

MAI Technologies AG SaaS-Service Terms and Conditions

Based on the order for SaaS-Services (hereinafter the "**Order**") provided by MAI Technologies AG (hereinafter the "**Provider**" or individually the "**Party**" and together with the Customer the "**Parties**"), the customer (hereinafter the "**Customer**" or individually the "**Party**" and together with the Provider the "**Parties**") agrees to be bound, without reservation, to the following MAI Technologies AG SaaS-Service Terms and Conditions (hereinafter "**T&C**").

The Order (including its annexes), these T&C and the annexes mentioned herein are all an integral part of the agreement between the Provider and the Customer (hereinafter the "**Agreement**").

1. Services

1.1. General

1.1.1. The Provider operates a platform and an application as described in the Order (hereinafter the "**Platform**") and in connection therewith provides to the Customer certain Software-as-a-Service services (hereinafter "**SaaS-Services**") as specified in the Order and in these T&C.

1.1.2. As part of its SaaS-Services, the Provider:

- a) sets up its Platform as specified in Annex 1;
- b) operates the Platform and provides the support services according to the Service Level Agreements in Annex 2 (hereinafter the "**Support Services**");
- c) grants the Customer access to the Platform to use the Platform and to receive the Support Services.

1.1.3. The SaaS-Services are subject to these T&C and to the timely payment of the fees set forth in the Order (hereinafter the "**Fees**") by the Customer.

1.2. Support Services and Upgrades

1.2.1. During the Term the Provider will provide the Support Services to the Customer, and may apply Upgrades to the Platform, in accordance with the service level agreement set out in Annex 2.

1.2.2. The Provider may sub-contract the provision of any of the SaaS-Services including Support Services at its own free discretion without requiring the consent of the Customer, subject, in respect of Subcontractors processing Customer Data, to the notification and objection mechanism set out in the respective Data Processing Agreement entered into between the Parties.

1.3. Customisation

1.3.1. From time to time the Provider and the Customer may agree that the Provider will customise the Platform in accordance with the specifications agreed in writing between the Parties (hereinafter "**Customisation**").

1.3.2. From the date when a Customisation is first made available to the Customer, the Customisation shall form part of the Platform under the Agreement, and accordingly from that date the Customer's rights to use the Customisation shall be governed by these T&C.

1.3.3. The Customer acknowledges that the Provider may make any Customisation available to its other customers at any time following the making available of that Customisation to the Customer.

1.3.4. Any and all intellectual property rights in the Customisations shall, as between the Parties, be the sole and exclusive property of the Provider.

1.4. AI-as-a-Service

1.4.1. As part of the SaaS-Services, and where specified in the Order, the Provider may make available certain artificial intelligence functionalities, including but not limited to machine learning models, predictive analytics, generative AI capabilities, or automated decision-support features (together the “**AI-Services**”). The AI-Services form part of the Platform and are provided to the Customer for the Permitted Purpose.

1.4.2. The AI-Services are currently powered primarily by Google Vertex AI (Gemini), used for document extraction and the conversational setup agent, with such processing taking place in Google's europe-west4 region (Netherlands), as further described in the Data Processing Agreement between the Parties.

1.4.3. AI-Services generate outputs automatically based on underlying models, algorithms and training data. The Customer acknowledges that:

- a) AI outputs may be probabilistic in nature and may contain inaccuracies, errors, hallucinations, or incomplete information;
- b) AI outputs, including any AI-generated reports, flags, or recommendations, are provided to support the Customer's own due diligence process and do not constitute legal, financial, or professional advice.**
- c) the Customer is solely responsible for reviewing and validating all AI outputs before using them for any operational, commercial, or decision-making purposes.
- d) where the Platform indicates a confidence level or similar indicator in respect of an AI output, reflecting the Provider's product philosophy of transparency regarding the reliability of its AI-generated outputs, such indication is provided for informational purposes only, does not constitute a warranty as to the accuracy of the relevant output, and does not reduce the Customer's obligations under paragraph (c) above.

1.4.4. Unless expressly excluded in the Order, or unless the Customer subsequently opts out by written notice to the Provider (any such opt-out shall take effect for future processing activities only):

- a) the Provider may use Customer Data in anonymized or aggregated form to calibrate, improve, or validate its own system;
- b) such anonymized or aggregated data shall not be considered Customer Confidential Information; and
- c) all improvements, derivative models, fine-tuned models, embeddings, or algorithmic enhancements resulting from such use shall remain the exclusive property of the Provider.

