

Privacy Policy

1. Introduction and Scope of this Policy

This Privacy Policy explains how **MAI Technologies AG** (“**Provider**”) processes personal data in connection with the use of its Platform for which the Provider is controller, including SaaS-Services and AI-Services.

It governs all processing activities carried out under the revised Swiss Federal Act on Data Protection (FADP).

Because the Provider may offer services to individuals located in the European Union, this Privacy Policy also incorporates the requirements of the European Union’s General Data Protection Regulation (GDPR), to the extent applicable.

The Provider acts in different roles depending on the type of processing. For processing carried out for the Provider’s own purposes (such as operating and securing the Platform, billing, and direct communication with customers), the Provider is controller. For the processing of customer personal data - including due-diligence documents and deal collaborator/invitee data, carried out on behalf of and under the instructions of the customer, the Provider acts solely as processor, and the respective customer is the controller. For transparency purposes, this Privacy Policy may also refer to personal data that the Provider processes solely in its capacity as a data processor on behalf of a customer. Any such references are provided for informational purposes only and are not intended to constitute a complete or exhaustive description of the personal data processed by the Provider in its capacity as a data processor. Such processing is governed by the Data Processing Agreement entered into between the Provider and the relevant customer, which shall prevail over this Privacy Policy in the event of any inconsistency with respect to such processing.

2. Identity and Contact Details of the Controller

Contact details are made available on the Provider’s website. If and to the extent that the Provider becomes subject to Article 27 GDPR, it will appoint an EU representative and publish the representative’s contact details in an appropriate form.

The Provider's identity and contact details are: MAI Technologies AG, Färberstrasse 6, 8008 Zürich, Switzerland; email: dataprotection@dilix.ch.

3. Categories of Personal Data Processed

The Provider processes personal data necessary for the operation of its Platform and the fulfilment of contractual obligations. Where AI-Services are used, the Provider may process user inputs, prompts, system outputs, and diagnostic or security-related metadata.

The Provider does not intend to process sensitive categories of data unless explicitly agreed. Under both FADP and GDPR, sensitive or special-category data requires enhanced protection and can only be processed under strict conditions.

This applies to the Provider's structured, core processing activities. Uploaded due-diligence documents, in respect of which the Provider acts as a data processor rather than a data controller, may nonetheless incidentally contain sensitive or special-category personal data within their encrypted payloads — for example, information relating to administrative or criminal proceedings (litigation files) — which remains subject to the same enhanced protection requirements under the FADP and GDPR.

The personal data processed includes in particular: (a) Platform user account data (name, email address, profile image, role, organisation, session data such as IP address and user agent, OAuth/authentication tokens, and passkey (WebAuthn) credential data) (processed by the Provider primarily as processor to enable access to the Platform on behalf of the customer; certain aspects, such as security monitoring and abuse prevention, are processed by the Provider as controller for its own purposes); (b) deal collaborator and invitee data (email address, first and last name, role, company-role information, and invite reason) (processed by the Provider as processor on behalf of the customer); (c) personal data extracted from uploaded due-diligence documents, which chiefly concerns third parties who are not Platform users — including names, titles or roles (e.g. board positions), signing dates and email addresses of document signatories, and resolved person identities — and, within encrypted document payloads, potentially broader personal data contained in the source documents, such as employee data, litigation files, financial information, national identification numbers and dates of birth (processed by the Provider as processor on behalf of the customer); and (d) product usage and telemetry data linked to individual users (processed by the Provider as processor to the extent used to fulfil the customer's contracted use of the Platform; also processed by the Provider as controller for its own purposes, such as service improvement and analytics) . The Provider has not identified any health data or biometric templates among the data processed; passkey (WebAuthn) credential data constitutes authentication material rather than a biometric template.

