organisation, role and per-missions; communication data: contents of emails, contact forms, meeting notes, chat messages and other com-munications with us; support data: information provided during support requests, including screenshots, exports and log files you choose to share.

3.2 Data collected automatically

When you visit our websites or use the Services, we may automatically collect: Technical data: IP address, device identifiers, brow-ser type and version, operating system, laguage settings, time zone, URL of the referring page. Usage data: pages and features used, clickstream data, access times, login time-stamps, error logs and similar usage information. Cookies and similar technologies: see Section 9 (Cookies and tracking technologies).

3.3 Data processed within ioFM on behalf of customers

Depending on how a customer uses ioFM, the platform may store: Project and building data: project na-mes, building names, room identifiers, room names, classifications, tags, attributes and similar metadata. Uploaded files: plans, photos, sections, 3D scans, point clouds, asset lists, room lists and other content. Free-text input: comments, notes and des-criptions that customers or users enter into ioFM, which may contain personal data if they choose to do so. The customer decides what information to upload or create in ioFM and remains responsible for ensuring this data is collected and processed lawfully.

4. How and why we use your data

We process personal data only where there is a legal basis under applicable law. Depending on the context, we may rely on one or more of the following legal bases: performance of a contract, legitimate interests, consent, or legal obligation.

4.1 To provide and operate the Services, we process personal data to register and authenticate users, provide access to ioFM and its features, operate, maintain and improve the platform and overall user experience, and deliver customer support and handle inquiries. For these purposes, we typically use account data and contact data, as well as usage and log data and support data.

4.2 For communication and customer relationship management, we process personal data to respond to inquiries, demo and trial requests, and support tickets, to manage our relationships with customers, partners and suppliers, and to send service-related notifications such as security or maintenance information. For these purposes, we typically use contact data, communication data and account data.

4.3 For marketing and information about our services, we process personal data to send infor-mation about ioFM and related products or events (such as newsletters, product updates or invitations), where permitted, and to analyse and improve the effectiveness of our marketing activities. For these purposes, we typically use contact data, communication preferences and information about interactions with our marketing communications. You can object to direct marketing at any time (see Section 9).

4.4 For security, fraud prevention and compliance, we process personal data to protect the security and integrity of the platform and its underlying infrastructure, to detect, prevent and investigate fraud, abuse and security incidents, and to comply with legal obligations (such as tax and accounting rules) as well as to establish, exercise or defend legal claims. For these purposes, we typically use log data, technical data and account data, and, where necessary (for example in the context of incident analysis), limited content.
4.5 Service Improvement and AI Model Training
ioLabs may use Customer Data to improve the Services and to train, develop, and enhance AI and machine learning models that power ioFM features, subject to the following terms:
(a) Purpose. Customer Data, including building models, floor plans, spatial configurations, and associated metadata, may be used to train AI models that improve accuracy, automate processes, and enhance functionality for all ioFM users.
(b) Safeguards. When Customer Data is used for AI training, it is processed in secure, access-controlled environments. Trained models do not contain, memorise or reproduce identifiable Customer Data or trade secrets, and Customer Data is not shared with third parties for their independent training purposes. Any data used for training is subject to the same security standards as production data.
(c) Opt-Out Right. Customers may opt out of AI training at any time by sending a written request to info@iolabs.ch. Upon opt-out, Customer Data will no longer be used for AI training purposes. Opting out will not affect Customer's access to the Services, features, or support quality. Data already incorporated into trained models prior to opt-out cannot be extracted, but no further Customer Data will be used.
(d) Legal Basis. This processing is based on ioLabs' legitimate interest in improving and developing its Services (Art. 6(1)(f) GDPR / Art. 31 nDSG), balanced against Customer's interests through the safeguards and opt-out mechanism described above.

5. Legal bases for processing

Where the EU General Data Protection Regulation (GDPR) or comparable data protection laws apply, the Company relies on one or more of the following legal bases for processing personal data:
5.1 Performance of a contract (Art. 6(1)(b) GDPR) The processing is necessary for the performance of a contract to which the data subject (or the data subject's organisation) is party, or in order to take steps at the request of the data subject prior to entering into a contract. This includes, in particular, providing the Services to customers and users, managing user accounts, and responding to demo or trial requests.
5.2 Legitimate interests (Art. 6(1)(f) GDPR) The processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Such legitimate interests include, for example, operating secure and efficient Services, preventing misuse and fraud, analysing and improving the Services, maintaining business relationships, and enforcing or defending legal claims.
5.3 Consent (Art. 6(1)(a) GDPR) The data subject has given consent to the processing of their personal data for one or more specific purposes, for example for receiving certain marketing communications, participating in optional surveys, or allowing the use of non-essential cookies and similar technologies where required by law. Consent may be withdrawn at any time with effect for the future.
5.4 Legal obligation (Art. 6(1)(c) GDPR) The processing is necessary for compliance with a legal obligation to which the Company is subject, such as statutory retention obligations, accounting and tax requirements, or responding to lawful requests from public authorities. When acting strictly as a processor on behalf of a customer, the Company processes personal data exclusively on the basis of the customer's documented instructions and in accordance with the legal basis determined by the customer (as controller) under the applicable data protection laws.