1.4.5. The Provider will not use Customer Data in identifiable form to train/improve its own system unless explicitly authorized by the Customer in writing.

1.4.6. The Customer agrees:

- a) to use the AI-Services only for the Permitted Purpose and in compliance with applicable law, including data protection, employment, consumer protection, and transparency legislation;
- b) to ensure that end-users understand when they are interacting with AI systems if required under applicable law;

- c) to ensure, in accordance with its warranty under Section 8.1, that it has all lawful grounds and has implemented all legally required safeguards for any special categories of personal data contained in documents or other content it uploads to the Platform, given that such data may be processed by the AI-Services as part of the Provider's automated document extraction functionality;
- d) not to use the AI-Services for any high-risk or use cases requiring certification or conformity assessment under the EU AI Act or similar laws, unless expressly agreed in writing.
- e) to acknowledge that the AI-Services incorporate underlying third-party foundation AI models which the Provider has not itself developed or trained, and that the Provider's own extraction functionality is built on top of, and orchestrates the use of, such underlying models; that the Parties' respective roles and obligations under the EU AI Act or any similar legislation are determined by the actual facts of the technical setup and are not altered by this Agreement; and that, in any event and irrespective of such regulatory characterisation, the Customer remains solely responsible for establishing and maintaining, prior to relying on any AI-Services outputs (including data extracted from due-diligence documents) for any operational, commercial, or decision-making purpose, an appropriate human-in-the-loop review process within its own organisation.

1.4.7. The Provider will:

- a) implement reasonable technical and organisational measures to ensure the safe operation of AI-Services;
- b) maintain documentation on AI model architecture, evaluation methods, and known limitations, as reasonably required for Customer compliance;
- c) provide transparency information on model capabilities, intended purpose, known risks, and limitations;
- d) not use Customer Data for any purpose not expressly permitted under the Agreement.

1.4.8. The Provider does not guarantee that AI-Services will be bias-free, error-free, or suitable for any specific Customer use case unless explicitly stated in the Order.

1.4.9. The Customer must not and agrees not to:

- a) attempt to extract model weights, training data, or underlying algorithms;
- b) use AI-Services to develop competing AI models;
- c) circumvent model safety, monitoring, rate limits, or usage restrictions;
- d) use the AI-Services for unlawful automated decision-making, biometric identification, surveillance, discrimination, or any other prohibited practice under applicable law.

1.4.10. Intellectual Property in AI Models and Outputs

- a) All AI models, model components, prompts, training data (excluding Customer Data), and algorithmic structures are and remain the exclusive property of the Provider.
- b) Subject to payment of Fees, the Customer receives a non-exclusive licence to use the AI-generated outputs for the Permitted Purpose.
- c) The Customer retains ownership of Customer Data used as input into the AI-Services.
- d) The Provider makes no representations regarding the non-infringement of AI-generated outputs, and the Customer assumes full responsibility for verifying that such outputs do not infringe third-party rights.

- 1.4.11. In addition to Section 7 (Limitations and exclusions of liability), the Provider shall not be liable for:
- a) decisions made by the Customer or by third parties based on AI outputs;
 - b) any damage resulting from reliance on incomplete, inaccurate, harmful, or biased AI outputs;
 - c) regulatory compliance of the Customer's use of AI-Services, including under the EU AI Act or equivalent legislation;
 - d) any content generated by end-users through the AI-Services.
- 1.4.12. The Customer remains fully responsible for all AI-assisted decisions, communications, or actions.
- 1.4.13. The Provider may monitor and log the Customer's use of the AI-Services for the purposes of:
- a) ensuring compliance with this Agreement;
 - b) system security, abuse detection and misuse prevention;
 - c) quality improvement and debugging;
 - d) meeting transparency and documentation obligations under applicable law.
- Such logs shall be handled in accordance with Section 8 (Data Protection).
- 1.4.14. The Provider may temporarily suspend the AI-Services (without suspending the entire SaaS-Service) where:
- a) necessary to maintain system security or safety;
 - b) required by law or regulatory guidance;
 - c) the Customer's use poses material risk to model integrity, system performance, or third-party rights.
- 1.4.15. Suspension of AI-Services does not entitle the Customer to a refund unless explicitly stated in the Order
- 1.4.16. The Provider may also temporarily suspend the Customer's access to the Platform and the SaaS-Services as a whole (without terminating the Agreement) where the Customer is in material breach of the Agreement, including through misuse or abuse of the Platform, and, where such breach is capable of remedy, has not remedied it within 10 Business Days of being notified thereof, or where immediate suspension is necessary to prevent harm to the Provider, other customers, or third parties. The no-refund principle set out in the preceding paragraph applies correspondingly to any such suspension.