The categories of data subjects concerned are: Platform end users, i.e. employees of client organisations (M&A advisory firms, law firms, private equity or venture capital investors, investment banks, and target-company staff) who use the Platform; and deal collaborators and invitees, i.e. external individuals invited to a specific transaction who may not be full Platform users; third parties named in due-diligence documents, such as signatories, company officers, directors, shareholders and other natural persons appearing in uploaded documents, who are not themselves Platform users; and individuals identified through public commercial registries (e.g. the Swiss commercial registry, Zefix) consulted during deal setup.

4. Purposes and Legal Bases for Processing

The Provider processes personal data solely for legitimate and transparent purposes, including operating the Platform, providing SaaS-Services, enabling AI-Services, supporting system security, fulfilling contractual obligations, communicating with customers, complying with legal requirements, and improving service functionality.

Under the revised FADP, personal data must be processed lawfully, proportionately, and in good faith.

If and to the extent that GDPR applies, the Provider processes personal data on the following legal bases:

- where processing is necessary for the performance of a contract (Art. 6(1)(b) GDPR);

- where processing is necessary for compliance with a legal obligation (Art. 6(1)(c) GDPR);
- where the Provider has a legitimate interest in processing (such as fraud prevention, network and information security, platform performance and analytics, and the establishment, exercise, or defence of legal claims), and those interests are not overridden by data subject rights (Art. 6(1)(f) GDPR);
- where consent is required, such processing is based on freely given, informed consent (Art. 6(1)(a) GDPR).

If special-category data is processed, the Provider will rely on an exception in Article 9 GDPR, such as explicit consent.

In particular, the Platform is operated as an M&A due-diligence support tool: it ingests, extracts and analyses uploaded deal documents (such as contracts, board minutes, cap tables, financial statements and correspondence, for which the Provider is controller) to build a structured overview of a target company, including entity, party and signatory extraction together with supporting evidence, for use by M&A advisors, law firms, investors and target companies collaborating on a transaction. Processing further supports Platform account management (authentication, including OAuth via Microsoft and Google and passkeys, session management, and deal collaborator/invitee management), as well as an AI-assisted extraction feature and a conversational “setup agent” that elicits deal and target information and cross-checks it against public company registries (e.g. the Swiss commercial registry, Zefix).

5. Principles Governing the Processing of Personal Data

All processing activities comply with the core principles of both FADP and GDPR, including purpose limitation, proportionality, transparency, accuracy, data minimisation, and secure processing.

The Provider implements **Privacy by Design** and **Privacy by Default**, both of which are expressly mandated under the revised Swiss FADP.

6. Processing Related to AI-Services

The Provider offers AI-based functionalities that may involve automated processing, profiling, and generation of probabilistic outputs. Where AI-Services process personal data (for which the Provider is controller), the Provider informs users appropriately about the nature and purpose of processing, the logic involved in automated processing, and the limitations inherent in AI-generated content.

The revised FADP explicitly recognises profiling and requires transparency about automated decision-making and its effects.

The Provider may use anonymized or aggregated data to improve its own system. Customer may at any time opt out of this use by written notice to the Provider; such opt-out takes effect for future processing activities only. Identifiable personal data will not be used for model/system training/improvement unless the customer has expressly authorized such use.

The Provider's primary production AI/LLM service is Google Vertex AI (Gemini), which is used for document extraction and for the conversational setup agent. This processing takes place in Google's europe-west4 region (Netherlands).

7. Disclosure of Personal Data to Third Parties

Personal data may be disclosed to trusted service providers where necessary to operate the Platform, fulfil contractual obligations, or comply with legal obligations. Under Article 9 FADP, the Provider is responsible for ensuring that processors provide adequate data security and that any subcontracting is approved. Where GDPR applies, disclosures will also comply with Articles 28 and 29 GDPR governing processors and sub-processors.