6. Applicable Law and Regional Privacy Frameworks

The Company operates ioFM and related services in a global environment and may process personal data of individuals in different countries and regions. Accordingly, the Company complies with the data protection and privacy laws that apply in the jurisdictions in which it offers its services or where data subjects are located. Without limitation, this includes in particular:
6.1 European Union / European Economic Area (EU/EEA)
For data subjects in the EU/EEA, the Company processes personal data in accordance with the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and any applicable implementing or supplementary national legislation.
The information provided in this Privacy Policy is intended to meet the transparency requirements of Articles 12–14 GDPR, and the rights described in the section on data subject rights are provided in line with Chapter III GDPR.
6.2 United Kingdom
For data subjects in the United Kingdom, the Company processes personal data in accordance with the UK GDPR (as incorporated into UK law by the European Union (Withdrawal) Act 2018) and the UK Data Protection Act 2018. References in this Privacy Policy to "GDPR" shall be read, where appropriate, as including the UK GDPR for data subjects in the UK.
6.3 Switzerland
For data subjects in Switzerland, the Company processes personal data in accordance with the Swiss Federal Act on Data Protection (FADP/DSG) as revised and effective from 1 September 2023 (co-mmonly referred to as "nDSG" or "revDSG"), together with its implementing Ordinance on Data Protection (DPO/DSV) and Ordinance on Data Protection Certification (DPCO/VDSZ).

Where this Privacy Policy refers to concepts from the GDPR, such references shall be interpreted in a manner consistent with the corresponding concepts under Swiss data protection law. The Company maintains safeguards that meet the requirements of both the GDPR and the Swiss FADP. The Swiss Federal Data Protection and Information Commissioner (FDPIC) is the competent supervisory authority for data protection matters in Switzerland.

6.4 United States and other non-European jurisdictions

For data subjects located in the United States, the Company endeavours to take into account applicable federal and state privacy laws, such as the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA) and, where relevant, similar state-level privacy laws in other U.S. jurisdictions. Where required, the Company provides additional notices or rights descriptions tailored to such local laws.

For data subjects in other countries, the Company complies with the data protection and privacy require-ments that apply under the laws of the relevant jurisdiction to the extent they govern the Company's activities in that territory.

6.5 Conflicts of law and higher standards

Where there is a conflict between applicable data protection laws, or where more than one legal regime could apply to the same processing activity, the Company will apply the legal framework that offers the higher level of protection for data subjects, insofar as this is feasible and consistent with its contractual obligations. In any event, the Company aims to main-tain a globally consistent baseline of privacy and security protections, while implementing regionspecific measures where required by law.

6.6 Additional regional notices

In certain jurisdictions, additional disclosures or specific rights may apply (for example, for residents of U.S. or specific non-European countries). Where this is the case, the Company may provide supplemental regional notices that should be read together with this Privacy Policy. In the event of any contradiction between such regional notices and this Privacy Policy, the regional notice shall prevail for data subjects in the relevant jurisdiction.

7. How we share personal data

We do not sell personal data. We share personal data only where necessary and with appropriate safeguards:

7.1 Within the Company

Personal data is made available only to departments and personnel who need it to perform their tasks (e.g. product, engineering, support, sales, finance), foll-owing the principle of least privilege.

7.2 Service providers and sub-processors

We engage carefully selected third-party service providers to support the operation of the Services, including:

- Cloud hosting and infrastructure providers
- Email and communication tools
- Customer support and ticketing systems
- Monitoring, logging and analytics services

These providers may have access to personal data only to the extent necessary to perform their services and are contractually bound to process such data solely on our instructions and with appropriate security measures.

A current list of sub-processors can be obtained upon request at info@iolabs.ch or as described in the applicable DPA.

7.3 Customers (controller relationship)

When we act as processor, certain log or support data may be shared with the relevant customer in order to analyse incidents, usage or support issues, in line with our contractual obligations.

7.4 Legal and regulatory disclosures

We may disclose personal data where required by law, regulation, court order or official request, to legal advisors, auditors or insurers where necessary to protect our rights, comply with legal obligations or resolve disputes, and in connection with corporate transactions (such as mergers, acquisitions or sales of assets), in each case subject to appropriate confidentiality safeguards.

8. International transfers

Where possible, we aim to process and store personal data within the European Union (EU) or European Economic Area (EEA).

If personal data is transferred to or accessed from a country outside the EU/EEA that does not provide an adequate level of data protection, we take appropriate safeguards, such as:

- Standard Contractual Clauses (SCCs) approved by the European Commission, and/or
- Additional technical and organisational measures (e.g. encryption, access controls).
- Further information about international transfers and the applicable safeguards is available upon request at info@iolabs.ch.