2. Customer Rights and Obligations

2.1. Use of Services by Customer

- 2.1.1. Subject to the Customer's compliance with the Agreement and to the Customer paying the Fees, the Provider grants to the Customer a non-exclusive licence to use the Platform for the purposes specified in the Order (hereinafter the "**Permitted Purpose**") during the term of the Agreement.
- 2.1.2. The use of the Platform by the Customer shall be subject to the following licensing terms:
- a) the Customer may only use the Platform for the Permitted Purpose;
 - b) the Customer must not and agrees not to:
 - (i) copy or reproduce Platform or any part of the Platform other than in accordance with the licence granted in the Order and/or these T&C;
 - (ii) sell, sub-license, resell, rent, lease, loan, supply, distribute, redistribute, publish or re-publish the Platform or any part of the Platform;

- (iii) modify, alter, adapt, translate or edit, or create derivative works of, the Platform or any part of the Platform;
 - (iv) reverse engineer, decompile, disassemble the Platform or any part of the Platform (except as mandated by applicable law);
 - (v) use the Platform other than in accordance with the Provider's instructions;
 - (vi) use the Platform in any way that is unlawful, illegal, fraudulent or harmful or use the Platform in connection with any unlawful, illegal, fraudulent or harmful purpose or activity;
 - (vii) use the Platform in any way that causes, or may cause, damage to the Platform or impairment of the availability or accessibility of the Platform, or any of the areas of, or services on, the Platform; or
 - (viii) circumvent or remove or attempt to circumvent or remove the technological measures applied to the Platform for the purposes of preventing unauthorised use.
- c) the Platform may only be used by the employees, agents and sub-contractors of the Customer;
 - d) the Customer must not and agrees not to sub-license its right to access and use the Platform or allow any unauthorised person to access or use the Platform
- 2.1.3. For the avoidance of doubt, the Customer has no right to directly or indirectly via a third party access the source code of the Platform, either during or after the Term.
- 2.1.4. The Customer shall use all reasonable endeavours to ensure that no unauthorised person will or could access the Platform using the Customer's account.
- 2.1.5. It is the Customer's responsibility to ensure and comply with its own internal policies, union contracts as well as legal requirements of the respective countries regarding the privacy protection of its own employees who access or use the Platform.
- 2.1.6. The Customer agrees to ensure that access to the Platform is strictly restricted to persons authorised to use it.

2.2. Duty to cooperate

- 2.2.1. It is the Customer's sole responsibility to access the Platform through the Provider's web application and to upload or otherwise submit the relevant data via the Platform's user interface. Where the Provider subsequently makes available an application programming interface ("API") for this purpose, this Section 2.2.1 will apply correspondingly to the Customer's use of such API."
- 2.2.2. The Customer will ensure that all instructions in relation to the Agreement and Customer's use of the SaaS-Service will be given by a duly authorized representative of the Customer to the Provider representative as notified to the Customer by the Provider in the Order.
- 2.2.3. The Provider:
- a) may treat all such instructions as the fully authorised instructions of the Customer; and
 - b) will not comply with any other instructions in relation to the Agreement without first obtaining the consent of a Customer representative.
- 2.2.4. The Parties will hold contract management meetings at Customer's site, or by telephone or via the internet at the reasonable request of either Party.

3. Fees

- 3.1. The Customer agrees to pay the Fees as set forth in the Order.

- 3.2. If the Customer does not timely pay any amount properly due to the Provider, the Provider may charge the Customer interest on the overdue amount at the rate of 5% per year from time to time (which interest will accrue daily and be compounded quarterly).
- 3.3. The Provider may suspend access to the Platform and the provision of the SaaS-Services if any amounts due to be paid by the Customer to the Provider are overdue by more than 30 calendar days. In the case of a suspension of the SaaS-Service, the Customer remains fully obligated to pay the Fees and the Customer is not entitled to claim any refunds or damages.

4. Intellectual Property

All intellectual property rights pertaining to the SaaS-Services and the Platform shall, as between the Parties, be the exclusive property of the Provider. This includes intellectual property rights in Customisations as per Section 1.3.4.