The Provider currently engages the following subprocessors: (a) Google Cloud EMEA Limited (70 Sir John Rogerson's Quay, Dublin, Ireland) for cloud hosting, compute, database, file and document storage, secret management, and encryption key management, processed in the europe-west6 region (Zurich, Switzerland); (b) Google Cloud EMEA Limited for Vertex AI (Gemini) AI/LLM processing, in the europe-west4 region (Netherlands); (c) Microsoft Ireland Operations Limited (Microsoft Entra ID) as an OAuth login and identity provider; (d) Google Ireland Limited as an OAuth login and identity provider; and (e) Inngest Inc. (San Francisco, California, USA), which provides the durable workflow and execution engine and receives only event identifiers (project, document and user IDs), without names, email addresses or document content.

8. International Transfers of Personal Data

The Provider may transfer personal data to countries recognized as adequate by the Swiss Federal Council or the European Commission. Transfers to countries without adequacy decisions rely on legally recognized safeguards, including Standard Contractual Clauses adapted for Swiss and EU requirements following relevant guidance.

Transfers to EU/EEA states are permitted under Swiss law due to their recognized adequacy.

Personal data is primarily processed and stored in Switzerland (Google Cloud, europe-west6 region, Zurich). AI/LLM processing takes place in the Netherlands (europe-west4 region). Background job orchestration (Inngest) takes place in the United States and is limited to identifiers only (no names, email addresses or document content); this transfer relies on Standard Contractual Clauses as an appropriate safeguard. The same subprocessor locations and safeguards apply where the Provider processes personal data as data processor on behalf of the customer under the Data Processing Agreement.

9. Data Security Measures

The Provider applies appropriate technical and organisational measures, such as encryption, access controls, secure hosting infrastructure, logging, and continuous monitoring. Under the revised FADP, companies must report data breaches that pose high risks to data subjects to the Federal Data Protection and Information Commissioner (FDPIC) as soon as possible.

If GDPR applies, the Provider will notify the competent supervisory authority within 72 hours and will notify affected individuals when the breach creates a high risk (Articles 33 and 34 GDPR).

In particular, the Provider applies the following measures: role-based access control tied to organisation membership; session-based authentication via OAuth (Microsoft Entra ID, Google) and passkeys (WebAuthn); encryption keys managed via Google Cloud KMS and Secret Manager; application-layer encryption of document payloads using AES-256-GCM; encryption in transit via HTTPS/TLS and enforced encrypted database connections; automated backups and point-in-time recovery with a seven-day retention window; redundant managed infrastructure (Google Cloud Run and Cloud SQL); continuous monitoring and alerting via Google Cloud Monitoring; a CI/CD pipeline using short-lived, federated credentials together with dependency and vulnerability scanning; and network-edge DDoS and web-application-firewall protection (rate limiting, geo-blocking, OWASP-based rules) on the production load balancer. Physical data-centre security is provided by Google Cloud Platform and evidenced by Google's ISO 27001 and SOC 2 attestations. Personnel with access to personal data are bound by confidentiality obligations and complete mandatory security-awareness and data-privacy training within 30 days of onboarding and annually thereafter.

10. Retention and Deletion of Personal Data

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected or as required by statutory retention obligations. Upon expiration of the retention period or termination of the contractual relationship, personal data will be deleted or anonymized unless further processing is legally permissible in an anonymized form. Personal data is retained only for as long as required to fulfil the specific operational purposes set out in this Policy, comply with statutory obligations, or assert and defend legal claims.

The following retention criteria will be applied:

- **Due Diligence Document Data (Processor Role):** Uploaded files, deal payloads, and extracted diligence entities are retained solely for the duration of the relevant project workspace. Upon contract expiration or customer request, all documents and derived payloads are securely erased or returned within 30 days, subject to existing rolling backups.
- **Platform User Account Data:** User profile data is maintained during active platform engagement. Following the termination of an organization's account, user identities are deleted or irreversibly anonymized within 90 days.
- **Billing and Financial Records:** Transaction histories, invoices, and billing contact data are retained for 10 years from the end of the relevant financial year, in compliance with Article 958f of the Swiss Code of Obligations (CO).
- **Session, Security Logs and Telemetry Data:** Security logs, authentication trails, and IP-level access events are maintained for 6 months, after which they are purged or aggregated without identifiers.
- **Backups:** Point-in-time database and snapshot backups are retained on an automated 7-day rolling cycle and systematically overwritten.