8.1 Transfers from Switzerland

- For personal data originating from Switzerland, the Company ensures that international transfers comply with the requirements of the Swiss FADP. This includes:
- Transfers to countries recognised by the Swiss Federal Council as providing adequate data protection (as listed in Annex 1 to the DPO/DSV);
- Where no adequacy decision exists, reliance on the Swiss-adapted Standard Contractual Clauses (SCCs) as recognised by the FDPIC, or other appropriate safeguards under Art. 16–17 FADP;
- Implementation of supplementary technical and organisational measures where required by the circumstances of the transfer.

The list of countries with adequate protection under Swiss law may differ from the EU adequacy decisions. Further information about specific transfer mechanisms is available upon request per email.

9. Your rights

Subject to applicable law and certain limitations, you have the following rights in relation to your personal data:

9.1 Right of access: to obtain confirmation whether we process personal data about you and to receive a copy.
9.2 Right to rectification: to have inaccurate or incomplete personal data corrected.
9.3 Right to erasure: to request deletion of your personal data in certain circumstances.
9.4 Right to restriction of processing: to request restriction where legally applicable.
9.5 Right to object: to object to processing based on our legitimate interests, including the right to object at any time to processing for direct marketing.
9.6 Right to withdraw consent: where processing is based on your consent, you may withdraw it at any time with effect for the future. To exercise these rights, please contact us at: info@iolabs.ch

If we process your data on behalf of a customer (as processor), we may refer your request to the relevant customer, who is responsible for handling it. You also have the right to lodge a complaint with a competent data protection supervisory authority, in particular in the EU/EEA member state of your habitual residence, place of work or place of the alleged infringement.

10. Cookies and tracking technologies

Our websites and the ioFM platform may use cookies and similar technologies to provide and improve the Services.

10.1 Strictly necessary cookies: required for basic site and platform functionality (e.g. login, session management).
10.2 Functional cookies: remember your settings and preferences (e.g. language).
10.3 Analytics cookies: help us understand how the Services are used and improve performance and usability.
10.4 Marketing cookies: where used, help measure and optimise marketing campaigns.

Where required by law, we only use non-essential cookies with your consent. You can manage or withdraw your consent at any time via the cookie banner or your browser settings.

11. Data retention

We retain personal data only for as long as necessary for the purposes for which it was collected, or as required by law. Retention periods vary by data type:

- Customer content and models: deleted within 30 days after contract termination (plus up to 60 days in encrypted backups)
- Modelling request input files: deleted 6 months after the subscription ends or upon written request
- User account and platform usage data: retained for 12 months after contract termination
- Billing and invoicing records: retained for 10 years as required by Swiss accounting law (Art. 958f CO)
- Security and access logs: retained for 12 months

Once retention periods expire, personal data is deleted, anonymised or archived in a secure and restricted manner.

12. Security

The Company uses appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse or alteration, including:

- Encryption of data in transit (TLS) and, where appropriate, at rest.
- Role-based access control and strong authentication mechanisms.
- Segregated environments and regular security updates.
- Backups and disaster recovery procedures.
- Logging and monitoring of relevant system events.
- Internal policies, confidentiality obligations and training for employees.

While no system can be completely secure, we continuously review and improve our security measures. ioLabs AG holds ISO/IEC 27001 certification for its Information Security Management System (ISMS), ensuring that appropriate technical and organisational measures are implemented and continuously improved. Additionally, ioLabs is ISO 9001 certified, reflecting a commitment to quality management and customer satisfaction across all business processes.

13. Children's privacy

The Services are intended for business and professional use and are not directed to children. We do not knowingly collect personal data from children for marketing or account purposes. If you believe that a child's data has been provided to us without appropriate authorisation, please contact us per email and we will take appropriate steps. The Com-pany does not use personal data for automated decision-making, including profiling, within the meaning of Article 22 GDPR that produces legal effects concerning data subjects or similarly significantly affects them.

14. Governing Law and Dispute Resolution

This Privacy Policy and any disputes arising out of or in connection with it (including non-contractual disputes) shall be governed by and construed in accordance with the substantive laws of Switzerland, without regard to its conflict of laws principles. The exclusive place of jurisdiction for any disputes shall be Küsnacht (Canton of Zurich), Switzerland, unless otherwise required by mandatory law (including, where applicable, the right of data subjects to bring claims in the courts of their habitual residence). For data subjects in the EU/EEA, this choice of law and jurisdiction does not deprive them of the protection afforded by mandatory provisions of the law of their country of habitual residence, nor of their right to bring proceedings before the courts of that country.

15. Changes to this Notice

We may update this Policy from time to time to reflect changes in legal requirements, our Services or our

processing activities. The latest version of this Policy will always be available at: https://iolabs.ch/en/iofm/
If we make material changes, we will notify customers and, where appropriate, users through suitable channels (e.g. by email or via in-app notifications).

16. Contact

Questions, concerns or requests relating to this Notice or to the processing of personal data by the Company may be directed to

Adress:	ioLabs AG Schübelstrasse 6 8700 Küsnacht Switzerland.
Email:	info@iolabs.ch
Phone:	+41 77 44 24 259
Product Website:	www.iolabs.ch
ioFM website:	www.iofm.ch