5. Data Ownership

- 5.1. The data collected and processed via the Platform consist of:
- a) the business documents uploaded to the Platform by the Customer or by other Platform user authorised in connection with the Agreement (including deal collaborators, invitees, and target company representatives) to the Provider in connection with the Agreement (such as but not limited to contracts, board minutes, cap tables, financial statements and correspondence); and
 - b) the system operations data (such as but not limited to Platform user account data, session and authentication data, deal collaborator/invitee data, and product usage/telemetry data); and
 - c) Any structured or extracted representation of the business documents referred to in para. a) above, to the extent generated by the Provider's processing of such documents and based on and derived from their content.
- (hereinafter "**Customer Data**").
- 5.2. The Customer is owner of the Customer Data and the Provider processes the Customer Data on behalf of the Customer subject to the Agreement. This does not restrict the Provider's own use of Platform user account data and product usage/telemetry data for the Provider's own purposes (such as platform security, abuse prevention, and service improvement) as described in the Privacy Policy, nor the Provider's right to use anonymized or aggregated Customer Data pursuant to Section 1.4.4. For the sake of clarity, classification as Customer Data pursuant to Section 5.1 governs only the ownership, export, and deletion of the underlying data; it does not affect the Provider's right to condition ongoing access to Provider's features on an active subscription and payment of the applicable fees under Section 3.
- 5.3. The Customer acknowledges that any data models, algorithms, or other derivative works generated by the Provider based on the use of the SaaS-Service and on Customer Data are the sole property of the Provider, provided that such generation is limited to Customer Data in anonymized or aggregated form in accordance with Section 1.4.4, or otherwise expressly authorized by the Customer in writing pursuant to Section 1.4.5. This Section 5.3 does not limit or override the Provider's processing obligations under the Data Processing Agreement between the Parties, including the

restriction on using Customer Data in identifiable form for the purposes described therein.

6. Warranties

6.1. The Customer warrants to the Provider that

- a) it has the legal right and authority to enter into and perform its obligations under the Agreement;
- b) it will use the SaaS-Services and the Platform strictly in compliance with any law and the conditions set forth in the Agreement.

6.2. The Provider warrants to the Customer that:

- c) it has the legal right and authority to enter into and perform its obligations under the Agreement;
- d) it will perform its obligations under the Agreement with reasonable care and skill.

6.3. The Customer acknowledges that:

- a) complex software is never wholly free from defects, errors and bugs, and the Provider gives no warranty or representation that the Platform will be wholly free from such defects, errors and bugs; and
- b) complex software is never entirely free from security vulnerabilities; and subject to the other provisions of the Agreement, the Provider gives no warranty or representation that the Platform will be entirely secure; and
- c) the Provider does not warrant or represent that the Platform will be compatible with any application, program or software not specifically identified as compatible in Annex 1.

6.4. All of the Parties' warranties and representations in respect of the subject matter of the Agreement are expressly set out in the terms of the Agreement. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of the Agreement will be made or implied into the Agreement.

7. Limitations and exclusions of liability

7.1. Nothing in the Agreement will:

- a) limit or exclude the liability of a Party for death or personal injury resulting from negligence;
- b) limit or exclude the liability of a Party for fraud or fraudulent misrepresentation by that Party;
- c) limit any liability of a Party in any way that is not permitted under applicable law; or
- d) exclude any liability of a Party that may not be excluded under applicable law.

7.2. The Provider will not be liable:

- a) in respect of any loss of profits, income, revenue, use, production or anticipated savings;
- b) for any loss of business, contracts or commercial opportunities;
- c) for any loss of or damage to goodwill or reputation;
- d) in respect of any loss or corruption of any data, database or software;
- e) in respect of any special, indirect or consequential loss or damage; and

- f) for any losses arising out of a Force Majeure Event, a Force Majeure Event meaning an event, or a series of related events, that is outside the reasonable control of the Party affected (including failures of or problems with the Internet or a part of the Internet, hacker attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third party, changes to the law, disasters, explosions, fires, floods, riots, terrorist attacks and wars).

8. Data protection

- 8.1. The Customer warrants that it has the legal right to disclose all data protected by any applicable data protection legislation (hereinafter "**Personal Data**") that it does in fact disclose to the Provider under or in connection with the Agreement.
- 8.2. The Provider warrants that:
 - a) it will act only on instructions from the Customer in relation to the processing of any Personal Data performed by the Provider on behalf of the Customer; and
 - b) it has in place appropriate security measures (both technical and organisational) against unlawful or unauthorised processing of Personal Data and against loss or corruption of Personal Data processed by the Provider on behalf of the Customer.
 - c) the categories of Personal Data processed, the purposes and duration of processing, the sub-processors engaged, and the specific technical and organisational measures applied are further set out in the Data Processing Agreement entered into between the Parties, which forms an integral part of the Agreement and shall prevail over this Section 8 in the event of any inconsistency regarding the processing of Personal Data.