Where statutory limitation periods under Swiss or applicable European law allow for claims (typically 5 to 10 years), relevant contractual correspondence may be preserved in restricted-access legal archives until those periods expire. Once retention obligations lapse, data is permanently erased or irreversibly anonymized.

11. Rights of Data Subjects

Individuals have the right to request access to their personal data, request corrections to inaccurate information, request deletion where legally permissible, and request portability of their data. The revised FADP significantly strengthens the right to access and introduces a right to data portability. Individuals also have the right to lodge a complaint or report with the Swiss Federal Data Protection and Information Commissioner (FDPIC / EDÖB).

Under GDPR, individuals also have the right to object to processing, the right to restrict processing, and the right to withdraw consent at any time, and they may lodge complaints with an EU supervisory authority.

The Provider responds to requests within the statutory 30-day period required by Swiss law. See Section 15 for how to exercise these rights, including the applicable procedure where the Provider acts as processor.

12. Automated Decision-Making and Profiling

Where AI-Services involve automated decision-making or profiling, the Provider provides meaningful information about the logic involved and offers safeguards.

Profiling is defined and regulated under the revised FADP, requiring clear transparency about automated decisions affecting individuals.

If GDPR applies, individuals may invoke Article 22 GDPR, which grants a right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects.

13. Cookies and Similar Tracking Technologies

The Provider uses cookies and similar technologies to ensure proper technical functioning, improve user experience, analyse usage, and support security.

Under Swiss law, cookies are regulated by both the FADP and the Telecommunications Act (TCA). Article 45c TCA requires that users be informed about the use and purpose of cookies and that they be offered a means to refuse non-essential cookies.

The 2025 FDPIC Cookie Guidelines clarify that essential cookies may be used without consent, whereas non-essential cookies, particularly those enabling cross-site tracking or high-risk profiling, may require consent. If and to the extent consent is required or GDPR applies, the Provider will obtain explicit opt-in consent before deploying non-essential cookies such as analytics, marketing, and profiling technologies, and users may withdraw such consent at any time.

Cookie preferences are managed through a consent banner shown as a fixed bar at the bottom of the screen on a visitor's first visit to the Platform's public website, offering a simple choice to Accept or Reject (no per-category toggles). No non-essential cookies or third-party tracking scripts (such as analytics, advertising, or tools including LinkedIn, Facebook, or Intercom) are loaded unless and until the visitor accepts; rejecting or ignoring the banner keeps the site free of any such tracking calls. The visitor's choice is stored locally in the browser (via localStorage) and applies across the whole site until changed. Visitors can change their preference at any time via the Platform's cookie preference panel ("Your preference"), which lets them toggle Analytics & Marketing cookies on or off, or by clearing their browser's stored site data.

14. Amendments to this Privacy Policy

The Provider may amend this Privacy Policy to reflect changes in law, technology, or data processing practices. Any updated version will be published on the Provider's website.

15. Contact

Individuals may contact the Provider at any time regarding the processing of their personal data or to exercise their rights. All such requests will be handled confidentially and in accordance with applicable law and may require an identity check before providing any information. Requests should be submitted by email to the address below. Where a request concerns personal data that the Provider processes as processor on behalf of a customer (such as due-diligence document data or deal collaborator/invitee data), the Provider will, where appropriate, forward the request to the relevant customer as controller; data subjects are encouraged to contact the relevant customer directly in such cases.

MAI Technologies AG, Färberstrasse 6, 8008 Zürich, Switzerland.
E Mail: dataprotection@dilix.ch.

MAI Technologies AG, 21 September 2026