9. Confidentiality and publicity

- 9.1. The Provider covenants to keep confidential and not disclose any information disclosed (whether in writing, orally or otherwise) by the Customer to the Provider, including without limitation all Customer Data (as defined in Section 5.1) (hereinafter "**Customer Confidential Information**") to any person save as expressly permitted by the Agreement. For the sake of clarity, nothing in this Section 9 shall restrict the Provider in engaging third party providers (for example third party Internet service providers) as set forth in Section 1.2.2.
- 9.2. The Customer covenants to keep confidential and not disclose any information disclosed (whether in writing, orally or otherwise) by the Provider to the Customer (hereinafter "**Provider Confidential Information**") save as expressly permitted by the Agreement.
- 9.3. Confidential information of a Party may be disclosed by the other Party to that other Party's officers, employees, agents, insurers and professional advisers, provided that the recipient is bound in writing to maintain the confidentiality of the confidential information disclosed.
- 9.4. The obligations set out in this Section 9 shall not apply to:
 - a) confidential information that is publicly known (other than through a breach of an obligation of confidence);

- b) Customer Confidential Information that is in possession of the Provider prior to disclosure by the Customer, and Provider Confidential Information that is in possession of the Customer prior to disclosure by the Provider;
 - c) Customer Confidential Information that is received by the Provider, and Provider Confidential Information that is received by the Customer, from an independent third party who has a right to disclose the relevant confidential information; or
 - d) confidential information that is required to be disclosed by law, or by a governmental authority, stock exchange or regulatory body, provided that the Party subject to such disclosure requirement must where permitted by law give to the other Party prompt written notice of the disclosure requirement.
- 9.5. Neither Party will make any public disclosure relating to the conditions of the Agreement (including press releases, public announcements and marketing materials) without the prior written consent of the other Party. Notwithstanding the aforesaid, the Provider shall be entitled to identify and name the Customer in any public disclosure for customer reference purposes.

10. Term and Termination

- 10.1. The Agreement is entered into for the fixed term specified in the Order (hereinafter the "**Term**").
- 10.2. Either Party may terminate the Agreement immediately by giving written notice to the other Party if the other Party:
- a) commits any breach of any term of the Agreement, and:
 - (i) the breach is not remediable; or
 - (ii) the breach is remediable, but the other Party fails to remedy the breach within 30 calendar days of receipt of a written notice requiring it to do so; or
 - (iii) persistently breaches the terms of the Agreement, provided that such breaches collectively constitute a material breach of the Agreement.
 - b) the other Party:
 - (i) is dissolved;
 - (ii) ceases to conduct all (or substantially all) of its business (other than the discontinuation of individual product lines or features while the Platform and Saas-Services continue to be provided);
 - (iii) is or becomes insolvent or is declared insolvent; or
 - (iv) is subject to bankruptcy proceedings (*Konkurs*) or a debt-restructuring moratorium (*Nachlassstundung*) under Swiss law, or equivalent proceedings in another jurisdiction, or is declared insolvent by a competent court, or
 - (v) an Order is made for the winding up of the other Party, or the other Party passes a resolution for its winding up (other than for the purpose of a solvent company reorganisation where the resulting entity will assume all the obligations of the other Party under the Agreement).

The Provider may further terminate the Agreement in accordance with the respective Data Processing Agreement between the Parties.

11. Effects of termination

- 11.1. Upon termination or expiry of the Agreement, all the provisions of the Agreement will cease to have effect, save that the following provisions of the Agreement will survive and continue to have effect (in accordance with their terms or otherwise indefinitely): 4, 8, 9, 11.1, 11.2 and 11.3.
- 11.2. Termination or expiry of the Agreement will not affect either Party's accrued liabilities and rights as at the date of termination.
- 11.3. Upon termination or expiry of the Agreement, the Provider will, upon the Customer's written request made within 30 days following the effective date of termination or expiry, make available to the Customer an export of its Customer Data in a commonly used, machine-readable format. Following the earlier of such export or the expiry of that 30-day period, Customer Data will be deleted or returned in accordance with the Data Processing Agreement between the Parties, unless the Provider is legally required to retain it.
- 11.4. Upon termination or expiry of the Agreement, the Provider will issue a final invoice for all Fees and expenses accrued but not yet invoiced up to the effective date of the termination or expiry, which the Customer will pay in accordance with the payment terms of the Agreement.

12. Force Majeure Event

- 12.1. Where a Force Majeure Event gives rise to a failure or delay in either Party performing its obligations under the Agreement (other than obligations to make payment), those obligations will be suspended for the duration of the Force Majeure Event.
- 12.2. A Party who becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in performing its obligations under the Agreement, will:
 - a) immediately notify the other; and
 - b) will inform the other of the period for which it is estimated that such failure or delay will continue.
- 12.3. The affected Party will take reasonable steps to mitigate the effects of the Force Majeure Event.

13. Miscellaneous

- 13.1. No breach of any provision of the Agreement will be waived except with the express written consent of the Party not in breach.
- 13.2. If a clause of the Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other clauses of the Agreement will continue in effect. If any unlawful and/or unenforceable clause would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the clause will continue in effect (unless that would contradict the clear intention of the Parties, in which case the entirety of the relevant clause will be deemed to be deleted). The Parties commit themselves to substitute the ineffective clause with one that most closely reflects the economic intention of the ineffective clause. The same applies to unintentional gaps in the contract.

- 13.3. Nothing in the Agreement will constitute a partnership, agency relationship or contract of employment between the Parties.
- 13.4. This Agreement may not be varied except by a written document signed by or on behalf of each of the Parties.
- 13.5. The Customer may not assign any or all of its contractual rights and/or obligation without the prior written consent of the Provider.
- 13.6. The Customer hereby agrees that the Provider may freely assign any or all of its contractual rights and/or obligations under the Agreement to any Affiliate or any successor to all or a substantial part of the business of the Provider from time to time.
- 13.7. Neither Party will, without the other Party's prior written consent, either during the term of the Agreement or within 6 months after the date of effective termination of the Agreement, engage, employ or otherwise solicit for employment any employee, agent or contractor of the other Party who has been involved in the performance of the Agreement.
- 13.8. Each Party agrees to execute (and arrange for the execution of) any documents and do (and arrange for the doing of) any things reasonably within that Party's power, which are necessary to enable the Parties to exercise their rights and fulfil their obligations under the Agreement.
- 13.9. This Agreement is made for the benefit of the Parties, and is not intended to benefit any third Party or be enforceable by any third party. The rights of the Parties to terminate, rescind, or agree any amendment, waiver, variation or settlement under or relating to the Agreement are not subject to the consent of any third party.
- 13.10. This Agreement constitutes the entire agreement between the Parties in relation to the subject matter of the Agreement, and supersedes all previous agreements, arrangements and understandings between the Parties in respect of that subject matter.
- 13.11. This Agreement will be governed by and construed in accordance with the substantive laws of Switzerland excluding its conflict of law provisions and excluding the United Nations Convention on the International Sale of Goods (CISG); and the exclusive place of jurisdiction is Zürich (City), Switzerland. The Provider may chose as alternative place of jurisdiction any competent court of justice worldwide.

Annex 1 – Set-up

1. Platform Scope and Functional Description

The Provider operates an M&A due-diligence support platform designed to ingest, extract, and analyse deal documents uploaded by the Customer (such as contracts, board minutes, cap tables, financial statements, and transaction correspondence). The Platform establishes a structured overview of a target company, generating entity, party, and signatory extractions alongside provenance and supporting evidence.

Core functionality includes:

- Account and Session Management: federated identity verification and authentication via Microsoft Entra ID, Google OAuth, and WebAuthn-compliant passkeys.
- Collaboration Infrastructure: workspace management, access delegation, and external deal collaborator/invitee workflows.
- AI-Assisted Extraction & Setup Agent: automated entity recognition and a conversational setup agent designed to elicit deal parameters and cross-reference records against public commercial registers (e.g., the Swiss commercial registry, Zefix).

2. Onboarding and Provisioning Steps

The Provider shall carry out the following implementation steps:

- Tenant Provisioning: deployment and isolation of the Customer's dedicated organisation environment within the Provider's Swiss cloud infrastructure (europa-west6, Zurich), including the configuration of envelope encryption keys via Google Cloud KMS and Secret Manager.
- Access & Identity Setup: configuration of organisation-level identity routing and validation of Customer administrative credentials via supported OAuth identity providers or WebAuthn credentials.
- Workspace Initialisation: creation of primary Customer administrator accounts, configuration of default organisational access controls, and provisioning of initial deal spaces.
- Platform Walkthrough: delivery of one remote onboarding and training session (up to 90 minutes) for authorised administrative personnel, covering ingestion workflows, extraction validation, and collaborator management.
- API Credential Delivery (Optional): where the Provider subsequently makes available an application programming interface (API) for this purpose and access to it is specified in the Order, generation and delivery of API access tokens together with technical documentation, in accordance with Section 2.2.1.

3. Configuration Timeline and Acceptance

- **Standard Timeline:** onboarding and initial tenant configuration will be completed within 10 Business Days following the effective date of the Order, subject to timely satisfaction of the Customer-side prerequisites set out in Section 5 below.
- **Acceptance Criteria:** set-up services under this Annex 1 shall be deemed accepted and complete upon the earlier of (a) delivery of active Customer administrator credentials and confirmation of workspace provisioning; or (b) completion of the guided platform walkthrough session.

4. Technical Constraints and Ingestion Standards

Supported File Formats: PDF, DOCX, XLSX, CSV, PNG, TIFF and JPG. Scanned documents must feature a minimum resolution of 300 DPI to enable optical character recognition (OCR) and accurate entity extraction.

- **Payload Limits:** maximum single file upload size is 30MB. Total volume limits, concurrent uploads, or active deal space quotas are governed by the tiers specified in the Order.
- **Supported Processing Languages:** extraction models and the conversational setup agent are optimised for source materials in English, German, French, and Italian. Document payloads that are corrupted, password-protected with third-party digital rights management (DRM), or handwritten fall outside automated extraction performance standards.
- **Public Registry Integration:** automated external verification is limited to public registries natively integrated into the Platform (such as the Swiss commercial registry, Zefix) and depends entirely on the uptime, query quotas, and availability of the respective public registries. For the avoidance of doubt, unavailability of such third-party public registries does not constitute Downtime under Annex 2, Section 1.

5. Customer-Side Prerequisites

To enable setup and ongoing functionality, the Customer shall:

- **Appoint Primary Administrators:** designate at least one authorised primary administrator to manage workspace memberships, issue binding technical instructions, and approve user access tiers.
- **Maintain Compatible Client Environments:** ensure authorised users access the Platform using modern, vendor-supported web browsers (Google Chrome, Microsoft Edge, Mozilla Firefox, or Apple Safari) enforcing TLS 1.2 or higher.
- **Manage Authentication Assets:** ensure that all invited end-users maintain valid organisational accounts with supported identity providers (Microsoft Entra ID or Google) or possess WebAuthn-compatible authenticators for passkey logins.
- **Independent Systems Integration:** the Customer remains exclusively responsible for the development, implementation, and network security of any internal endpoints or connectors interfacing with any API made available by the Provider pursuant to Section 2.2.1.

Annex 2 - Service Level Agreement (SLA)

6. Service Availability

The Provider will use commercially reasonable efforts to ensure that the Platform will be available for 99% of the time, calculated on a calendar monthly basis. Downtime" (calculated as the difference between 100% of the time in a calendar month and the actual percentage of time during that month that the Platform is available) will exclude unavailability due to (i) scheduled maintenance; (ii) technical malfunctions in the Provider's website systems or any other circumstances beyond the Provider's reasonable control (for example but not limited to Internet delays, network congestion and ISP malfunctions); or (iii) unavailability, downtime, rate-limiting, degradation, or API disruptions of underlying upstream third-party AI or cloud providers (such as Google Cloud Platform, as further described in Section 1.4.2 of these T&C.

7. Helpdesk

The Provider will use commercially reasonable efforts to make available a 24/7 email helpdesk facility.

The Customer must make all requests for Support Services through the helpdesk at support@dilix.ch.

7.1. Response Times

The Provider will use reasonable endeavours to respond to requests for Support Services made through the helpdesk as swiftly as possible and within the following response times:

Level	Description	Service Time	Response Time
1	Issue affects all or at least core functionality of Application preventing the Customer from carrying out core business processes related to the service.	Office hours: 8.00 - 17:00 CET/CEST on Business Days*	4 hours
2	All other issues with the Application with the core functionalities being usable.	Office hours: 08:00 – 17:00 CET/CEST on Business Days*	2 Business Days

*Business Day meaning Monday-Friday except Swiss public national holidays and holidays in the municipality of Zurich City.

7.2. Resolution Times

The Provider will use reasonable endeavours to resolve issues raised by the Customer through the Helpdesk as swiftly as possible taking into account the severity of the incident, it being understood, however, that the Provider cannot guarantee resolution times.

8. Measurement and Penalties

Uptime is measured using the Provider's automated systems over each calendar month. It is calculated to the nearest minute, based on the number of minutes in the given month (for instance, a 31-day month contains 44'640 minutes). If uptime for any item drops below the threshold for Service Availability (this SLA, Section 1), a penalty will be applied in the form of a credit for the client meaning that the following month's Fee will be reduced accordingly.

The level of penalty will be calculated depending on the number of hours for which the Platform was unavailable, minus the Downtime permitted by this SLA (Section 1).

Level	Failure description	Penalty per Hour (pro-rated to nearest minute)
1	All users and critical functions are affected. Service is completely unavailable.	2.5% of total monthly Fee
2	Large number of users or functions are affected.	1% of total monthly Fee
3	Limited number of users or functions are affected. Business processes can continue.	0.5% of total monthly Fee
4	Minimal impact on users and/or functions. Business processes can continue.	No penalty.

The Provider will reasonably determine, in to which level an issue falls.

Penalties in any month are capped at 50% of the total monthly Fee.

Notwithstanding the foregoing, no penalty under this Section 3 shall apply in respect of any unavailability occurring during the first six (6) months following the start of the Term (as defined in Section 10.1 of these T&C); for the avoidance of doubt, this does not affect the Provider's other obligations under this SLA during that period.

9. Limits on Support Services

The Provider shall have no obligation under the Agreement to provide Support Services in respect of any fault or error caused by:

- a) the improper use of the Platform by the Customer; or
- b) the use of the Platform otherwise than in accordance with the terms and conditions of the Agreement.

10. Upgrades

The Customer acknowledges that from time to time during the Term the Provider may apply Upgrades to the Platform, "**Upgrade**" meaning new versions of, and updates to the Platform or the Application, whether for the purposes of fixing an error, bug or other issue or enhancing the functionality of the Platform or Application. The Customer acknowledges that such Upgrades may, result in changes the appearance and/or functionality of the Platform and/or Application.

The Provider will give to the Customer prior written notice of any significant Upgrade to the Platform. Such notice shall include details of the specific changes to the functionality of the Platform and/or Application resulting from the application of the Upgrade.

11. Annexed maintenance

The Provider may suspend its SaaS-Services (including access to the Platform and/or the Application) in order to carry out scheduled maintenance, such maintenance to be carried out whenever possible outside office hours (as per Section 2.1 above).

The Provider must give to the Customer at least 3 calendar days' written notice of a scheduled maintenance, including full details of the expected Downtime.

12. Data Storage

12.1. Operational Data Storage

Data is stored at rest using AES-256 encryption, with uploaded due-diligence document payloads additionally protected via application-layer AES-256-GCM encryption using cryptographic keys managed through Google Cloud Key Management Service (Cloud KMS). Client Data is primarily processed and stored in Switzerland (Google Cloud, europe-west6 region, Zurich). The Provider is free to change the physical location of data processing and storage to any other country recognized as offering an adequate level of data protection under the Swiss Federal Act on Data Protection (FADP) or the GDPR, without any notification requirement to the Customer.

12.2. Operational Data Transport

All data in transit across public networks and internal connections, including communication between the Application and internal or external components (e.g. web browsers), is secured using TLS encryption (TLS 1.2 or higher).

13. Data Backups

The Provider's database is automatically backed up on a rolling basis approximately every four (4) hours, with a rolling retention period of seven (7) days and support for point-in-time recovery within that retention window. All backups are encrypted at rest using AES-256 encryption.

14. System Access

Access to a running system is controlled via federated, passwordless login (OAuth via Microsoft Entra ID and Google, and passkeys (WebAuthn)) as well as a permissions and invitations system configured by the Provider in cooperation with the Customer.

Non-customer access to the running system is restricted to the Provider's engineers for the purpose of support, system testing and maintenance.

15. Contract Termination

Upon termination of a customer relationship, the Customer may request the removal of the personal data of its users included in the Customer Data. The Provider shall remove such data but shall in any event be entitled to keep and use, for the purposes described in Section 1.4.4 (including to calibrate, improve, or validate its AI models), any Customer Data in anonymized or aggregated form (for example but not limited to user ID, year of birth, gender), subject to the Customer's opt-out rights under Sections 1.4.4 and 1.4.5.